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
How many layers can we attack?

Biryukov, Khovratovich, Perrin

Multiset-Algebraic Cryptanalysis of Reduced Kuznyechik, Khazad, and secret SPNs
How many layers can we attack?
Introduction

Generic Attacks Against SPNs

... but why?
Introduction

Generic Attacks Against SPNs

... but why?

- For attacking actual block ciphers
Introduction

Generic Attacks Against SPNs

... but why?

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

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

1. Introduction
2. Attacks Against 5 rounds
3. More Rounds!
4. Division Property
5. Conclusion
Plan

1. Introduction

2. Attacks Against 5 rounds
   - Attack SASAS
   - Attack ASASA

3. More Rounds!

4. Division Property

5. Conclusion
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.

$$
\begin{align*}
S_{0,0} & \quad S_{0,1} & \quad \ldots & \quad S_{0,n/m-1} \\
& \downarrow & \quad & \downarrow \\
L_0 & \quad & \quad & \quad \\
S_{1,0} & \quad S_{1,1} & \quad \ldots & \quad S_{1,n/m-1} \\
& \downarrow & \quad & \downarrow \\
L_1 & \quad & \quad & \quad
\end{align*}
$$
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 $S_i$,

$$\bigoplus_{x \in C_i} \text{SASA}(x) = 0.$$
S-Box Recovery Against SASAS

\[ S_0,0 \to S_0,1 \to \ldots \to S_0,n/m-1 \]
\[ S_1,0 \to S_1,1 \to \ldots \to S_1,n/m-1 \]
\[ S_2,0 \to S_2,1 \to \ldots \to S_2,n/m-1 \]

\[ j \]

\[ 0 \]

\[ 0 \]

\[ y_0^j \]

\[ y_1^j \]

\[ y_{n/m-1}^j \]
S-Box Recovery Against SASAS

Zero sums

\[ j \]

\[ H_0 \]

\[ S_{0,0} \]

\[ S_{0,1} \]

\[ \ldots \]

\[ S_{0,n/m-1} \]

\[ L_0 \]

\[ H_1 \]

\[ S_{1,0} \]

\[ S_{1,1} \]

\[ \ldots \]

\[ S_{1,n/m-1} \]

\[ L_1 \]

\[ S_{2,0} \]

\[ S_{2,1} \]

\[ \ldots \]

\[ S_{2,n/m-1} \]

\[ y_0^j \]

\[ y_1^j \]

\[ y_{n/m-1}^j \]
S-Box Recovery Against SASAS

\[ \bigoplus_{j=0}^{2^{m-1}} S_{2,j}(y_i^j) = 0, \text{ for all } i. \]
S-Box Recovery Against SASAS

\[ \bigoplus_{j=0}^{2^{m-1}} S_{2,i}(y^j_i) = 0, \text{ for all } i. \text{ Repeat for different constant then solve system } \text{[Biryukov, Shamir, 2001]} \]
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 $2(m - 1)$
Assuming property of more rounds!

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

\[ n = 128 ; \quad m = 4 \]
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
  \[ \deg ((AS)^r) \leq (n - 2) \]
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
  \[ \deg ((AS)^r) \leq (n - 2) \]

- **Free-S-layer Attack**: if \( r \leq 2\ell \) and \( n/(m - 1)^\ell > 2 \) then
  \[ \deg ((AS)^r) \leq (n - m - 1) \]
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
  \[ \deg((AS)^r) \leq (n - 2) \]

- **Free-S-layer Attack**: if \( r \leq 2\ell \) and \( n/(m - 1)^\ell > 2 \) then
  \[ \deg((AS)^r) \leq (n - m - 1) \]

*Other similar results depend on the base-\((m - 1)\) expansion of \( n \)*
What We Can Attack

<table>
<thead>
<tr>
<th>$m$</th>
<th>$n$</th>
<th>“Key” size</th>
<th>$2^{11}$</th>
<th>$2^{15}$</th>
<th>$2^{15}$</th>
<th>$2^{24}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>12</td>
<td>270</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>420</td>
<td>$2^{11}$</td>
<td>$2^{15}$</td>
<td>$2^{15}$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>1060</td>
<td>$2^{11}$</td>
<td>$2^{15}$</td>
<td>$2^{15}$</td>
<td>$2^{24}$</td>
</tr>
<tr>
<td>6</td>
<td>12</td>
<td>728</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>18</td>
<td>1200</td>
<td>$2^{12}$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>1744</td>
<td>$2^{21}$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>36</td>
<td>3048</td>
<td>$2^{28}$</td>
<td>$2^{36}$</td>
<td>$2^{36}$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>120</td>
<td>$2^{14}$</td>
<td>$2^{28}$</td>
<td>$2^{36}$</td>
<td>$2^{106}$</td>
<td>$2^{114}$</td>
</tr>
<tr>
<td>8</td>
<td>128</td>
<td>$2^{15}$</td>
<td>$2^{52}$</td>
<td>$2^{64}$</td>
<td>$2^{118}$</td>
<td>$2^{128}$</td>
</tr>
<tr>
<td></td>
<td>256</td>
<td>$2^{17}$</td>
<td>$2^{52}$</td>
<td>$2^{64}$</td>
<td>$2^{230}$</td>
<td>$2^{240}$</td>
</tr>
</tbody>
</table>
Kuznyechik

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

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

7-round Attack

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

Time = $2^{154.5}$, Memory = $2^{140}$, 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 $\deg(3\text{-}r \text{ Khaz.}) \leq 62$. Add 1-round at the top, 2 at the bottom.

\[
\text{Time} = 2^{90}, \quad \text{Memory} = 2^{72}, \quad \text{Data} = 2^{64}.
\]
Plan

1. Introduction
2. Attacks Against 5 rounds
3. More Rounds!
4. Division Property
5. Conclusion
Definition (Division Property (simplified))

A multiset $\mathcal{X}$ on $\mathbb{F}_2^n$ has division property $\mathcal{D}^n_k$ 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 $\mathcal{D}^n_k$.
- If a multiset with $\mathcal{D}^n_k$ is mapped to one with $\mathcal{D}^n_2$, it sums to 0.
Algebraic View

\[ \mathbb{1}_X(x) = 1 \text{ if and only if } x \in X \]

**Theorem**

A multiset \( X \) has division property \( D^\chi_k \) if and only if

\[ \deg(\mathbb{1}_X) \leq n - k. \]
Algebraic View

\[ \mathbb{1}_X(x) = 1 \text{ if and only if } x \in X \]

**Theorem**

A multiset \( X \) has division property \( D^n_k \) if and only if

\[ \deg(\mathbb{1}_X) \leq n - k . \]

**Division Property and Algebraic Degree**

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

1. Introduction
2. Attacks Against 5 rounds
3. More Rounds!
4. Division Property
5. Conclusion
## Conclusion

Secure ASASA-like cryptosystems:

<table>
<thead>
<tr>
<th>Block</th>
<th>Layers</th>
<th>Structure</th>
<th>S-layer</th>
<th>BB mem.</th>
<th>WB mem.</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>12 bits</td>
<td>7</td>
<td>SASASAS</td>
<td>2×(6 bits)</td>
<td>512 B</td>
<td>8 KB</td>
<td>64 bits</td>
</tr>
<tr>
<td>16 bits</td>
<td>7</td>
<td>SASASAS</td>
<td>2×(8 bits)</td>
<td>2 KB</td>
<td>132 KB</td>
<td>64 bits</td>
</tr>
<tr>
<td>24 bits</td>
<td>7</td>
<td>SASASAS</td>
<td>3×(8 bits)</td>
<td>3 KB</td>
<td>50 MB</td>
<td>128 bits</td>
</tr>
<tr>
<td>32 bits</td>
<td>7</td>
<td>SASASAS</td>
<td>4×(8 bits)</td>
<td>4 KB</td>
<td>18 GB</td>
<td>128 bits</td>
</tr>
<tr>
<td>64 bits</td>
<td>7</td>
<td>SASASAS</td>
<td>8×(8 bits)</td>
<td>8 KB</td>
<td>–</td>
<td>128 bits</td>
</tr>
<tr>
<td>128 bits</td>
<td>11</td>
<td>$S(AS)^5$</td>
<td>16×(8 bits)</td>
<td>24 KB</td>
<td>–</td>
<td>128 bits</td>
</tr>
</tbody>
</table>
**Conclusion**

Secure ASASA-like cryptosystems:

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

Thank you!