RUHR-UNIVERSITÄT BOCHUM

The Uniqueness of (SPN-)Round Function Decompositions

Baptiste Lambin, Gregor Leander, Patrick Neumann

1 Uniqueness of Decompositions

2 Some Intuition

3 An Example: DEFAULT

4 Open Questions

1 Uniqueness of Decompositions

2 Some Intuition

3 An Example: DEFAULT

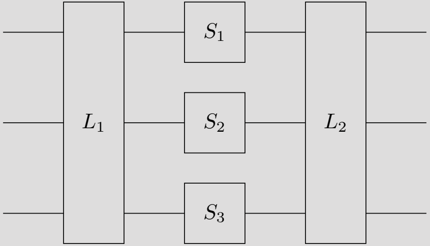
4 Open Questions

Motivation

- Most security analysis of symmetric primitives is based on their representation, not the primitive itself
- We should make sure that the result of our analysis is independent of the representation
- Here: Focus on round function
- One common design strategy: Substitution-Permutation Network (SPN)

(SPN-)Round Function Decomposition

- Given: A representation of an SPN round function



- Question: Is this representation unique?
- Up to reordering the S-boxes
- Up to linear equivalence of the S-boxes
- While maximizing the number of S-boxes

(SPN-)Round Function Decomposition – Why Two Linear Layers?

- Using two linear layers may seem strange
- More sensible to use just one for cipher design
- But: Can see additional linear layer as part of the next round
- Essentially looking at a linear equivalent cipher/primitive

$$\left(L_2 \circ \begin{pmatrix} S_1 \\ \vdots \\ S_n \end{pmatrix} \circ L_1 \right)^r = L_1^{-1} \circ \left(L_1 \cdot L_2 \circ \begin{pmatrix} S_1 \\ \vdots \\ S_n \end{pmatrix} \right)^r \circ L_1$$

- Both versions should have the same security properties
- Conclusion: More natural to allow two linear layers when decomposing

Maximal Differential Uniformity

Definition

A function F has maximal differential uniformity if $F(x) + F(x + \alpha)$ is constant for some non-zero α.

Lemma

F has maximal differential uniformity if and only if F is affine equivalent to a function of the form

$$G\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} f(x) \\ g(x) + y \end{pmatrix}.$$

Maximal Linearity

RUB

Definition

A function F has maximal linearity if $\alpha^{\mathrm{T}} \cdot \mathrm{F}$ is affine for some non-zero α.

Lemma

F has maximal linearity if and only if F is affine equivalent to a function of the form

$$\mathrm{H}\begin{pmatrix} \mathrm{x} \\ \mathrm{y} \end{pmatrix} = \begin{pmatrix} \mathrm{x} \\ \mathrm{h}\begin{pmatrix} \mathrm{x} \\ \mathrm{y} \end{pmatrix} \end{pmatrix}.$$

Uniqueness of Decompositions

Theorem

A (maximal) decomposition is not unique if and only if one S-box has maximal differential uniformity and another one has maximal linearity.

Corollary

Functions without unique (maximal) decomposition are exactly those affine equivalent to ones of the form

$$R\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} f(x_1) \\ g(x_1) + x_2 \\ x_3 \\ h\begin{pmatrix} x_3 \\ x_4 \end{pmatrix} \end{pmatrix} \begin{array}{l} \left.\vphantom{\begin{matrix} a \\ b \end{matrix}}\right\} \text{S-box(es)} \\ \left.\vphantom{\begin{matrix} a \\ b \\ c \end{matrix}}\right\} \text{S-box(es)} \end{array}.$$

1 Uniqueness of Decompositions

2 Some Intuition

3 An Example: DEFAULT

4 Open Questions

Uniqueness of Decompositions – Some Intuition

- Ideally, we would like to decompose iteratively
- Starting with one S-box (the whole round function), we would like to split one S-box into two, and iterate until no S-box can be decomposed anymore
- Problem: The choice of one S-box can affect other S-boxes

Uniqueness of Decompositions – Some Intuition

- Decompositions can be modeled using projections
  - If $V = U_1 \oplus U_2$ for a vector space V and subspaces U_1, U_2 this means that $v \in V$ can be written as $u_1 + u_2$ for unique $u_1 \in U_1$ and $u_2 \in U_2$
  - $\pi_i^U : V \to U_i,\ v \mapsto u_i$ are the projections onto those subspaces
- U_i is the input (before applying the first linear layer) to the i-th S-box
- Example: $U_1 = \mathbb{F}_2^{n/2} \times 0^{n/2}$, $U_2 = 0^{n/2} \times \mathbb{F}_2^{n/2}$ and $S_1, S_2 : \mathbb{F}_2^{n/2} \to \mathbb{F}_2^{n/2}$

$$\begin{aligned}\begin{pmatrix} S_1(x_1) \\ S_2(x_2) \end{pmatrix} + \begin{pmatrix} S_1(0) \\ S_2(0) \end{pmatrix} &= \begin{pmatrix} S_1(x_1) \\ S_2(0) \end{pmatrix} + \begin{pmatrix} S_1(0) \\ S_2(x_2) \end{pmatrix} \\ &= \begin{pmatrix} S_1 \\ S_2 \end{pmatrix} \circ \pi_1^U \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} S_1 \\ S_2 \end{pmatrix} \circ \pi_2^U \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\end{aligned}$$

- Decomposing an S-box is now equivalent to decomposing one of the subspaces U_i

Uniqueness of Decompositions – Some Intuition

- Using R from above
- One decomposition: $U_1 = \{(x_1, x_2, 0, 0)^T | x_1, x_2\}$ and $U_2 = \{(0, 0, x_3, x_4)^T | x_3, x_4\}$

$$R \circ \pi_1^U \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} f(x_1) \\ g(x_1) + x_2 \\ 0 \\ h(0) \end{pmatrix}, R \circ \pi_2^U \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} f(0) \\ g(0) \\ x_3 \\ h\begin{pmatrix} x_3 \\ x_4 \end{pmatrix} \end{pmatrix}$$

- Another decomposition: $W_1 = U_1$ and $W_2 = \{(0, x_3, x_3, x_4)^T | x_3, x_4\}$

$$R \circ \pi_1^W \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} f(x_1) \\ g(x_1) + x_2 + x_3 \\ 0 \\ h(0) \end{pmatrix}, R \circ \pi_2^W \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} f(0) \\ g(0) + x_3 \\ x_3 \\ h\begin{pmatrix} x_3 \\ x_4 \end{pmatrix} \end{pmatrix}$$

Uniqueness of Decompositions – Some Intuition

$$R\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} f(x_1) \\ g(x_1) + x_2 \\ x_3 \\ h\begin{pmatrix} x_3 \\ x_4 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} f(x_1) \\ g(x_1) + (x_2 + x_3) + x_3 \\ x_3 \\ h\begin{pmatrix} x_3 \\ x_4 \end{pmatrix} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} R \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

- R is self linear equivalent, where the linear equivalence mixes the S-boxes
- Matrices don't have to be identical in general

1 Uniqueness of Decompositions

2 Some Intuition

3 An Example: DEFAULT

4 Open Questions

An Example: DEFAULT

- DEFAULT[1] is an SPN block cipher aimed at fault attack resilience
- Two different round functions:
  - Inner part aimed at classical security
  - Outer part aimed at fault attack resilience
- S-box of outer part

$$S\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 + x_3 \\ (x_1 + x_4)(x_2 + x_3) + x_1 + x_2 \\ x_2 + x_3 + x_4 \\ (x_1 + x_4)(x_2 + x_3) + x_3 + x_4 \end{pmatrix}$$

- S-box has both, maximal differential uniformity and linearity
- With that, its round function representation is not unique!

[1] By Anubhab Baksi, Shivam Bhasin, Jakub Breier, Mustafa Khairallah, Thomas Peyrin, Sumanta Sarkar, and Siang Meng Sim

1 Uniqueness of Decompositions

2 Some Intuition

3 An Example: DEFAULT

4 Open Questions

Open Questions

- Are there any security implications from a non-unique decomposition?
- Are there implications for implementing a cipher/primitive?
- Besides DEFAULT, can we find other (SPN-)ciphers that don't have a unique decomposition?
- Are there properties that assume a unique decomposition (that also are evaluated for ciphers without one)? (One Example: Alignment[2])

Thank you for your attention!

[2] By Nicolas Bordes, Joan Daemen, Daniël Kuijsters, and Gilles Van Assche

Open Questions

- Are there any security implications from a non-unique decomposition?
- Are there implications for implementing a cipher/primitive?
- Besides DEFAULT, can we find other (SPN-)ciphers that don't have a unique decomposition?
- Are there properties that assume a unique decomposition (that also are evaluated for ciphers without one)? (One Example: Alignment[2])

Thank you for your attention!

[2] By Nicolas Bordes, Joan Daemen, Daniël Kuijsters, and Gilles Van Assche