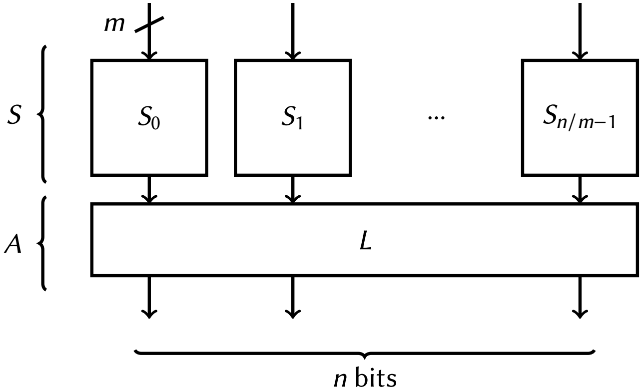
Multiset-Algebraic Cryptanalysis of Reduced Kuznyechik, Khazad, and secret SPNs

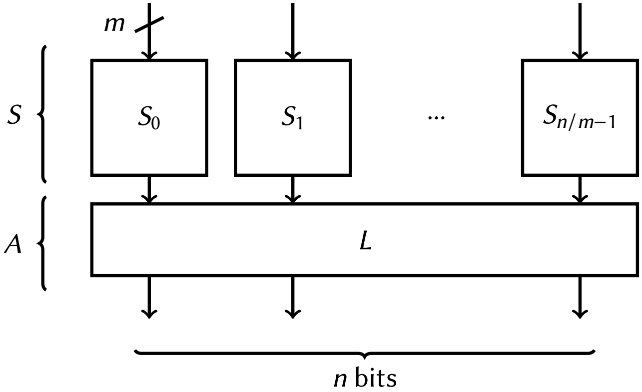
Alex Biryukov[1,2], Dmitry Khovratovich[2], Léo Perrin[2]

[1]CSC, University of Luxembourg
[2]SnT, University of Luxembourg

https://www.cryptolux.org

March 6, 2017
Fast Software Encryption 2017


m
S
A
S_0
S_1
...
$S_{n/m-1}$
L
n bits



How many layers can we attack?

Generic Attacks Against SPNs

... but why?

Generic Attacks Against SPNs

... but why?

- For attacking actual block ciphers

Generic Attacks Against SPNs

... but why?

- For attacking actual block ciphers
- For attacking White-box schemes
  - ASASA
  - AES white-box implementations
  - SPNbox

Generic Attacks Against SPNs

... but why?

- For attacking actual block ciphers
- For attacking White-box schemes
  - ASASA
  - AES white-box implementations
  - SPNbox
- For decomposing S-Boxes

Outline

Plan

Core Lemma

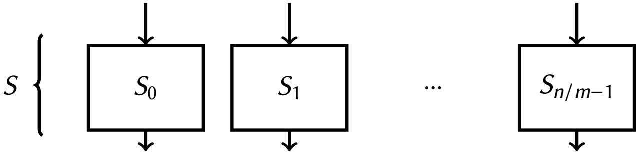
Lemma

If $F : \{0,1\}^n \rightarrow \{0,1\}^m$ has degree d, then

$$\bigoplus_{x \in C} F(x) = 0$$

for all *cube* $C = \{a + v, \forall v \in \mathcal{V}\}$, where $\mathcal{V}$ is a vector space of size $\geq 2^{d+1}$.

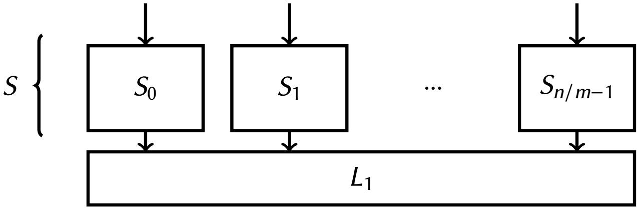
Distinguisher for S-layer



For all cube C of size $\geq 2^m$:

$$\bigoplus_{x \in C} S(x) = 0.$$

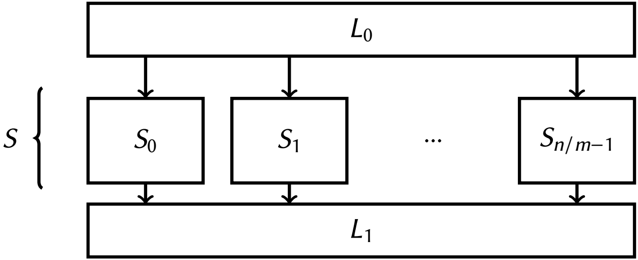
Distinguisher for S-layer



For all cube C of size $\geq 2^m$:

$$\bigoplus_{x \in C} SA(x) = 0.$$

Distinguisher for S-layer



For all cube C of size $\geq 2^m$:

$$\bigoplus_{x \in C} ASA(x) = 0.$$

Free S-Layer Trick

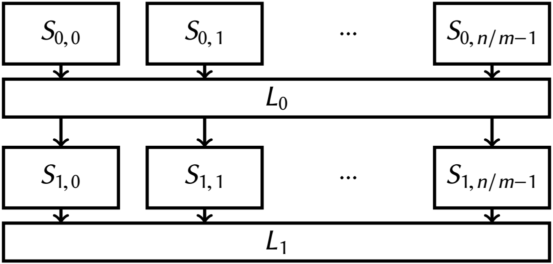
Observation

If $\mathcal{V}$ consists in the input bits of some S-Boxes, then $S(\mathcal{V}) = \mathcal{V}$.
Cubes based on $\mathcal{V}$ simply change their offsets.

Free S-Layer Trick

Observation

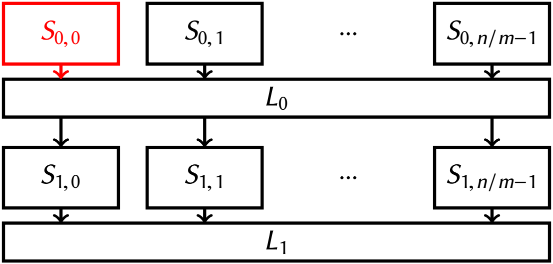
If $\mathcal{V}$ consists in the input bits of some S-Boxes, then $S(\mathcal{V}) = \mathcal{V}$.
Cubes based on $\mathcal{V}$ simply change their offsets.



Free S-Layer Trick

Observation

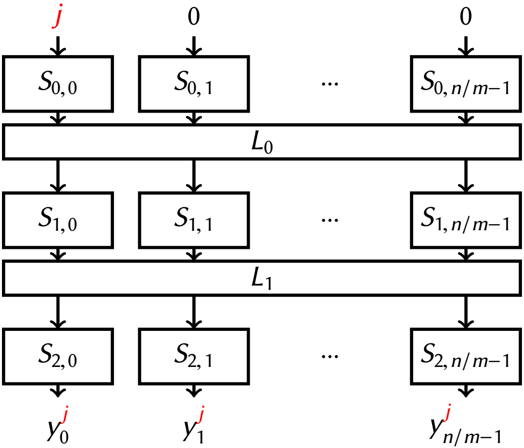
If $\mathcal{V}$ consists in the input bits of some S-Boxes, then $S(\mathcal{V}) = \mathcal{V}$.
Cubes based on $\mathcal{V}$ simply change their offsets.



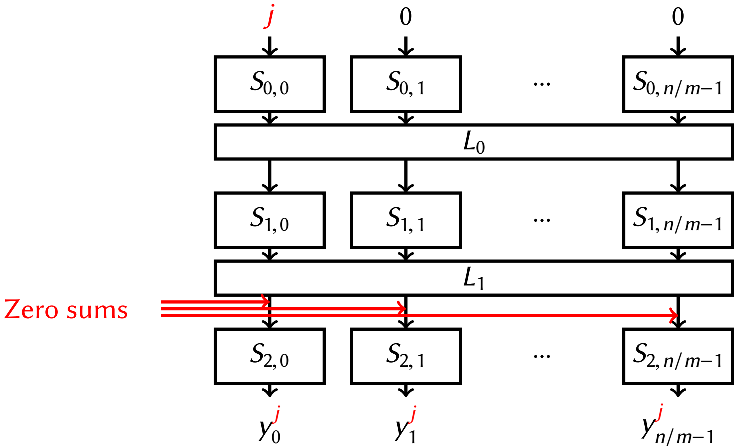
For **the** cubes C_i of size $\geq 2^m$ corresponding to the inputs of S_i,

$$\bigoplus_{x \in C_i} SASA(x) = 0.$$

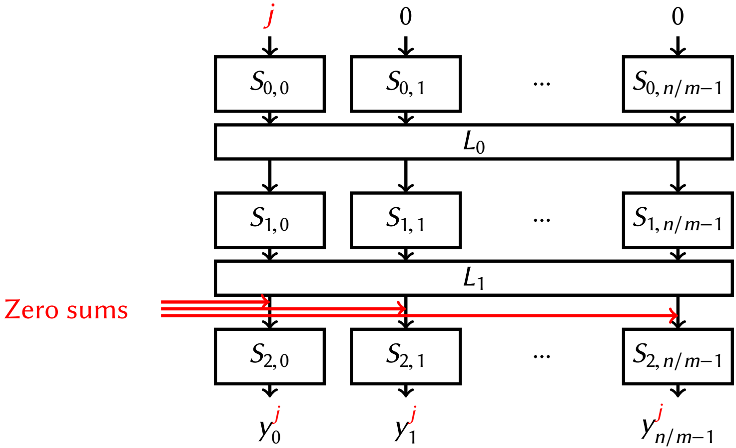
S-Box Recovery Against SASAS



S-Box Recovery Against SASAS

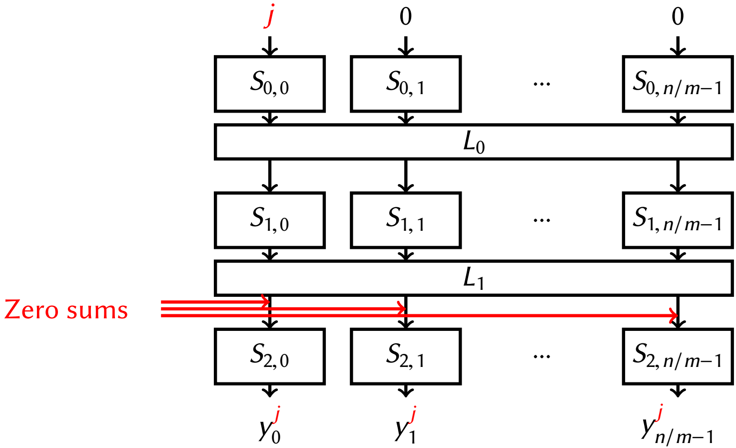


S-Box Recovery Against SASAS



$\bigoplus_{j=0}^{2^m-1} S_{2,i}(y_i^j) = 0,$ for all i.

S-Box Recovery Against SASAS



$\bigoplus_{j=0}^{2^m-1} S_{2,i}(y_i^j) = 0$, for all i. Repeat for different constant then solve system [Biryukov, Shamir, 2001]

Attack Against ASASA

Observation [Minaud et. al, 2015]

Consider S with two parallel S-Boxes S_0, S_1. The scalar product of...

- ... two outputs of S_0 has degree at most $m - 1$;
- ... one output of S_0 and one of S_1 has degree at most $2(m - 1)$

Attack Against ASASA

Observation [Minaud et. al, 2015]

Consider S with two parallel S-Boxes S_0, S_1. The scalar product of...

- ... two outputs of S_0 has degree at most $m-1$;
- ... one output of S_0 and one of S_1 has degree at most $2(m-1)$

For SASAS and ASASA, algebraic degree bound is crucial!

Plan

1. Introduction
2. Attacks Against 5 rounds
3. More Rounds!
   - Iterated Degree Bound
   - How Many Rounds?
   - Applications to Actual Block Ciphers
4. Division Property
5. Conclusion

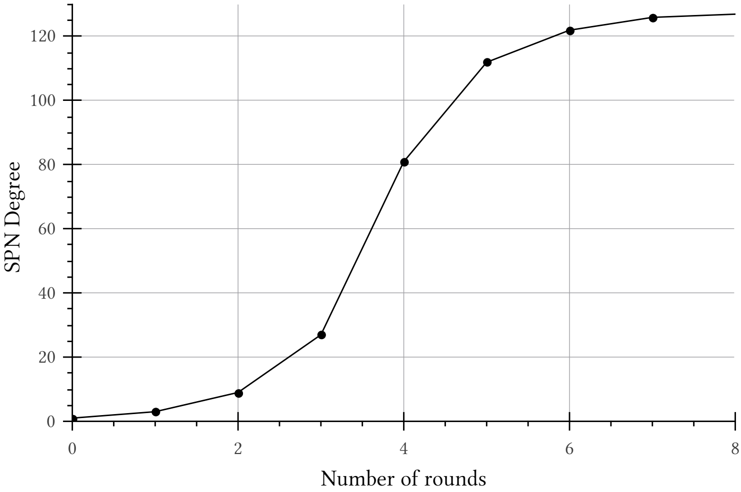
Degree Bound of Boura et al

Theorem ([Boura et al 2011])

Let P be an arbitrary function on $\mathbb{F}_2^n$. Let S be an S-Box layer of $\mathbb{F}_2^n$ corresponding to the parallel application of m-bit bijective S-Boxes of degree $m-1$. Then

$$\deg(P \circ S) \ \leq \ n - \left\lceil \frac{n - \deg(P)}{m-1} \right\rceil .$$

Example



$n = 128$; $m = 4$

How Many Rounds Can We Attack?

$$\ell = \log_{m-1}(n).$$

How Many Rounds Can We Attack?

$$\ell = \log_{m-1}(n).$$

Theorem (greatly simplified)

- *Basic Attack: if $r \leq 2\ell$ and $n/(m-1)^{\ell} > 1$ then*

$$\deg\left((AS)^{r}\right) \leq (n-2)$$

How Many Rounds Can We Attack?

$$\ell = \log_{m-1}(n).$$

Theorem (greatly simplified)

- *Basic Attack: if* $r \leq 2\ell$ *and* $n/(m-1)^{\ell} > 1$ *then*

$$\deg\left((AS)^{r}\right) \leq (n-2)$$

- *Free-S-layer Attack: if* $r \leq 2\ell$ *and* $n/(m-1)^{\ell} > 2$ *then*

$$\deg\left((AS)^{r}\right) \leq (n-m-1)$$

How Many Rounds Can We Attack?

$$\ell = \log_{m-1}(n).$$

Theorem (greatly simplified)

- *Basic Attack: if* $r \leq 2\ell$ *and* $n/(m-1)^{\ell} > 1$ *then*

$$\deg\left((AS)^{r}\right) \leq (n-2)$$

- *Free-S-layer Attack: if* $r \leq 2\ell$ *and* $n/(m-1)^{\ell} > 2$ *then*

$$\deg\left((AS)^{r}\right) \leq (n-m-1)$$

Other similar results depend on the base-$(m-1)$ *expansion of* n

What We Can Attack

m	n	"Key" size	ASASAS	SASASAS	ASASASAS	SASASASAS
4	12	270	2^{11}	-	-	-
	16	420	2^{11}	2^{15}	2^{15}	-
	24	1060	2^{11}	2^{15}	2^{15}	2^{24}
6	12	728	2^{12}	-	-	-
	18	1200	2^{17}	-	-	-
	24	1744	2^{21}	-	-	-
	36	3048	2^{28}	2^{36}	2^{36}	-
	120	2^{14}	2^{28}	2^{36}	2^{106}	2^{114}
8	128	2^{15}	2^{52}	2^{64}	2^{118}	2^{128}
	256	2^{17}	2^{52}	2^{64}	2^{230}	2^{240}

Kuznyechik

- Standardized in 2015 (GOST)
- 128-bit block ; 8-bit S-Box (remember π?)
- 9 rounds, 256-bit key

Kuznyechik

- Standardized in 2015 (GOST)
- 128-bit block ; 8-bit S-Box (remember π?)
- 9 rounds, 256-bit key
- MDS linear layer operating on 16 bytes

Kuznyechik

- Standardized in 2015 (GOST)
- 128-bit block ; 8-bit S-Box (remember π?)
- 9 rounds, 256-bit key
- MDS linear layer operating on 16 bytes

7-round Attack

We use that deg(4-r Kuzn.) $\leq$ 126. Add 1-round at the top, 2 at the bottom.

$$\text{Time} = 2^{154.5}, \ \text{Memory} = 2^{140}, \ \text{Data} = 2^{128}.$$

Khazad

- Published in 2000 (NESSIE candidate)
- 64-bit block ; 8-bit S-Box
- 8 rounds, 128-bit key

Khazad

- Published in 2000 (NESSIE candidate)
- 64-bit block ; 8-bit S-Box
- 8 rounds, 128-bit key

6-round Attack

We use that deg(3-r Khaz.) $\leq$ 62. Add 1-round at the top, 2 at the bottom.

$$\text{Time} = 2^{90},\ \text{Memory} = 2^{72},\ \text{Data} = 2^{64}.$$

Plan

Division Property

Definition (Division Property (simplified))

A multiset $\mathcal{X}$ on $\mathbb{F}_2^n$ has division property $\mathcal{D}_k^n$ if

$$\bigoplus_{x \in \mathcal{X}} x^u = 0$$

for all u in $\mathbb{F}_2^n$ such that $\text{hw}(u) < k$; where $x^u = \prod_{i=0}^{n-1} x_i^{u_i}$.

Example

- A cube of size 2^k has division property $\mathcal{D}_k^n$
- If a multiset with $\mathcal{D}_k^n$ is mapped to one with $\mathcal{D}_2^n$, it sums to 0.

Algebraic View

$$\mathbb{I}_{\mathcal{X}}(x) = 1 \text{ if and only if } x \in \mathcal{X}$$

Theorem

A multiset $\mathcal{X}$ has division property $\mathcal{D}_k^n$ if and only if

$$\deg(\mathbb{I}_{\mathcal{X}}) \leq n - k .$$

Algebraic View

$$\mathbb{I}_{\mathcal{X}}(x) = 1 \text{ if and only if } x \in \mathcal{X}$$

Theorem

A multiset $\mathcal{X}$ has division property $\mathcal{D}_k^n$ if and only if

$$\deg(\mathbb{I}_{\mathcal{X}}) \leq n - k .$$

Division Property and Algebraic Degree

The increase in the division property is the increase in the algebraic degree of the indicator function!

Plan

Conclusion

Secure ASASA-like cryptosystems:

Block	Layers	Structure	S-layer	BB mem.	WB mem.	Security
12 bits	7	$SASASAS$	2×(6 bits)	512 B	8 KB	64 bits
16 bits	7	$SASASAS$	2×(8 bits)	2 KB	132 KB	64 bits
24 bits	7	$SASASAS$	3×(8 bits)	3 KB	50 MB	128 bits
32 bits	7	$SASASAS$	4×(8 bits)	4 KB	18 GB	128 bits
64 bits	7	$SASASAS$	8×(8 bits)	8 KB	–	128 bits
128 bits	11	$S(AS)^5$	16×(8 bits)	24 KB	–	128 bits

Conclusion

Secure ASASA-like cryptosystems:

Block	Layers	Structure	S-layer	BB mem.	WB mem.	Security
12 bits	7	$SASASAS$	2×(6 bits)	512 B	8 KB	64 bits
16 bits	7	$SASASAS$	2×(8 bits)	2 KB	132 KB	64 bits
24 bits	7	$SASASAS$	3×(8 bits)	3 KB	50 MB	128 bits
32 bits	7	$SASASAS$	4×(8 bits)	4 KB	18 GB	128 bits
64 bits	7	$SASASAS$	8×(8 bits)	8 KB	–	128 bits
128 bits	11	$S(AS)^5$	16×(8 bits)	24 KB	–	128 bits

Thank you!