Extended Truncated-Differential Distinguishers on Reduced-Round AES

Zhenzhen Bao[1] Jian Guo[1] Eik List[2]

[1]CATF, Nanyang Technical University, Singapore

[2]Bauhaus-Universität Weimar, Germany

November 2020

Section 1

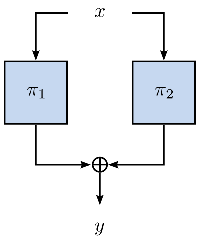
Motivation

Sum of Independent Permutations

- Simple approach to turn PRPs into a PRF:

$$\Sigma_k(x) \stackrel{\text{def}}{=} \bigoplus_{i=1}^{k} \pi_i(x)$$

- Assume: $\pi_i \twoheadleftarrow \text{Perm}(\mathbb{F}_2^n)$
- Goal of distinguisher $\mathbf{A}$: Distinguish $\sum_k$ from random function

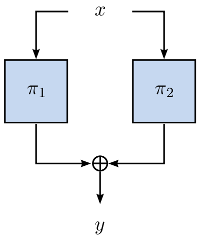


$X \twoheadleftarrow \mathcal{X} = X$ is sampled uniformly at random and independently from other samplings from a set $\mathcal{X}$.

Sum of PRPs

Results from Provable Security

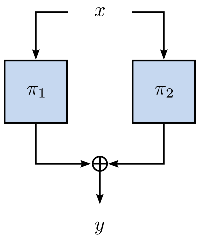
- XOR of k PRPs gives a PRF with security at least in $O(2^{\frac{k}{k+1}n})$ [Luc00].
- Intensive analysis, mostly on Σ_2 [BI99, CLP14, Luc00, MP15, Pat08a, Pat08b, Pat10, Pat13]
- Indistinguishable from PRF up to $q \in O(2^n)$ queries [BN18a, DHT17, MN17]
- Indifferentiable from PRF up to $q \in O(2^n)$ queries [BN18b]



Sum of PRPs

[Pat08b, Pat13]

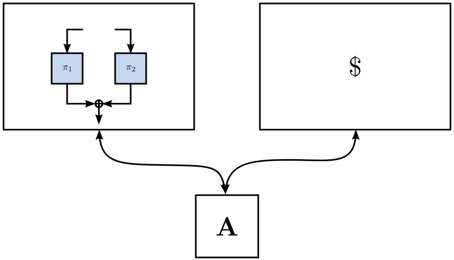
- Security maximum: $q < 2^n$:
- Interest of most provable security ends here
- What if few responses are random?
  $\implies$ other distinguishing approaches needed
- Motivated Patarin's studies [Pat08b, Pat13]



Sum of PRPs

[Pat08b, Pat13]

- $\mathbf{A}$ has access to function generator $\mathcal{G}(F)$
  - $g \geq 1$ random constructions
  - $q \leq 2^n$ queries on each
- Approach: Count #collisions
- Expectations (and standard deviations) differ slightly
  $\implies$ distinguisher given sufficiently many queries

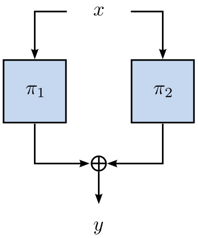


Example: Sum of 2 PRPs

Example

- $q = 2^8$ queries/experiment

```
./test_sum_of_prps.py -k 2 -n 8 -e 65536
Sum of 2 PRPs
127.922623 11.393390
PRF
127.584320 11.303495
```



$$\Sigma_2 : \quad \mu = \frac{\binom{q}{2}}{2^n - 1} \qquad \text{PRF} : \quad \mu = \frac{\binom{q}{2}}{2^n}$$

Distinguishing Complexity for Sum of k PRPs

[Pat08b, Pat13]

Table: #Collisions $\mathbb{E}[\mathsf{N}_k]$ after q queries and distinguishing complexity for $q \simeq 2^n$ [Pat08b].

#Permutations	2	3	4	k
$\mathbb{E}[\mathsf{N}_k]$	$\frac{g\binom{q}{2}}{2^n} + \frac{g\binom{q}{2}}{2^n(2^n-1)}$	$\frac{g\binom{q}{2}}{2^n} - \frac{g\binom{q}{2}}{2^n(2^n-1)^2}$	$\frac{g\binom{q}{2}}{2^n} + \frac{g\binom{q}{2}}{2^n(2^n-1)^3}$	$\frac{g\binom{q}{2}}{2^n} + \frac{(-1)^k g\binom{q}{2}}{2^n(2^n-1)^{k-1}}$
#Queries	$O(2^{2n})$	$O(2^{4n})$	$O(2^{6n})$	$O(2^{(2k-2)n})$

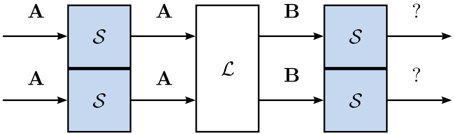
$$\Pr[\mathsf{COLL}] = \frac{1}{2^n} + \frac{(-1)^k}{2^n(2^n-1)^{k-1}} .$$

N_k = #Collisions for Σ_k; g = #Functions; q = #Queries

Expectation Cryptanalysis

Chen et al. [CMSZ15]

- First to observe applicability of expectation cryptanalysis for extending integrals
- Start: Propagation of ALL-subsets in SPNs ($\mathbf{A}$, iterate over all elements)
- Affine layer $\mathcal{L}$:
  - ALL ($\mathbf{A}$) $\xrightarrow{\mathcal{L}}$ BALANCED ($\mathbf{B}$)
- Next non-linear layer $\mathcal{S}$:
  - BALANCED ($\mathbf{B}$) $\xrightarrow{\mathcal{S}}$ UNKNOWN ($?$)



Expectation Cryptanalysis (cont'd)

Core Observation by Chen et al. [CMSZ15]

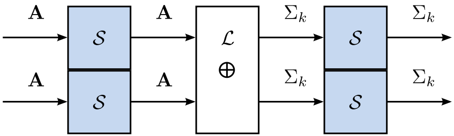
- Affine layers $\mathcal{L}(x) = \mathbf{M} \cdot x + \mathbf{b}$
  - $\mathbf{M} = \text{circ}(\mathbf{v})$ where

$$\mathbf{v} = (a_1, \ldots, a_m), \qquad a_i \in \mathbb{F}$$

  - Often: $k = \text{wt}(\mathbf{v}) > 1$: $\mathbf{v}$ is Σ_k-sum of components

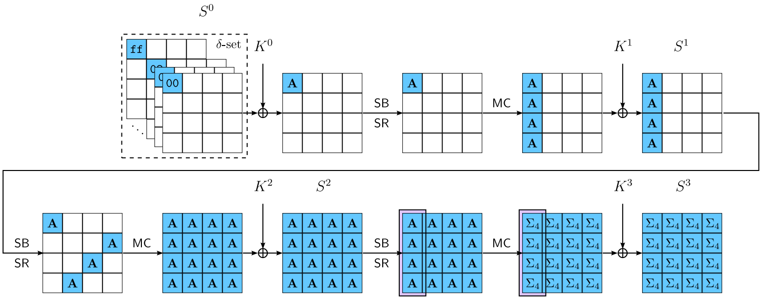
$$\mathbf{A} \xrightarrow{\mathcal{L}} \Sigma_k$$

  - Distribution of collisions preserved by subsequent non-linear layer $\mathcal{S}$



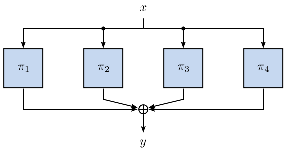
- Focused on Type-II and Nyberg Feistel Networks with 4-bit S-boxes

An Interesting Application Target: AES



- MixColumns: $\mathbf{M} = \text{circ}(2, 3, 1, 1)$
- $\implies$ Σ_4 for the well-known 3-round integral:

$$(\mathbf{A}, \mathbf{A}, \mathbf{A}, \mathbf{A}) \xrightarrow{\text{MC}} (\Sigma_4, \Sigma_4, \Sigma_4, \Sigma_4)$$



Distinguishers on 5^+-round AES

- Intensive studies since 2016:
  - Sun et al.'s key-dependent integral [SLG$^+$16]
  - Open question: why only chosen ciphertext, full codebook
- Improvements:
  - Key-dependent impossible differentials [GRR16, Gra18a, HCGW18]
  - Key-dependent integral [HCGW18].
- Second direction: differential-based, subspace trail, invariant
  - Multiple-of-n [GRR17, BCC19] [1]
  - Mixture differentials [Gra18b]
  - Best current distinguishers: Yoyo/Exchange [BR19b] [2]
- Similar to our focus:
  - Expectation and variance cryptanalysis [GR18, GR19]
- Interesting topic, many things still in the dark

---

[1] The key-recovery attack complexity was reduced by [BDK$^+$18].

[2] The key-recovery attacks by [DKRS20] represent a follow-up work that follows this direction, but considers conditional boomerangs distinguishers on fewer rounds.

Section 2

Four-round Distinguisher

Statistical Framework

[Gra18b]

- For success probability $\geq p_S$, #Experiments n must satisfy:

$$n \geq \frac{2\left(p_{\mathsf{rand}}(1-p_{\mathsf{rand}}) + \frac{\sigma^2_{\mathsf{AES}}}{\sigma^2_{\mathsf{rand}}} p_{\mathsf{AES}}(1-p_{\mathsf{AES}})\right)}{(p_{\mathsf{AES}} - p_{\mathsf{rand}})^2} \cdot \left(\mathsf{erfinv}(2 \cdot p_S - 1)^2\right),$$

$\mathsf{erfinv}(x) = \Pr[X \in [-x, +x]],\ X \sim \mathcal{N}(0, 0.5)$
p_{rand} = probability for random experiment
p_{AES} = probability for the reduced AES
σ^2 = variance

Four-round Distinguisher

- For 4-round AES:

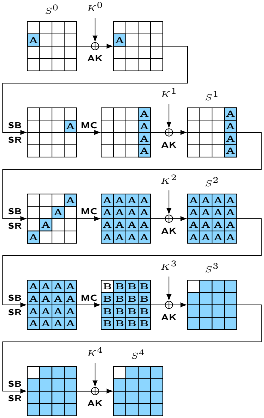
$$\Pr_{\text{AES}}\left[S^{3,i}_{r,c} = S^{3,j}_{r,c}\right] \simeq \frac{1}{2^8} + \frac{1}{2^8(2^8-1)^3} \simeq 2^{-8} + 2^{-31.983}$$

- For random truncated permutation:

$$\Pr_{\text{rand}}\left[S^{3,i}_{r,c} = S^{3,j}_{r,c}\right] = \frac{2^{120}-1}{2^{128}-1} \simeq 2^{-8} - 2^{-128}.$$

- $p_S \geq 0.95$:
  $\implies n \geq 2^{58.402}$ pairs
  $\implies 2^{43.41}$ δ-sets of $2^{51.41}$ CPs

- Optimizations: use all output bytes, build plaintext structures



$r, c \in \{0,1,2,3\}$ = row, column.

Four-round Distinguisher
Small-AES

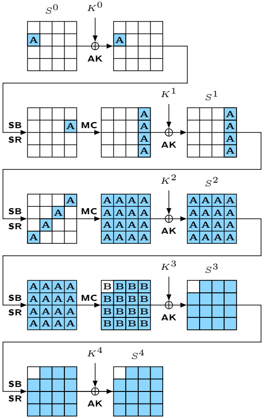
- For 4-round Small-AES:

$$\Pr_{\text{Small-AES}}\left[S^{3,i}_{r,c} = S^{3,j}_{r,c}\right] \simeq \frac{1}{2^4} + \frac{1}{2^4(2^4-1)^3} \simeq 2^{-4} + 2^{-15.721}$$

- For a truncated random permutation:

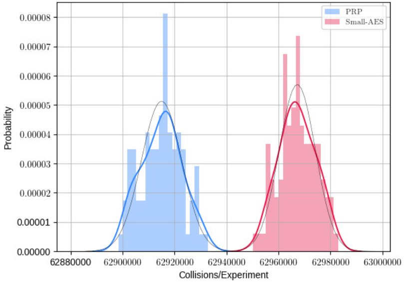
$$\Pr_{\text{rand}}\left[S^{3,i}_{r,c} = S^{3,j}_{r,c}\right] = \frac{2^{60}-1}{2^{64}-1} \simeq 2^{-4} - 2^{-64.093}$$

- $p_S \geq 0.95$:
  $\implies n > 2^{29.878}$ pairs
  $\implies 2^{23}$ δ-sets of 2^{27} CPs



Four-round Distinguisher

Small-AES



#δ-sets	Theory		Experiments			
	Small-AES	π	Small-AES		π	
$(\log_2)$	μ	μ	μ	σ	μ	σ
20	7 866 650	7 863 200	7 870 789.	2 918.	7 864 396.	2 566.
21	15 733 300	15 728 600	15 742 188.	3 809.	15 728 650.	3 957.
22	31 466 600	31 457 300	31 484 544.	6 007.	31 457 205.	5 096.
23	62 933 200	62 914 600	62 967 244.	7 030.	62 915 004.	7 820.

100 random independent keys and 2^s random δ-sets. Experimental values are rounded. π = Speck-64-96

Section 3

Five-round Distinguisher

Five-round Distinguisher

- Goal: At least one inactive inverse diagonal after 5 rounds
- Probabilities for concrete inactive anti-diagonal:

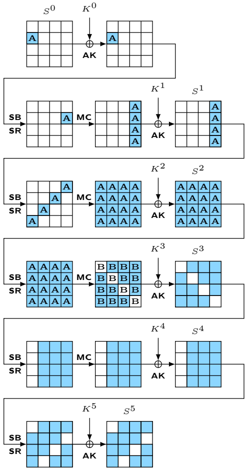
$$\Pr_{\mathsf{AES}}\left[S^3 \in \mathcal{D}_{\{c\}}\right] \simeq \left(2^{-8} + \frac{1}{2^8 \cdot (2^8-1)^3}\right)^4 \simeq 2^{-32} + 2^{-53.983}$$

$$\Pr_{\mathsf{rand}}\left[S^3 \in \mathcal{D}_{\{c\}}\right] \simeq \frac{2^{96}-1}{2^{128}-1} \simeq 2^{-32} - 2^{-128}$$

- Probability for at least one inactive anti-diagonal:

$$p_{\mathsf{AES}} \simeq 1 - \left(1 - \Pr_{\mathsf{AES}}\left[S^3 \in \mathcal{D}_{\{c\}}\right]\right)^4 \simeq 2^{-30} + 2^{-51.985}$$

$$p_{\mathsf{rand}} \simeq 1 - \left(1 - \Pr_{\mathsf{rand}}\left[S^3 \in \mathcal{D}_{\{c\}}\right]\right)^4 \simeq 2^{-30} - 2^{-61.415}$$



$c \in \{0, 1, 2, 3\}$ = column.

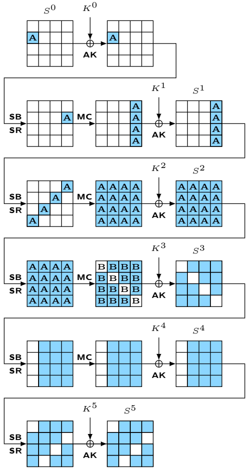
Five-round Distinguisher

Complexities

- For a success probability of approximately $p = 0.95$: $n > 2^{76.406}$ pairs
- Data: 2^{36} structures of 2^{32} texts each
- Form $4 \cdot 2^{24} \cdot \binom{2^8}{2}$ pairs

$$2^{36} \cdot 4 \cdot 2^{24} \cdot \binom{2^8}{2} \simeq 2^{77} \text{ pairs}$$

- Memory: Dominated by 2^{32} states in $\mathcal{Q}$ and four lists L_i of 4×2^{32} columns at a time
- Time: $2^{73.3}$ MAs + $2^{68.3}$ Encs



Five-round Distinguisher

Small AES

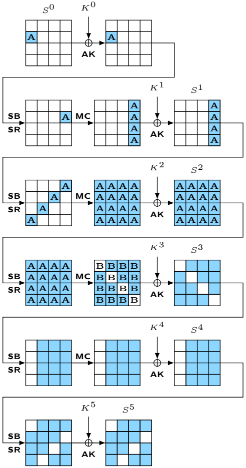
- Probability for at least one inactive anti-diagonal:

$$p_{\text{Small-AES}} \simeq 1 - \left(1 - \Pr_{\text{Small-AES}}\left[S^3 \in \mathcal{D}_{\{c\}}\right]\right)^4 \simeq 2^{-14} + 2^{-23.748}$$

- For a truncated random permutation:

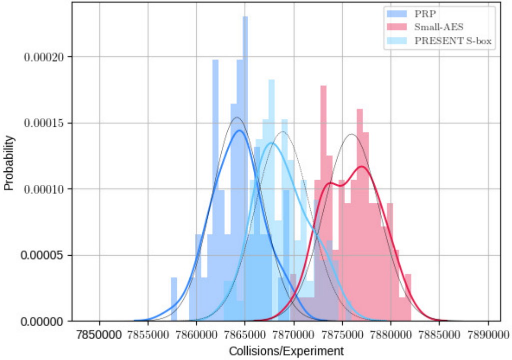
$$p_{\text{rand}} \simeq 1 - \left(1 - \Pr_{\text{rand}}\left[S^3 \in \mathcal{D}_{\{c\}}\right]\right)^4 \simeq 2^{-14} - 2^{-29.415}$$

- $p_S \geq 0.95 \implies n > 2^{35.878}$



Five-round Distinguisher

Verification with Small-scale AES



Instance	μ	σ
π		
Theory	7 864 140	2 804.22
Experiment	7 864 379.	2 492.46
Small-AES		
Theory	7 873 286	2 805.85
Experiments	7 875 860.	2 844.95
PRESENT S-box	7 868 881.	2 785.78

100 random independent keys and 2^{30} random δ-sets. W/o MC in final round and tested on first column. Experimental values are rounded. π = Speck-64-96.

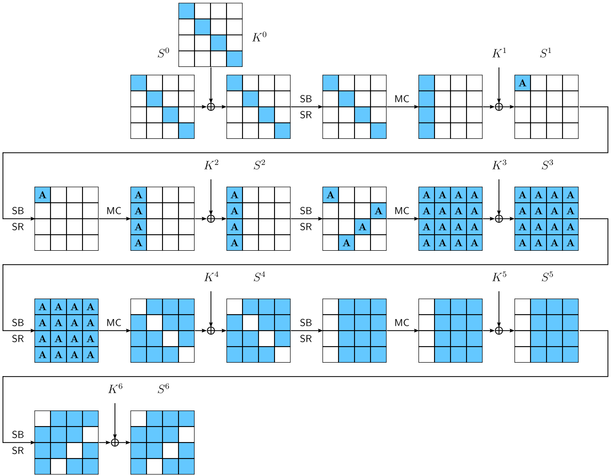
Section 4

Six-round Key Recovery

Key-recovery on Six-round AES

Overview

- Prepend one round
- Recover $K^0[0, 5, 10, 15]$

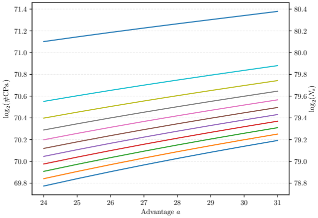


Key-recovery on Six-round AES

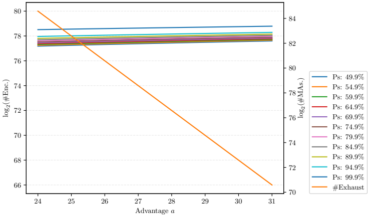
Optimizing Complexities

Selçuk [Sel08]

Data complexity:

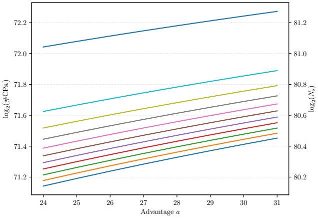


Computational complexity:

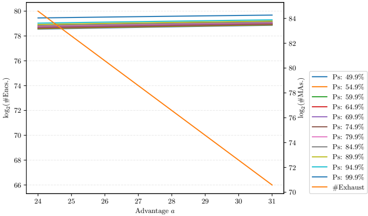


Samajder and Sarkar [SS17]

Data complexity:



Computational complexity:



Selçuk [Sel08]:

$a = 25.5$

$N = 2^{79.045}$ pairs

$D = 2^{70.045}$ CPs

$T = 2^{77.455}$ Encs

Samajder and Sarkar [SS17]:

$a = 25$

$N = 2^{80.285}$ pairs

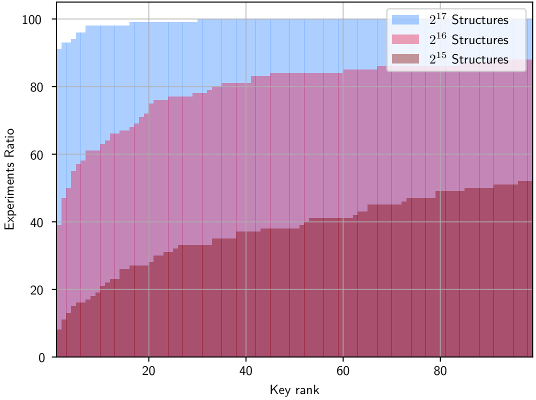
$D = 2^{71.285}$ CPs

$T = 2^{78.695}$ Encs

Key-recovery on Six-round AES

Experimental Results on Small-AES

- Goal: Recover $K^0[0, 5, 10, 15]$
- 2^{15} structures:
  - $53\times$ among top 100 keys
- 2^{16} structures:
  - $92\times$ among top 100 keys
  - Worst: rank 313



Ranks for the correct key from 100 runs; random keys and 2^{15} or 2^{16} structures of 2^{16} texts each.

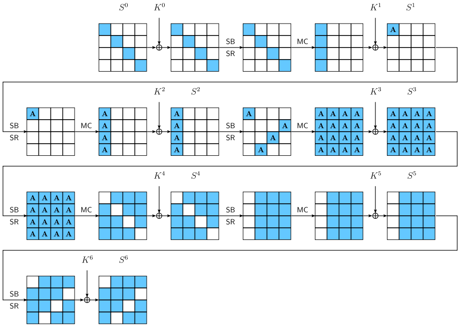
Section 5

Six-round Distinguisher

Extending the Distinguisher to Six Rounds

Idea

- Diagonal $\mathcal{D}_0 = \mathcal{X}_0 \cup \mathcal{X}_1$ (disjoint)



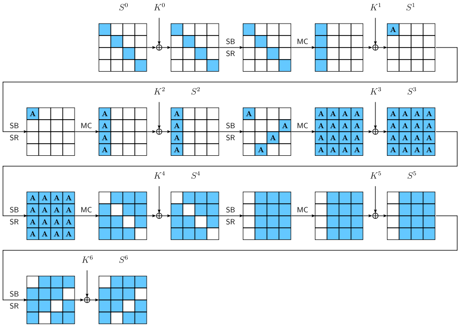
$$p_{\mathsf{AES}_6} \simeq \frac{4 \cdot 2^{24} \cdot \binom{2^8}{2} \cdot \left(2^{-30} + 2^{-51.985}\right) + \binom{2^{32}}{2} - \left(4 \cdot 2^{24} \cdot \binom{2^8}{2}\right) \cdot \left(2^{-30} - 2^{-61.415}\right)}{\binom{2^{32}}{2}}$$

$$\simeq 2^{-30} - 2^{-61.415} + 2^{-73.989}$$

Extending the Distinguisher to Six Rounds

Idea

- Diagonal $\mathcal{D}_0 = \mathcal{X}_0 \cup \mathcal{X}_1$ (disjoint)
- $\mathcal{X}_1$ = good pairs
  p_{AES_5} for all $x = 4 \cdot \binom{2^8}{2} \cdot 2^{24}$ pairs in δ-sets



$$p_{\mathsf{AES}_6} \simeq \frac{4 \cdot 2^{24} \cdot \binom{2^8}{2} \cdot \left(2^{-30} + 2^{-51.985}\right) + \binom{2^{32}}{2} - \left(4 \cdot 2^{24} \cdot \binom{2^8}{2}\right) \cdot \left(2^{-30} - 2^{-61.415}\right)}{\binom{2^{32}}{2}}$$

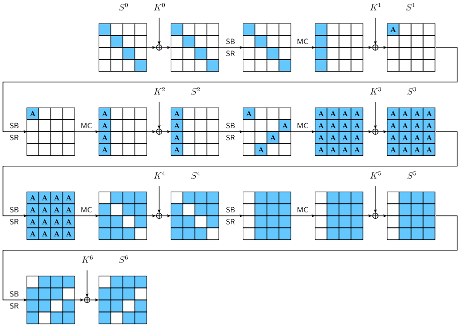
$$\simeq 2^{-30} - 2^{-61.415} + 2^{-73.989}$$

Extending the Distinguisher to Six Rounds

Idea

- Diagonal $\mathcal{D}_0 = \mathcal{X}_0 \cup \mathcal{X}_1$ (disjoint)
- $\mathcal{X}_1$ = good pairs
  $p_{\mathsf{AES}\,5}$ for all $x = 4 \cdot \binom{2^8}{2} \cdot 2^{24}$ pairs in δ-sets
- $\mathcal{X}_0 = \binom{2^{32}}{2} - x$ "random" pairs
  Assumption: They behave "randomly"

$$p_{\mathsf{AES}\,6} = \frac{|\mathcal{X}_0| \cdot p_{\mathsf{rand}} + |\mathcal{X}_1| \cdot p_{\mathsf{AES}\,5}}{|\mathcal{D}_0|}$$



$$p_{\mathsf{AES}\,6} \simeq \frac{4 \cdot 2^{24} \cdot \binom{2^8}{2} \cdot \left(2^{-30} + 2^{-51.985}\right) + \binom{2^{32}}{2} - \left(4 \cdot 2^{24} \cdot \binom{2^8}{2}\right) \cdot \left(2^{-30} - 2^{-61.415}\right)}{\binom{2^{32}}{2}}$$

$$\simeq 2^{-30} - 2^{-61.415} + 2^{-73.989}$$

Extending the Distinguisher to Six Rounds

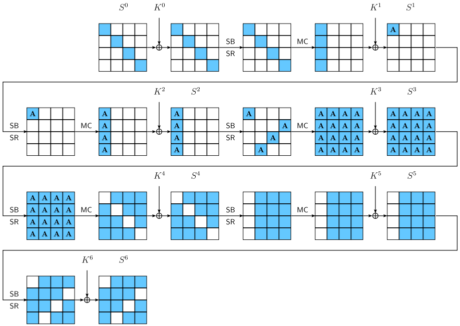
Idea

- Diagonal $\mathcal{D}_0 = \mathcal{X}_0 \cup \mathcal{X}_1$ (disjoint)
- $\mathcal{X}_1$ = good pairs
  $p_{\mathsf{AES}\,5}$ for all $x = 4 \cdot \binom{2^8}{2} \cdot 2^{24}$ pairs in δ-sets
- $\mathcal{X}_0 = \binom{2^{32}}{2} - x$ "random" pairs
  Assumption: They behave "randomly"

$$p_{\mathsf{AES}\,6} = \frac{|\mathcal{X}_0| \cdot p_{\mathsf{rand}} + |\mathcal{X}_1| \cdot p_{\mathsf{AES}\,5}}{|\mathcal{D}_0|}$$

- Random truncated permutation:

$$p_{\mathsf{rand}} \simeq 2^{-30} - 2^{-61.415}$$



$$p_{\mathsf{AES}\,6} \simeq \frac{4 \cdot 2^{24} \cdot \binom{2^8}{2} \cdot \left(2^{-30} + 2^{-51.985}\right) + \binom{2^{32}}{2} - \left(4 \cdot 2^{24} \cdot \binom{2^8}{2}\right) \cdot \left(2^{-30} - 2^{-61.415}\right)}{\binom{2^{32}}{2}}$$

$$\simeq 2^{-30} - 2^{-61.415} + 2^{-73.989}$$

Extending the Distinguisher to Six Rounds

Idea

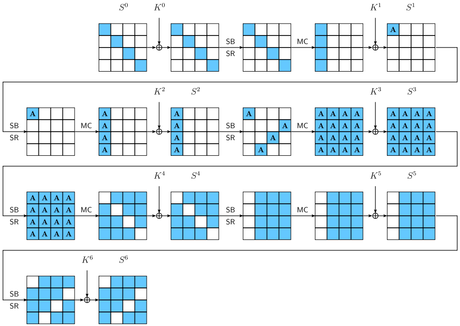
- Diagonal $\mathcal{D}_0 = \mathcal{X}_0 \cup \mathcal{X}_1$ (disjoint)
- $\mathcal{X}_1$ = good pairs
  $p_{\mathsf{AES}\,5}$ for all $x = 4 \cdot \binom{2^8}{2} \cdot 2^{24}$ pairs in δ-sets
- $\mathcal{X}_0 = \binom{2^{32}}{2} - x$ "random" pairs
  Assumption: They behave "randomly"

$$p_{\mathsf{AES}\,6} = \frac{|\mathcal{X}_0| \cdot p_{\mathsf{rand}} + |\mathcal{X}_1| \cdot p_{\mathsf{AES}\,5}}{|\mathcal{D}_0|}$$

- Random truncated permutation:

$$p_{\mathsf{rand}} \simeq 2^{-30} - 2^{-61.415}$$

- Theoretical p_{AES} after six rounds:



$$p_{\mathsf{AES}\,6} \simeq \frac{4 \cdot 2^{24} \cdot \binom{2^8}{2} \cdot \left(2^{-30} + 2^{-51.985}\right) + \binom{2^{32}}{2} - \left(4 \cdot 2^{24} \cdot \binom{2^8}{2}\right) \cdot \left(2^{-30} - 2^{-61.415}\right)}{\binom{2^{32}}{2}}$$

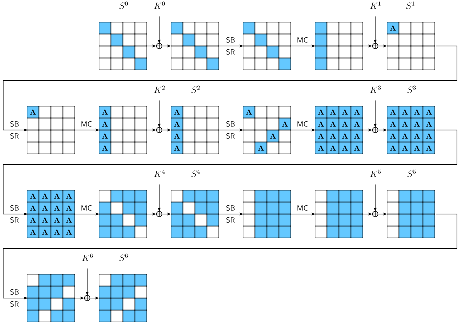
$$\simeq 2^{-30} - 2^{-61.415} + 2^{-73.989}$$

Six-round Distinguisher

- Difference would be tiny

$$\left|p_{\mathsf{rand}} - p_{\mathsf{AES}_6}\right| \simeq 2^{-73.989}.$$

- For $p_S \geq 0.95$: $n \geq 2^{120.5}$ pairs
- Diagonal structure of 2^{32} texts $= \binom{2^{32}}{2}$ pairs
  $\implies 2^{57.5}$ structures
  $\implies 2^{89.5}$ CPs



Six-round Distinguisher

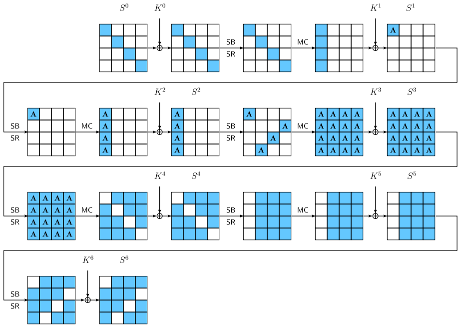
Verification with Small-AES

- Here

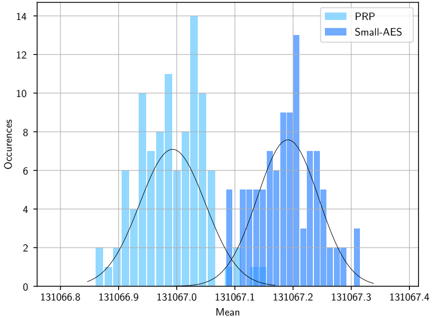
$$p_{\text{rand}} \simeq 2^{-14} - 2^{-29.415}$$

$$p_{\text{Small-AES}_6} \simeq 2^{-14} - 2^{-29.415} + 2^{-33.869}$$

- $n \geq 2^{56.18}$ pairs $\Longrightarrow \simeq 2^{41.18}$ CPs
- Practical!



- Results with Small-AES of 5 Rounds + SB + AK
- 100 experiments
- #collisions in at least one ciphertext column per structure of 2^{16} texts
- π = Speck-64-96



Instance		Per structure		Per experiment	
		μ	σ	μ	σ
π	Theory	131 067.000	362.021	5 085 047 291 904.000	2 254 936.126
	Experiment	131 066.993	362.022	5 085 047 013 804.869	2 182 652.286
Small-AES	Theory	131 067.137	362.021	5 085 052 607 135.744	2 254 937.303
	Experiments	131 067.191	362.041	5 085 054 704 906.403	2 040 063.345

Theoretical Verification

3 approaches for verifications of the theoretical probabilities:

1. Patarin's sum of permutation
2. Proof following the footsteps of Grassi and Rechberger [GR19] under assumptions:
   - Ideal S-box
   - Any combination of input-output cells is equally successful
3. Rønjom's truncated-differential propagation matrices [Røn19]

- Equal theoretical probabilities for all three
- But. . . not completely the real-world setting

More Precision: Dependencies

We analyzed dependencies

- Index dependencies of active input cells and concerned output cells
- Effects of the S-box

In appendix and in paper

Section 6

Summary

Summary

Truncated-differential distinguishers

- On 4-round AES
- On 5-round AES
- On 6-round AES
- Theoretical probabilities verified with approach by Rønjom [Røn19]
- All implemented with Small-AES

Attack Type	Time		Data		Ref.
Five Rounds					
Integral	2^{128}	XORs	2^{128}	CC	[SLG+16]
Threshold MD	$2^{98.1}$	MAs	2^{89}	CP	[Gra17]
Impossible MD	$2^{97.8}$	MAs	2^{82}	CP	[Gra17]
Truncated differential	$\mathbf{2^{73.3}}$	**MAs**	$\mathbf{2^{68}}$	**CP**	**[This work]**
Probabilistic MD	$2^{71.5}$	MAs	2^{52}	CP	[Gra19, Gra17]
Truncated differential$^{(1)}$	$2^{52.6}$	MAs	$2^{48.96}$	CP	[GR18, GR19]
Variance of TD$^{(1)}$	$2^{37.6}$	MAs	2^{34}	CP	[GR18, GR19]
Multiple-of-8	$2^{35.6}$	MAs	2^{32}	CP	[GRR17]
Yoyo	$2^{26.2}$	XORs	$2^{27.2}$	ACC	[BR19a]
Yoyo	$2^{25.8}$	XORs	$2^{26.8}$	ACC	[RBH17]
Six Rounds					
Impossible Yoyo	$2^{121.83}$	XORs	$2^{122.83}$	ACC	[RBH17]
Truncated differential	$\mathbf{2^{96.52}}$	**MAs**	$\mathbf{2^{89.43}}$	**CP**	**[This work]**
Exchange	$2^{88.2}$	Encs.	$2^{88.2}$	CP	[BR19c, BR19b]
Exchange	2^{83}	Encs.	2^{83}	ACC	[Bar19]

MAs = memory accesses; CP = chosen plaintexts; (A)CC = (adaptive) chosen ciphertexts; ID = impossible differential; TD = truncated differential; MD = mixture differential

`https://github.com/medsec/expectation-cryptanalysis-on-round-reduced-aes`

- 6-round AES
- Implemented with Small-AES

#Rds.	Attack type	Time (Enc.)	Data (CP)	P_S	Ref.
6	Impossible Differential	$2^{122.0}$	$2^{91.5}$	≈ 1	[CKK+01]
6	MitM	$2^{106.2}$	2^{8}	≈ 1	[DFJ13]
6	Prob. Mixture-differential	$2^{105.0}$	$2^{72.8}$	≥ 0.95	[Gra17, Gra19]
6	Mixture-differential	$2^{81.0}$	$2^{27.5}$	0.632	[BDK+18]
6	**Truncated differential**	$\mathbf{2^{78.7}}$	$\mathbf{2^{71.3}}$	0.632	**[This work]**
6	Integral	$2^{51.7}$	2^{35}	≈ 1	[Tod14, TA14]
6	Partial Sum	$2^{42.0}$	2^{32}	≈ 1	[Tun12a, Tun12b]
7	Impossible Differential	$2^{106.88}$	2^{105}	≈ 1	[BLNS18]
7	MitM	$2^{99.0}$	2^{97}	≈ 1	[DFJ13]

Conclusion

- Small-bias distinguishers are highly useful
  Good paper prior to ours: [GR19]
- Interesting: S-box and index dependencies
- Claim: The more uniform the S-box, the lower deviations from theory [GR19]
  Reason still unclear, but indications
- Large deviations mostly due to the small size of Small-AES

Questions?

Bibliography I

Navid Ghaedi Bardeh.
A Key-Independent Distinguisher for 6-round AES in an Adaptive Setting.
IACR Cryptology ePrint Archive, 2019:945, 2019.
http://eprint.iacr.org/2019/945.

Christina Boura, Anne Canteaut, and Daniel Coggia.
A general proof framework for recent AES distinguishers.
IACR Trans. Symmetric Cryptol., 2019(1):170–191, 2019.

Achiya Bar-On, Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir.
Improved Key Recovery Attacks on Reduced-Round AES with Practical Data and Memory Complexities.
In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO II*, volume 10992 of *Lecture Notes in Computer Science*, pages 185–212. Springer, 2018.

Mihir Bellare and Russell Impagliazzo.
A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion.
IACR Cryptology ePrint Archive, 1999:24, 1999.

Christina Boura, Virginie Lallemand, María Naya-Plasencia, and Valentin Suder.
Making the Impossible Possible.
J. Cryptology, 31(1):101–133, 2018.
https://doi.org/10.1007/s00145-016-9251-7.

Srimanta Bhattacharya and Mridul Nandi.
A note on the chi-square method: A tool for proving cryptographic security.
Cryptography and Communications, 10(5):935–957, 2018.

Srimanta Bhattacharya and Mridul Nandi.
Full Indifferentiable Security of the Xor of Two or More Random Permutations Using the \chi ^2 Method.
In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT I*, volume 10820 of *Lecture Notes in Computer Science*, pages 387–412. Springer, 2018.

Bibliography II

Navid Ghaedi Bardeh and Sondre Rønjom.
Practical Attacks on Reduced-Round AES.
In Johannes Buchmann, Abderrahmane Nitaj, and Tajje-eddine Rachidi, editors, *Africacrypt*, volume 11627 of *LNCS*, pages 297–310. Springer, 2019.
https://doi.org/10.1007/978-3-030-23696-0_15.

Navid Ghaedi Bardeh and Sondre Rønjom.
The Exchange Attack: How to Distinguish 6 Rounds of AES with $2^{88.2}$ chosen plaintexts.
In Mitsuru Matsui, Steven Galbraith, and Shiho Moriai, editors, *ASIACRYPT*, volume 11273 of *LNCS*. Springer, 2019.
To appear.

Navid Ghaedi Bardeh and Sondre Rønjom.
The Exchange Attack: How to Distinguish 6 Rounds of AES with $2^{88.2}$ chosen plaintexts.
IACR Cryptology ePrint Archive, 2019:652, 2019.
https://eprint.iacr.org/2019/652.

Jung Hee Cheon, MunJu Kim, Kwangjo Kim, Jung-Yeun Lee, and SungWoo Kang.
Improved Impossible Differential Cryptanalysis of Rijndael and Crypton.
In Kwangjo Kim, editor, *ICISC*, volume 2288 of *LNCS*, pages 39–49. Springer, 2001.
https://doi.org/10.1007/3-540-45861-1_4.

Benoit Cogliati, Rodolphe Lampe, and Jacques Patarin.
The Indistinguishability of the XOR of k Permutations.
In Carlos Cid and Christian Rechberger, editors, *FSE*, volume 8540 of *LNCS*, pages 285–302. Springer, 2014.

Jiageng Chen, Atsuko Miyaji, Chunhua Su, and Liang Zhao.
A New Statistical Approach for Integral Attack.
In Meikang Qiu, Shouhuai Xu, Moti Yung, and Haibo Zhang, editors, *NSS*, volume 9408 of *Lecture Notes in Computer Science*, pages 345–356. Springer, 2015.

Bibliography III

Patrick Derbez, Pierre-Alain Fouque, and Jérémy Jean.
Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting.
In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT*, volume 7881 of *Lecture Notes in Computer Science*, pages 371–387. Springer, 2013.

Wei Dai, Viet Tung Hoang, and Stefano Tessaro.
Information-Theoretic Indistinguishability via the Chi-Squared Method.
In Jonathan Katz and Hovav Shacham, editors, *CRYPTO Part III*, volume 10403 of *LNCS*, pages 497–523. Springer, 2017.
Full version at http://eprint.iacr.org/2017/537, latest version 20170616:190106.

Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir.
The Retracing Boomerang Attack.
In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT I*, volume 12105 of *LNCS*, pages 280–309. Springer, 2020.
https://doi.org/10.1007/978-3-030-45721-1_11.

Lorenzo Grassi and Christian Rechberger.
New Rigorous Analysis of Truncated Differentials for 5-round AES.
IACR Cryptology ePrint Archive, 2018:182, 2018.

Lorenzo Grassi and Christian Rechberger.
Rigorous Analysis of Truncated Differentials for 5-round AES.
IACR Cryptology ePrint Archive, 2018:182, April 06 2019.
http://eprint.iacr.org/2018/182, updated version 20190604:090617.

Lorenzo Grassi.
Mixture Differential Cryptanalysis: a New Approach to Distinguishers and Attacks on round-reduced AES.
IACR Cryptology ePrint Archive, 2017:832, 2017.

Bibliography IV

Lorenzo Grassi.
MixColumns Properties and Attacks on (Round-Reduced) AES with a Single Secret S-Box.
In Nigel P. Smart, editor, *CT-RSA*, volume 10808 of *Lecture Notes in Computer Science*, pages 243–263. Springer, 2018.

Lorenzo Grassi.
Mixture Differential Cryptanalysis: a New Approach to Distinguishers and Attacks on round-reduced AES.
IACR Transactions on Symmetric Cryptology, 2018(2):133–160, 2018.

Lorenzo Grassi.
Probabilistic Mixture Differential Cryptanalysis on round-reduced AES.
In Douglas Stebila and Kenneth G. Paterson, editors, *SAC*, LNCS. Springer, 2019.
22 pages (to appear).

Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom.
Subspace Trail Cryptanalysis and its Applications to AES.
IACR Trans. Symmetric Cryptol., 2016(2):192–225, 2016.

Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom.
A New Structural-Differential Property of 5-Round AES.
In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT II*, volume 10211 of *Lecture Notes in Computer Science*, pages 289–317, 2017.

Kai Hu, Tingting Cui, Chao Gao, and Meiqin Wang.
Towards Key-Dependent Integral and Impossible Differential Distinguishers on 5-Round AES.
In Carlos Cid and Michael J. Jacobson Jr., editors, *SAC*, volume 11349 of *Lecture Notes in Computer Science*, pages 139–162. Springer, 2018.

Stefan Lucks.
The Sum of PRPs Is a Secure PRF.
In Bart Preneel, editor, *EUROCRYPT*, volume 1807 of *LNCS*, pages 470–484. Springer, 2000.

Bibliography V

Bart Mennink and Samuel Neves.
Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory.
In Jonathan Katz and Hovav Shacham, editors, *CRYPTO, Part III*, volume 10403 of *LNCS*, pages 556–583. Springer, 2017.
Full version at https://eprint.iacr.org/2017/473.

Bart Mennink and Bart Preneel.
On the XOR of Multiple Random Permutations.
In Tal Malkin, Vladimir Kolesnikov, Allison Bishop Lewko, and Michalis Polychronakis, editors, *ACNS*, volume 9092 of *LNCS*, pages 619–634. Springer, 2015.

Jacques Patarin.
A Proof of Security in O(2n) for the Xor of Two Random Permutations.
In Reihaneh Safavi-Naini, editor, *ICITS*, volume 5155 of *LNCS*, pages 232–248. Springer, 2008.
Full version at https://eprint.iacr.org/2008/010.

Jacques Patarin.
Generic Attacks for the Xor of k random permutations.
IACR Cryptology ePrint Archive, 2008:9, 2008.

Jacques Patarin.
Introduction to Mirror Theory: Analysis of Systems of Linear Equalities and Linear Non Equalities for Cryptography.
IACR Cryptology ePrint Archive, 2010:287, 2010.

Jacques Patarin.
Generic Attacks for the Xor of k Random Permutations.
In Michael J. Jacobson Jr., Michael E. Locasto, Payman Mohassel, and Reihaneh Safavi-Naini, editors, *ACNS*, volume 7954 of *Lecture Notes in Computer Science*, pages 154–169. Springer, 2013.

Bibliography VI

Sondre Rønjom, Navid Ghaedi Bardeh, and Tor Helleseth.
Yoyo Tricks with AES.
In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT I*, volume 10624 of *Lecture Notes in Computer Science*, pages 217–243. Springer, 2017.

Sondre Rønjom.
A Short Note on a Weight Probability Distribution Related to SPNs.
IACR Cryptology ePrint Archive, 2019:750, 2019.

Ali Aydin Selçuk.
On Probability of Success in Linear and Differential Cryptanalysis.
J. Cryptology, 21(1):131–147, 2008.
http://dx.doi.org/10.1007/s00145-007-9013-7.

Bing Sun, Meicheng Liu, Jian Guo, Longjiang Qu, and Vincent Rijmen.
New Insights on AES-Like SPN Ciphers.
In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO I*, volume 9814 of *Lecture Notes in Computer Science*, pages 605–624. Springer, 2016.

Subhabrata Samajder and Palash Sarkar.
Rigorous upper bounds on data complexities of block cipher cryptanalysis.
J. Mathematical Cryptology, 11(3):147–175, 2017.
https://doi.org/10.1515/jmc-2016-0026.

Yosuke Todo and Kazumaro Aoki.
FFT Key Recovery for Integral Attack.
In Dimitris Gritzalis, Aggelos Kiayias, and Ioannis G. Askoxylakis, editors, *CANS*, volume 8813 of *LNCS*, pages 64–81. Springer, 2014.
https://doi.org/10.1007/978-3-319-12280-9_5.

Bibliography VII

Yosuke Todo.
FFT-Based Key Recovery for the Integral Attack.
IACR Cryptology ePrint Archive, 2014:187, 2014.
http://eprint.iacr.org/2014/187.

Michael Tunstall.
Improved Partial Sums-based Square Attack on AES.
In Pierangela Samarati, Wenjing Lou, and Jianying Zhou, editors, *SECRYPT*, pages 25–34. SciTePress, 2012.

Michael Tunstall.
Improved "Partial Sums"-based Square Attack on AES.
IACR Cryptology ePrint Archive, 2012:280, 2012.
http://eprint.iacr.org/2012/280.

Yale.
The Yale Literary Magazine.
Number 47 in The Yale Literary Magazine. Herrick & Noyes, 1882.

Section 7

Supporting Slides

More Precision: Dependencies

"In theory, there is no difference between theory and practice. But, in practice, there is."

Benjamin Brewster [Yal82, p.202]

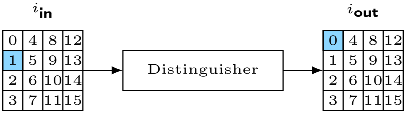
We analyzed

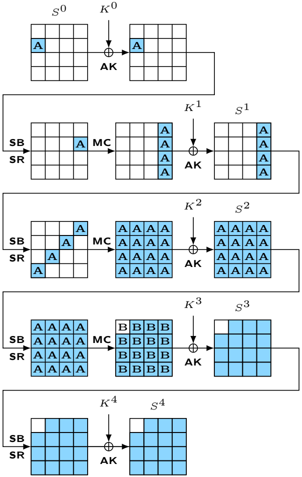
- Index dependencies of active input cells and concerned output cells
- Effects of the S-box

Index Dependencies: Model

How do different combinations of input (i_{in}) and output (i_{out}) indices behave?

- Active cell in $S^0[i_{\text{in}}]$
- Collision search in $S^4[i_{\text{out}}]$ (no final MC)
- Compare in terms of $|p_{\text{Small-AES}} - p_{\text{rand}}|$





Index Dependencies: Theory

- Equation system
- Four terms per output cell:

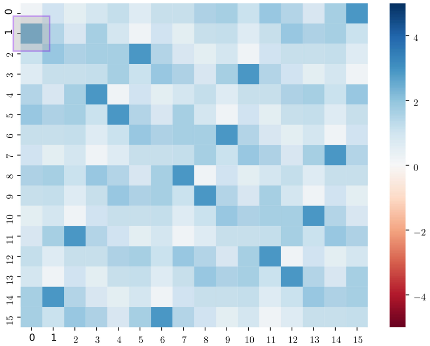
For example, for $(i_{\mathsf{in}}, i_{\mathsf{out}}) = (0, 0)$:

$$\begin{aligned} & \mathbf{2}S\big(\mathbf{2}S(\mathbf{2}x_i \oplus K^1[0]) \oplus K^2[0]\big) \oplus \mathbf{3}S\big(S(\mathbf{3}x_i \oplus K^1[1]) \oplus K^2[5]\big) \\ & \oplus S\big(\mathbf{2}S(x_i \oplus K^1[2]) \oplus K^2[10]\big) \oplus S\big(S(x_i \oplus K^1[3]) \oplus K^2[15]\big) \\ = & \mathbf{2}S\big(\mathbf{2}S(\mathbf{2}x_j \oplus K^1[0]) \oplus K^2[0]\big) \oplus \mathbf{3}S\big(S(\mathbf{3}x_j \oplus K^1[1]) \oplus K^2[5]\big) \\ & \oplus S\big(\mathbf{2}S(x_j \oplus K^1[2]) \oplus K^2[10]\big) \oplus S\big(S(x_j \oplus K^1[3]) \oplus K^2[15]\big) \end{aligned}$$

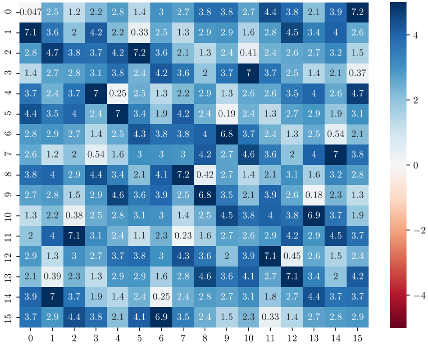
for $i \neq j$. For different in- or output positions, the equations differ naturally.

Index Dependencies: Experimental Results on Small-AES

- In multiples of $|p_{\text{Small-AES}} - p_{\text{rand}}|$
- $0.0 =$ no distinguisher
- $1.0 =$ distinguisher as expected
- $> |\pm 1| =$ good distinguisher
- Range of $[0.. + 7]$: most combinations better than expected, but not $(i_{\text{in}}, i_{\text{out}}) = (0, 0)$



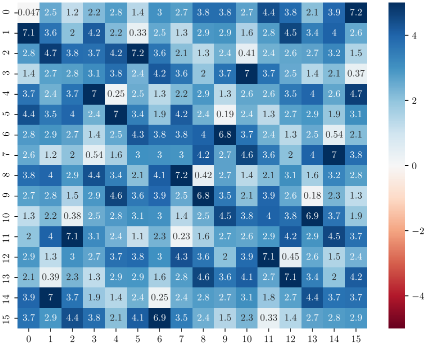
Theoretical for Small-AES



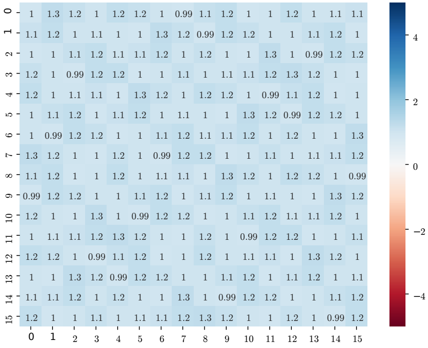
Experimental for Small-AES

Index Dependencies: Theoretical Results on The AES

- In multiples of $|p_{\text{AES}} - p_{\text{rand}}|$
- Range of $[0.99..1.35] \implies$ any $(i_{\text{in}}, i_{\text{out}})$ works well
- Potential interpretation: Small size and few rounds produce side effects



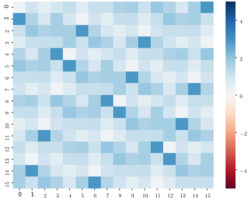
Experimental for Small-AES



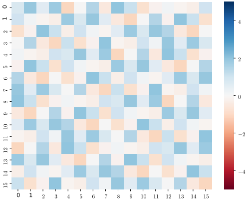
Theoretical for AES

S-box Dependencies

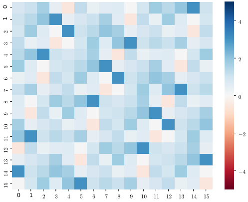
Small-AES



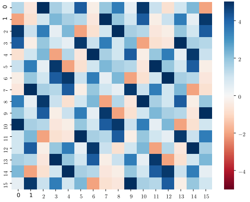
Original S-box



PRESENT S-box

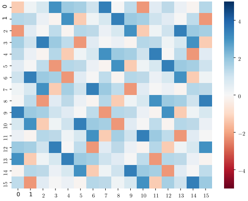


PRINCE S-box

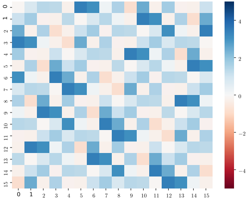


PRIDE S-box

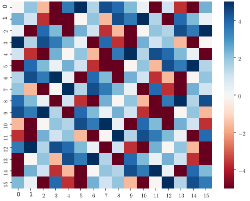
- Small-AES with alternative S-boxes
- Practical 4-bit S-boxes



Toy-6 S-box



Toy-8 S-box



Toy-10 S-box

Which S-box Properties Cause The Deviations?

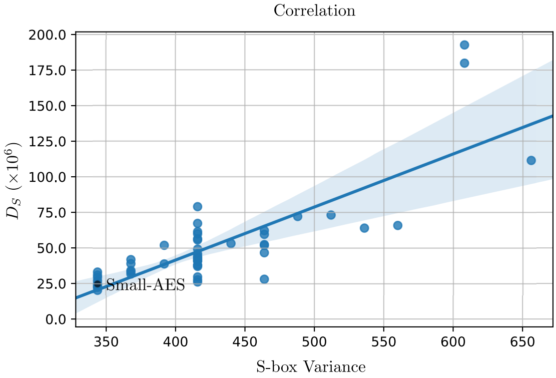
- Variance? (Already suspected by [GR19])
- D_S = distance to expected #collisions for input cell

$$D_S \stackrel{\text{def}}{=} \sqrt{\sum_{i_{\text{out}}=0}^{15} \left| \mathsf{X}^S_{i_{\text{out}}} - \mathbb{E}[\mathsf{X}] \right|^2}$$

- Pearson correlation of variance and D_S

$$\rho_{\mathsf{X},\mathsf{Y}} \stackrel{\text{def}}{=} \frac{\text{cov}(\mathsf{X},\mathsf{Y})}{\sigma_{\mathsf{X}} \cdot \sigma_{\mathsf{Y}}},$$

- $(r, p) \simeq (0.812, 1.637 \cdot 10^{-13})$ high correlation, low error probability
- But not full story...



$\text{cov}(\mathsf{X},\mathsf{Y}) =^{\text{def}} \mathbb{E}[(\mathsf{X} - \mu_{\mathsf{X}}) \cdot (\mathsf{Y} - \mu_{\mathsf{Y}})]$ is the covariance of X and Y.