Proving the Security of AES Substitution-Permutation Network

T. Baignères  S. Vaudenay

SAC 2005
Outline

1. On the need to consider multipath characteristics
2. AES*: A Luby-Rackoff-like approach for the SPN of AES
3. Simplifying the LP computation for AES*
4. Towards the True Random Cipher
5. Further Results
What does Cryptanalysis mean?

- Breaking a cryptographic algorithm? **Not only!**
- Proving the security of a construction/algorithm

As breaking $\neq$ proving security

$\Downarrow$

different techniques must be applied.

$\rightsquigarrow$ **An example: Linear Cryptanalysis**
Example: Linear Cryptanalysis (LC)

Efficency of LC on a cipher $C$ is measured by the Linear Probability: $LP^C(a, b) = (2 \Pr_X [a \cdot X = b \cdot C(X)] - 1)^2$
Computing the **exact** LP of a SPN is usually not practical.

\[ \Delta \to \text{concatenate round-LP's and apply the Piling-up Lemma} \]

\[ \text{LP}^3 \text{ rounds} \left( c_0, c_3 \right) \approx \prod_{i=1,2,3} \text{LP}^{\text{Round}_i} \left( c_{i-1}, c_i \right) \]
Example: Linear Cryptanalysis (LC)

Following [Nyberg94], the approximation corresponds to considering only one characteristic among a linear hull.

\[
LP^3\text{ rounds} (c_0, c_3) = \sum_{c_1, c_2} \prod_{i=1,2,3} LP^{\text{Round}_i} (c_{i-1}, c_i)
\]
Example: Linear Cryptanalysis (LC)

How accurate is the approximation?

- It is ok when one characteristic is overwhelming (ex: DES)
- It is ok when it leads to an efficient attack
- This is not always the case (ex: AES)

It actually underestimates the LP!

\[ \leadsto \text{an attack can only work better than expected...} \]
\[ \leadsto \ldots \text{a security proof becomes meaningless} \]
Example: Linear Cryptanalysis (LC)

Conclusion

For security proofs, the LP cannot be approximated by the LP of one characteristic. Linear hull must be taken into account.

For AES, two (rigorous) alternatives have been studied:

- **Upperbound** the LP (e.g., [Keliher-Meijer-Tavares01], [Park-Sung-Chee-Yoon-Lim02], and [Keliher04])
- **Adopt a Luby-Rackoff-like approach** (e.g., [Moriai-Vaudenay00] and [Keliher-Meijer-Tavares03])
A Luby-Rackoff-like approach in a SPN

- $S^*$ is a **random** permutation, uniformly distributed
- all random S-boxes are **independent** from each-other
- the subkey addition is included in $S^*$
On the need to consider multipath characteristics

AES*: A Luby-Rackoff-like approach for the SPN of AES

Simplifying the LP computation for AES*

Towards the True Random Cipher

Further Results

AES vs. AES*

One round of AES (Round)

```
[2 3 1 1]
[1 2 3 1]
[1 1 2 3]
[3 1 1 2]
```

AddRoundKey

One round of AES* (Round*)

```
[2 3 1 1]
[1 2 3 1]
[1 1 2 3]
[3 1 1 2]
```

AddRoundKey

T. Baignères, S. Vaudenay

Proving the Security of AES Substitution-Permutation Network
Results on AES*

- AES* is made of all identical rounds, except for the last one which excludes both linear transformations.
- The LP on AES* is taken on average over all the random S-boxes.

Summary of our results:

- AES* is protected against linear and differential cryptanalysis after 4 inner rounds.
- AES* is protected against iterated attacks of order one after 10 inner rounds.
- $\text{LP}^{AES*}$ tends towards the LP of the perfect cipher as the number of rounds increases.
On the Complexity of the Exact LP Computation

Given input/output masks $c_0$ and $c_r$, 

$$\text{LP}^{\text{AES}^*}(c_0, c_r) = \sum_{c_1, \ldots, c_{r-1}} \prod_{i=1, \ldots, r} \text{LP}^{\text{Round}_i^*}(c_{i-1}, c_i)$$

Needs about $(2^{128})^3 \log r$ field operations $\leadsto$ Prohibitive!

First reduction: summing over intermediate supports instead of intermediate masks
Masks and Supports

The support of a mask $c$ is the $4 \times 4$ array $\gamma$ indicating which entries of $c$ are zero and which are not:

<table>
<thead>
<tr>
<th>Mask $c$</th>
<th>Support $\gamma$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x45 0x91 0xAB 0x00</td>
<td>1 1 1 0</td>
</tr>
<tr>
<td>0xF3 0x23 0x2C 0x37</td>
<td>1 1 1 1</td>
</tr>
<tr>
<td>0xFE 0x11 0x00 0xD1</td>
<td>1 1 0 1</td>
</tr>
<tr>
<td>0xB1 0x63 0x0A 0x00</td>
<td>1 1 1 0</td>
</tr>
</tbody>
</table>

Hamming weight of $\gamma$ is denoted $|\gamma|$ (in this example, $|\gamma| = 13$)

Supports are useful to compute the LP on one round of AES*...
Average LP on SubBytes$^*$

For any non-zero input/output masks $a, b$ on $S^*$

$$E_{S^*}[LP^{S^*}(a, b)] = \frac{1}{2^8 - 1} = \sigma^{-1}$$

Lemma

For any non-zero masks $a, b \in GF(2^8)^{16}$ of respective supports $\alpha$ and $\beta$

$$E[LP^{SubBytes^*}(a, b)] = \begin{cases} \sigma^{-|\alpha|} & \text{if } \alpha = \beta \\ 0 & \text{otherwise.} \end{cases}$$
LP on LT = \text{MixColumns} \circ \text{ShiftRows}

- LT denotes \text{MixColumns} \circ \text{ShiftRows}.
- For any state \( x \) and masks \( a, b \):
  \[
  a \bullet x = b \bullet (LT \times x) \quad \iff \quad a = LT^T \times b
  \]
  We say that \( a \) and \( b \) are connected through LT.
- \( N[\alpha, \beta] \) denotes the number of possible connections through LT, given the input/output supports \( \alpha \) and \( \beta \).
Theorem

For any non-zero masks $c_0, c_r \in GF(2^8)^{16}$ of respective supports $\gamma_0$ and $\gamma_r$

$$E[LP^{AES^*}(c_0, c_r)] = \sigma^{-|\gamma_r|} \times (M^{r-1})_{\gamma_0, \gamma_r}$$

where $M$ is a $2^{16} \times 2^{16}$ matrix indexed by pairs of masks $(\gamma_{i-1}, \gamma_i)$ such that

$$M_{\gamma_{i-1}, \gamma_i} = \sigma^{-(\gamma_{i-1})}N[\gamma_{i-1}, \gamma_i]$$

The computation roughly needs $(2^{16})^3 \log r$ field operations almost feasible!
In order to further reduce the complexity, we used properties inherent to any MDS matrix (not only the one in LT) which induce symmetries in the table N[·].

After some (frightening) computations...

...using rather (horrible) notations...
Final Expression for the LP

(Simplified) Theorem

For any non-zero masks $c_0, c_r \in GF(2^8)^{16}$ of respective supports $\gamma_0$ and $\gamma_r$

$$E[LP^{AES^*}(c_0, c_r)] = U^T \times L^{r-2} \times V$$

where

- $U$ only depends on the diagonal weights of $c_0$
- $V$ only depends on the column weights of $c_r$
- $L$ is a matrix $1001 \times 1001$ matrix

Computing all the LP for AES* can be done on a laptop.
Experimental Results

- Maximum value of $E[LP^{AES^*}(a, b)]$ for various number of rounds:

<table>
<thead>
<tr>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^{-33.9774}$</td>
<td>$2^{-55.9605}$</td>
<td>$2^{-127.9096}$</td>
<td>$2^{-127.9096}$</td>
<td>$2^{-127.9999}$</td>
<td>$2^{-127.9999}$</td>
<td>$2^{-128.0}$</td>
<td>$2^{-128.0}$</td>
</tr>
</tbody>
</table>

- Conclusion: AES$^*$ is protected against linear cryptanalysis after 4 rounds
- These results can be extended to differential cryptanalysis and to various S-box sizes
Properties of the matrix $\mathcal{M}$

In the previous Theorem

$$E[\text{LP}^{\text{AES}}(c_0, c_r)] = \sigma^{-|\gamma_r|} \times (\mathcal{M}^{r-1})_{\gamma_0, \gamma_r}$$

The $2^{16} \times 2^{16}$ matrix $\mathcal{M}$ actually looks like

$$
\begin{pmatrix}
1 & 0 \\
0 & \mathcal{M}'
\end{pmatrix}
$$

where $\mathcal{M}'$ is a $(2^{16} - 1) \times (2^{16} - 1)$ indexed by non-zero supports.
Properties of the matrix $\mathcal{M}'$

**Property**

$\mathcal{M}'$ is the transition matrix of a Markov chain, i.e., $\mathcal{M}_{\gamma,\gamma'}'$ is the transition probability from a non-zero support $\gamma$ to a non-zero support $\gamma'$.

From the study of supports propagation (based on the MDS criterion) $\leadsto$ the Markov chain is **irreducible** and **aperiodic**.

$\Rightarrow$ there exists a **stationary distribution** $\pi$, which can be determined. Then

$$ (\mathcal{M}'^r)_{\gamma,\gamma'} \xrightarrow{r \to \infty} \pi_{\gamma'} $$
Towards the LP of the True Random Cipher

Theorem

For any non-zero input/output masks $a, b,$

$$\lim_{r \to \infty} E[L^{AES^*}(a, b)] = \frac{1}{2^{128} - 1}$$
Iterated Attacks of Order 1

Consider an adversary $\mathcal{A}$ in the Luby-Rackoff model: unlimited computational power, limited access to an oracle $\mathcal{O}$ implementing either AES* or the perfect cipher $C^*$. $\mathcal{A}$ must guess which is the case.

$\mathcal{A}$ can adapt $x_2$ depending on $y_1$

$\sim\sim$ 2-limited adaptative distinguisher of advantage $\text{Adv}_{2\text{-limited}}$
Iterated Attacks of Order 1

- Iterated attacks of order 1 are similar to linear cryptanalysis, except that the bit of information is not necessarily derived in a linear way (and that can make a huge difference, see [Baignères-Junod-Vaudenay04])

- Resistance against 2-limited adaptative distinguishers is sufficient to resist iterated attacks of order 1 (result from Decorrelation theory)

(Simplified) Theorem

Let $\epsilon = \max_{a \neq 0, b} E[DP^{AES^*}(a, b)] - \frac{1}{2^{128}-1}$, then

$$\text{Adv}_{2\text{-limited}} \leq 2^{128} \epsilon$$
Iterated Attacks of Order 1: practical results

- Experimental values of $\epsilon$ depending on the number of rounds $r$:

<table>
<thead>
<tr>
<th>$r$</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$2^{-33.98}$</td>
</tr>
<tr>
<td>3</td>
<td>$2^{-55.96}$</td>
</tr>
<tr>
<td>4</td>
<td>$2^{-131.95}$</td>
</tr>
<tr>
<td>5</td>
<td>$2^{-131.95}$</td>
</tr>
<tr>
<td>6</td>
<td>$2^{-152.17}$</td>
</tr>
<tr>
<td>7</td>
<td>$2^{-174.74}$</td>
</tr>
<tr>
<td>8</td>
<td>$2^{-200.39}$</td>
</tr>
<tr>
<td>9</td>
<td>$2^{-223.93}$</td>
</tr>
<tr>
<td>10</td>
<td>$2^{-270.82}$</td>
</tr>
</tbody>
</table>

- Conclusion: provable security achieved for 10 rounds of AES*
Conclusion

- Study of the SPN of AES using a Luby-Rackoff-like approach $\rightsquigarrow$ AES*
- AES* is protected against linear and differential cryptanalysis after 4 inner rounds
- $LPAES^*$ tends towards the LP of the perfect cipher as the number of rounds increases
- AES* is protected against iterated attacks of order one after 10 inner rounds

Thank you for your attention!