CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

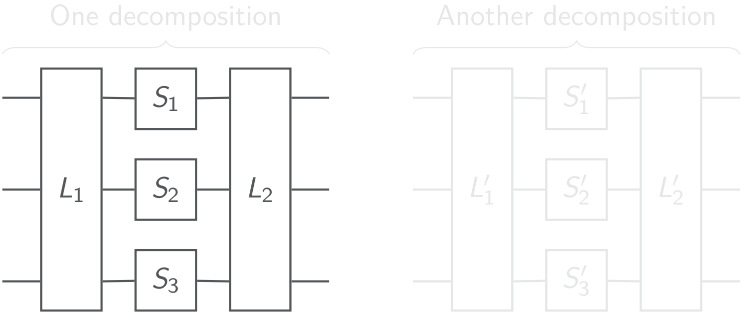
Pitfalls and Shortcomings for Decompositions and Alignment

Lyon, April 25

Baptiste Lambin[1,2] Gregor Leander[1] Patrick Neumann[1]
[1]Ruhr-University Bochum
[2]University of Luxembourg

RUHR UNIVERSITÄT BOCHUM RUB
UNIVERSITÉ DU LUXEMBOURG
Gefördert durch DFG Deutsche Forschungsgemeinschaft
HORST GÖRTZ INSTITUT

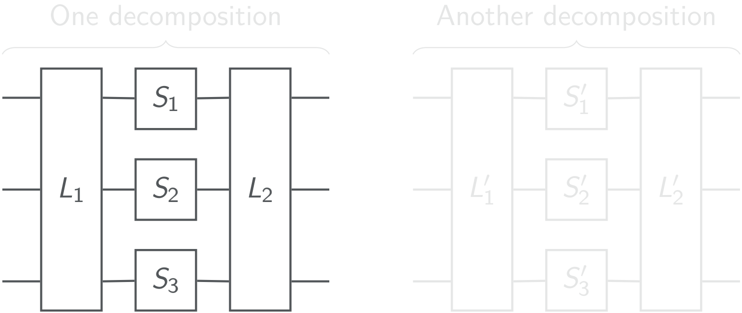
Decomposition of SPN Round Function



- Linear layers:
  L_1, L_2, L'_1, L'_2
- S-boxes:
  S_1, S_2, S_3, S'_1, S'_2, S'_3

- Security arguments based on decomposition
- Example: Bound probability of differential characteristic by counting active S-boxes
- Potential problem: Result may depend on the decomposition
- Question: When do multiple decompositions exist?

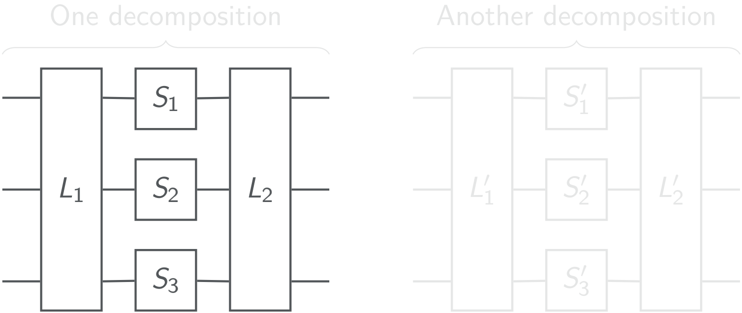
Decomposition of SPN Round Function



- Linear layers: L_1, L_2, L'_1, L'_2
- S-boxes: S_1, S_2, S_3, S'_1, S'_2, S'_3

- Security arguments based on decomposition
- Example: Bound probability of differential characteristic by counting active S-boxes
- Potential problem: Result may depend on the decomposition
- Question: When do multiple decompositions exist?

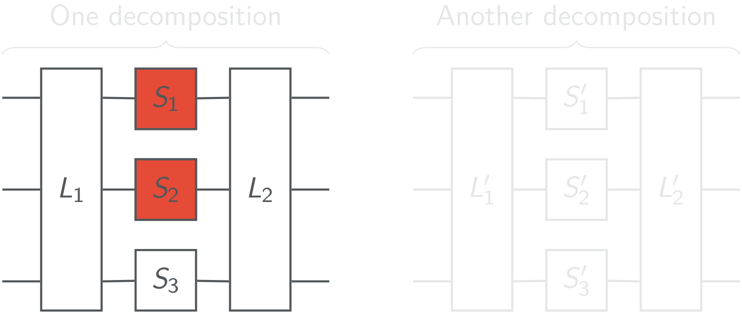
Decomposition of SPN Round Function



- Linear layers: L_1, L_2, L'_1, L'_2
- S-boxes: S_1, S_2, S_3, S'_1, S'_2, S'_3

- Security arguments based on decomposition
- Example: Bound probability of differential characteristic by counting active S-boxes
- Potential problem: Result may depend on the decomposition
- Question: When do multiple decompositions exist?

Decomposition of SPN Round Function

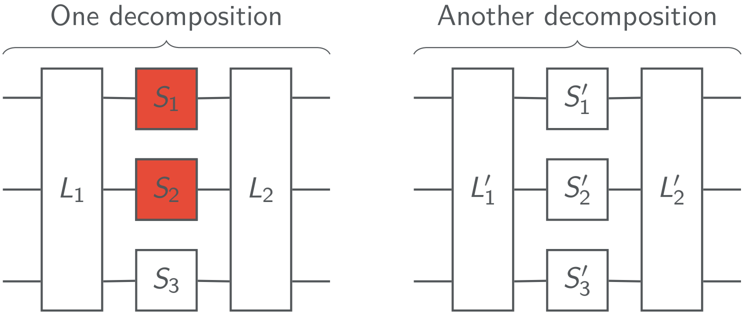


- Linear layers: L_1, L_2, L'_1, L'_2
- S-boxes: S_1, S_2, S_3, S'_1, S'_2, S'_3

- Security arguments based on decomposition
- Example: Bound probability of differential characteristic by counting active S-boxes
- Potential problem: Result may depend on the decomposition
- Question: When do multiple decompositions exist?

Decomposition of SPN Round Function

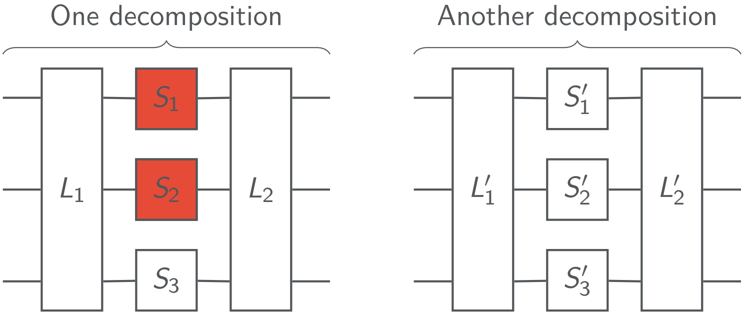
CASA
Cyber Security in the Age of Large-Scale Adversaries



- Linear layers: L_1, L_2, L'_1, L'_2
- S-boxes: S_1, S_2, S_3, S'_1, S'_2, S'_3

- Security arguments based on decomposition
- Example: Bound probability of differential characteristic by counting active S-boxes
- Potential problem: Result may depend on the decomposition
- Question: When do multiple decompositions exist?

Decomposition of SPN Round Function

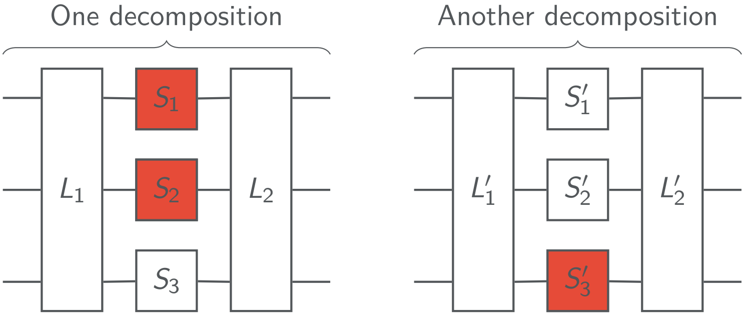


- Linear layers: L_1, L_2, L'_1, L'_2
- S-boxes: S_1, S_2, S_3, S'_1, S'_2, S'_3

- Security arguments based on decomposition
- Example: Bound probability of differential characteristic by counting active S-boxes
- Potential problem: Result may depend on the decomposition
- Question: When do multiple decompositions exist?

Decomposition of SPN Round Function

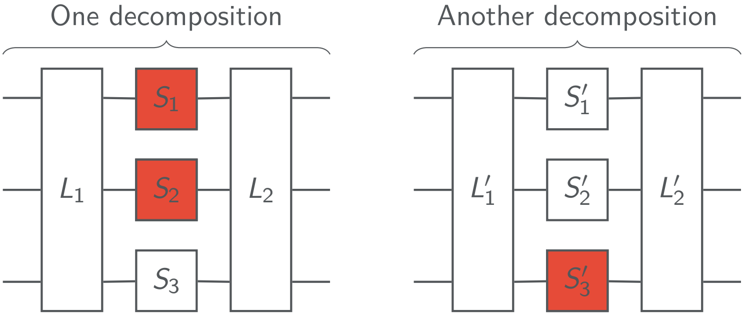
CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES



- Linear layers: L_1, L_2, L'_1, L'_2
- S-boxes: S_1, S_2, S_3, S'_1, S'_2, S'_3

- Security arguments based on decomposition
- Example: Bound probability of differential characteristic by counting active S-boxes
- Potential problem: Result may depend on the decomposition
- Question: When do multiple decompositions exist?

Decomposition of SPN Round Function

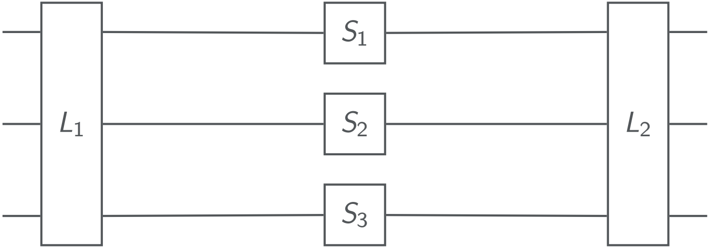


- Linear layers: L_1, L_2, L'_1, L'_2
- S-boxes: S_1, S_2, S_3, S'_1, S'_2, S'_3

- Security arguments based on decomposition
- Example: Bound probability of differential characteristic by counting active S-boxes
- Potential problem: Result may depend on the decomposition
- Question: When do multiple decompositions exist?

Uniqueness of Decompositions

- Well knows limitations to uniqueness
  - Reordering the S-boxes
  - Linear equivalence of the S-boxes
  - Combining S-boxes

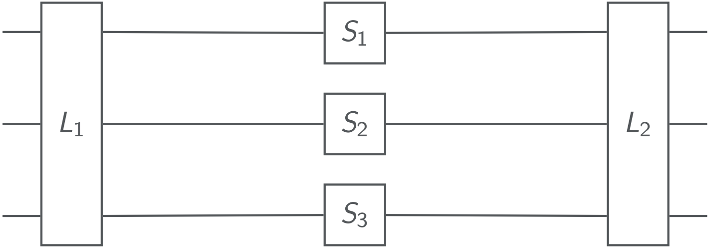


Main Question

When is a decomposition unique (up to those limitations)?

Uniqueness of Decompositions

- Well knows limitations to uniqueness
  - Reordering the S-boxes
  - Linear equivalence of the S-boxes
  - Combining S-boxes

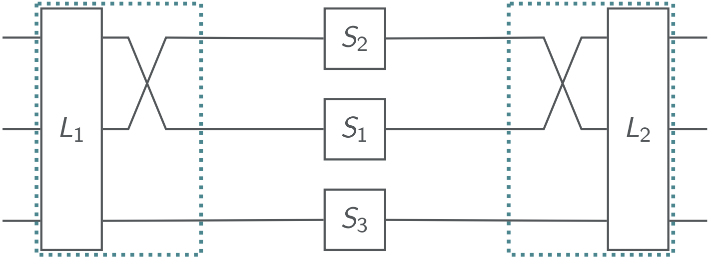


Main Question

When is a decomposition unique (up to those limitations)?

Uniqueness of Decompositions

- Well knows limitations to uniqueness
  - Reordering the S-boxes
  - Linear equivalence of the S-boxes
  - Combining S-boxes

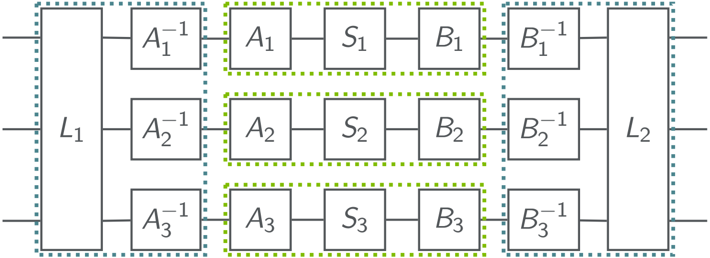


Main Question

When is a decomposition unique (up to those limitations)?

Uniqueness of Decompositions

- Well knows limitations to uniqueness
  - Reordering the S-boxes
  - Linear equivalence of the S-boxes
  - Combining S-boxes

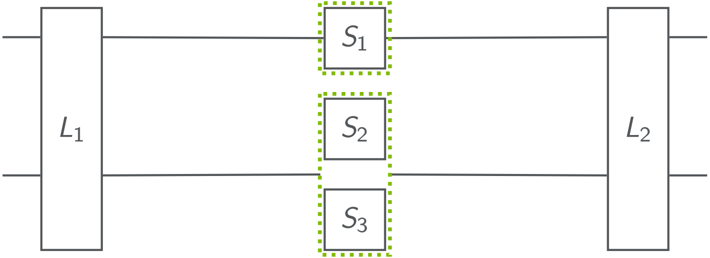


Main Question

When is a decomposition unique (up to those limitations)?

Uniqueness of Decompositions

- Well knows limitations to uniqueness
  - Reordering the S-boxes
  - Linear equivalence of the S-boxes
  - Combining S-boxes

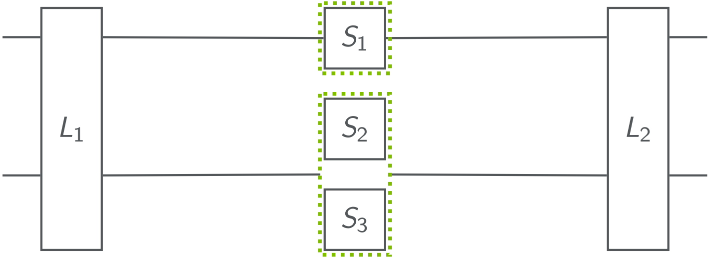


Main Question

When is a decomposition unique (up to those limitations)?

Uniqueness of Decompositions

- Well knows limitations to uniqueness
  - Reordering the S-boxes
  - Linear equivalence of the S-boxes
  - Combining S-boxes



Main Question

When is a decomposition unique (up to those limitations)?

Uniqueness of Decompositions

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Definition

A function F has maximal differential uniformity if $F(x) + F(x + \alpha) = \beta$ for some non-zero α, some β and all x.

Definition

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

Main Theorem

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

- Good, since decomposition is unique for all cryptographically strong S-boxes
- Easy/efficient to check (for all common S-box sizes)

Uniqueness of Decompositions

Definition

A function F has maximal differential uniformity if $F(x) + F(x + \alpha) = \beta$ for some non-zero α, some β and all x.

Definition

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

Main Theorem

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

- Good, since decomposition is unique for all cryptographically strong S-boxes
- Easy/efficient to check (for all common S-box sizes)

Uniqueness of Decompositions

CASA
Cyber Security in the Age of Large-Scale Adversaries

Definition

A function F has maximal differential uniformity if $F(x) + F(x + \alpha) = \beta$ for some non-zero α, some β and all x.

Definition

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

Main Theorem

A decomposition is <u>not</u> unique if and only if one S-box has maximal differential uniformity and another one has maximal linearity.

- Good, since decomposition is unique for all cryptographically strong S-boxes
- Easy/efficient to check (for all common S-box sizes)

Uniqueness of Decompositions

CASA
Cyber Security in the Age of Large-Scale Adversaries

Definition

A function F has maximal differential uniformity if $F(x) + F(x + \alpha) = \beta$ for some non-zero α, some β and all x.

Definition

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

Main Theorem

A decomposition is <u>not</u> unique if and only if one S-box has maximal differential uniformity and another one has maximal linearity.

- Good, since decomposition is unique for all cryptographically strong S-boxes
- Easy/efficient to check (for all common S-box sizes)

Uniqueness of Decompositions

Definition

A function F has maximal differential uniformity if $F(x) + F(x + \alpha) = \beta$ for some non-zero α, some β and all x.

Definition

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

Main Theorem

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

- Good, since decomposition is unique for all cryptographically strong S-boxes
- Easy/efficient to check (for all common S-box sizes)

Sketch of Proof

CASA
Cyber Security in the Age of Large-Scale Adversaries

- Backward direction: If one S-box has maximal differential uniformity and another one has maximal linearity then there exist multiple decompositions

Lemma

Functions with maximal differential uniformity are exactly those that are linear equivalent to functions of the form

$$G\begin{pmatrix} x \\ y \end{pmatrix} = G\begin{pmatrix} x \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ y \end{pmatrix}.$$

Idea of Proof:

- F has maximal differential uniformity $\implies F(x') + F(x' + \alpha) = \beta$ for some $\alpha \neq 0, \beta$
- Linearly transform F to G such that α and β correspond to last bit y

Sketch of Proof

- Backward direction: If one S-box has maximal differential uniformity and another one has maximal linearity then there exist multiple decompositions

Lemma

Functions with maximal differential uniformity are exactly those that are linear equivalent to functions of the form

$$G\begin{pmatrix}x\\y\end{pmatrix} = G\begin{pmatrix}x\\0\end{pmatrix} + \begin{pmatrix}0\\y\end{pmatrix}.$$

Idea of Proof:

- F has maximal differential uniformity $\implies F(x') + F(x' + \alpha) = \beta$ for some $\alpha \neq 0, \beta$
- Linearly transform F to G such that α and β correspond to last bit y

Sketch of Proof

- Backward direction: If one S-box has maximal differential uniformity and another one has maximal linearity then there exist multiple decompositions

Lemma

Functions with maximal differential uniformity are exactly those that are linear equivalent to functions of the form

$$G\begin{pmatrix} x \\ y \end{pmatrix} = G\begin{pmatrix} x \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ y \end{pmatrix}.$$

Idea of Proof:

- F has maximal differential uniformity $\implies F(x') + F(x' + \alpha) = \beta$ for some $\alpha \neq 0$, β
- Linearly transform F to G such that α and β correspond to last bit y

Sketch of Proof

- Backward direction: If one S-box has maximal differential uniformity and another one has maximal linearity then there exist multiple decompositions

Lemma

Functions with maximal differential uniformity are exactly those that are linear equivalent to functions of the form

$$G\begin{pmatrix} x \\ y \end{pmatrix} = G\begin{pmatrix} x \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ y \end{pmatrix}.$$

Idea of Proof:

- F has maximal differential uniformity $\implies$ $F(x') + F(x' + \alpha) = \beta$ for some $\alpha \neq 0$, β
- Linearly transform F to G such that α and β correspond to last bit y

Sketch of Proof

Lemma

Functions with maximal linearity are exactly those that are affine equivalent to functions of the form

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

Idea of Proof:

- F has maximal linearity $\implies$ $\alpha^T \cdot F(x') = \beta^T \cdot x' + c$ for some $\alpha \neq 0$, β and c
- Add $F(0)$ to F, as $\alpha^T \cdot (F + F(0))$ is linear
- Linearly transform $F + F(0)$ to H such that α and β both correspond to $(1, 0, \ldots, 0)^T$

Sketch of Proof

Lemma

Functions with maximal linearity are exactly those that are affine equivalent to functions of the form

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

Idea of Proof:

- F has maximal linearity $\implies \alpha^T \cdot F(x') = \beta^T \cdot x' + c$ for some $\alpha \neq 0$, β and c
- Add $F(0)$ to F, as $\alpha^T \cdot (F + F(0))$ is linear
- Linearly transform $F + F(0)$ to H such that α and β both correspond to $(1, 0, \ldots, 0)^T$

Sketch of Proof

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Lemma

Functions with maximal linearity are exactly those that are affine equivalent to functions of the form

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

Idea of Proof:

- F has maximal linearity $\implies \alpha^T \cdot F(x') = \beta^T \cdot x' + c$ for some $\alpha \neq 0$, β and c
- Add $F(0)$ to F, as $\alpha^T \cdot (F + F(0))$ is linear
- Linearly transform $F + F(0)$ to H such that α and β both correspond to $(1, 0, \ldots, 0)^T$

Sketch of Proof

Lemma

Functions with maximal linearity are exactly those that are affine equivalent to functions of the form

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

Idea of Proof:

- F has maximal linearity $\implies \alpha^T \cdot F(x') = \beta^T \cdot x' + c$ for some $\alpha \neq 0$, β and c
- Add $F(0)$ to F, as $\alpha^T \cdot (F + F(0))$ is linear
- Linearly transform $F + F(0)$ to H such that α and β both correspond to $(1, 0, \ldots, 0)^T$

Sketch of Proof

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Corollary

Functions <u>without</u> unique decomposition are exactly those affine equivalent to ones of the form

$$R\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix} = \begin{pmatrix} G\begin{pmatrix}x_1\\0\end{pmatrix} + \begin{pmatrix}0\\x_2\end{pmatrix} \\ x_3 \\ h\begin{pmatrix}x_3\\x_4\end{pmatrix}\end{pmatrix} \begin{matrix}\}\ \textit{S-box(es)} \\ \}\ \textit{S-box(es)}\end{matrix}.$$

Sketch of Proof

$$R\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix} = \begin{pmatrix} G\begin{pmatrix}x_1\\0\end{pmatrix} + \begin{pmatrix}0\\x_2\end{pmatrix} \\ x_3 \\ h\begin{pmatrix}x_3\\x_4\end{pmatrix}\end{pmatrix} = \begin{pmatrix} G\begin{pmatrix}x_1\\0\end{pmatrix} + \begin{pmatrix}0\\x_2+x_3\end{pmatrix} + \begin{pmatrix}0\\x_3\end{pmatrix} \\ x_3 \\ h\begin{pmatrix}x_3\\x_4\end{pmatrix}\end{pmatrix}$$

$$= \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) R \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) \begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}$$

- Decomposition not unique, as linear layers are different
- Other direction: See paper

Sketch of Proof

$$R\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix} = \begin{pmatrix} G\begin{pmatrix}x_1\\0\end{pmatrix} + \begin{pmatrix}0\\x_2\end{pmatrix} \\ x_3 \\ h\begin{pmatrix}x_3\\x_4\end{pmatrix}\end{pmatrix} = \begin{pmatrix} G\begin{pmatrix}x_1\\0\end{pmatrix} + \begin{pmatrix}0\\x_2 + {\color{red}x_3}\end{pmatrix} + \begin{pmatrix}0\\{\color{red}x_3}\end{pmatrix} \\ x_3 \\ h\begin{pmatrix}x_3\\x_4\end{pmatrix}\end{pmatrix}$$

$$= \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & {\color{red}1} & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) R \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & {\color{red}1} & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) \begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}$$

- Decomposition not unique, as linear layers are different
- Other direction: See paper

Sketch of Proof

$$R\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}=\begin{pmatrix}G\begin{pmatrix}x_1\\0\end{pmatrix}+\begin{pmatrix}0\\x_2\end{pmatrix}\\x_3\\h\begin{pmatrix}x_3\\x_4\end{pmatrix}\end{pmatrix}=\begin{pmatrix}G\begin{pmatrix}x_1\\0\end{pmatrix}+\begin{pmatrix}0\\x_2+x_3\end{pmatrix}+\begin{pmatrix}0\\x_3\end{pmatrix}\\x_3\\h\begin{pmatrix}x_3\\x_4\end{pmatrix}\end{pmatrix}$$

$$=\left(\begin{array}{cc|cc}1&0&0&0\\0&1&1&0\\\hline 0&0&1&0\\0&0&0&1\end{array}\right)R\left(\begin{array}{cc|cc}1&0&0&0\\0&1&1&0\\\hline 0&0&1&0\\0&0&0&1\end{array}\right)\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}$$

- Decomposition not unique, as linear layers are different
- Other direction: See paper

Sketch of Proof

CASA
Cyber Security in the Age of Large-Scale Adversaries

$$R\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix} = \begin{pmatrix} G\begin{pmatrix}x_1\\0\end{pmatrix} + \begin{pmatrix}0\\x_2\end{pmatrix} \\ x_3 \\ h\begin{pmatrix}x_3\\x_4\end{pmatrix}\end{pmatrix} = \begin{pmatrix} G\begin{pmatrix}x_1\\0\end{pmatrix} + \begin{pmatrix}0\\x_2 + x_3\end{pmatrix} + \begin{pmatrix}0\\x_3\end{pmatrix} \\ x_3 \\ h\begin{pmatrix}x_3\\x_4\end{pmatrix}\end{pmatrix}$$

$$= \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) R \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) \begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}$$

- Decomposition not unique, as linear layers are different
- Other direction: See paper

Sketch of Proof

$$R\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix} = \begin{pmatrix} G\begin{pmatrix}x_1\\0\end{pmatrix} + \begin{pmatrix}0\\x_2\end{pmatrix} \\ x_3 \\ h\begin{pmatrix}x_3\\x_4\end{pmatrix}\end{pmatrix} = \begin{pmatrix} G\begin{pmatrix}x_1\\0\end{pmatrix} + \begin{pmatrix}0\\x_2 + \color{red}{x_3}\end{pmatrix} + \begin{pmatrix}0\\\color{red}{x_3}\end{pmatrix} \\ x_3 \\ h\begin{pmatrix}x_3\\x_4\end{pmatrix}\end{pmatrix}$$

$$= \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & \color{red}{1} & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) R \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & \color{red}{1} & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) \begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}$$

- Decomposition not unique, as linear layers are different
- Other direction: See paper

Uniqueness of Decompositions

- Example without unique decomposition: DEFAULT[1]
- Have to be careful if S-boxes with maximal differential uniformity and linearity are/can be used!
- One such case: Alignment
  - Misterious property:
    - Positive & negative correlations
    - For a long time: Not formally defined
  - First formal definition at CRYPTO'21[2]
  - Informally, alignment means that two rounds decompose with at least two S-boxes (referred to as super-boxes)
  - Investigate: Definition & impact of alignment

[1] A. Baksi, S. Bhasin, J. Breier, M. Khairallah, T. Peyrin, S. Sarkar, and S. M. Sim at ASIACRYPT'21

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

Uniqueness of Decompositions

CASA
Cyber Security in the Age of Large-Scale Adversaries

- Example without unique decomposition: DEFAULT[1]
- Have to be careful if S-boxes with maximal differential uniformity and linearity are/can be used!
- One such case: Alignment
  - Misterious property:
    - Positive & negative connotations
    - For a long time: Not formally defined
  - First formal definition at CRYPTO'21[2]
  - Informally, alignment means that two rounds decompose with at least two S-boxes (referred to as super-boxes)
  - Investigate: Definition & impact of alignment

[1] A. Baksi, S. Bhasin, J. Breier, M. Khairallah, T. Peyrin, S. Sarkar, and S. M. Sim at ASIACRYPT'21

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

Uniqueness of Decompositions

- Example without unique decomposition: DEFAULT[1]
- Have to be careful if S-boxes with maximal differential uniformity and linearity are/can be used!
- One such case: Alignment
  - Misterious property:
    - Positive & negative connotations
    - For a long time: Not formally defined
  - First formal definition at CRYPTO'21[2]
  - Informally, alignment means that two rounds decompose with at least two S-boxes (referred to as super-boxes)
  - Investigate: Definition & impact of alignment

[1] A. Baksi, S. Bhasin, J. Breier, M. Khairallah, T. Peyrin, S. Sarkar, and S. M. Sim at ASIACRYPT'21

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

Uniqueness of Decompositions

- Example without unique decomposition: DEFAULT[1]
- Have to be careful if S-boxes with maximal differential uniformity and linearity are/can be used!
- One such case: Alignment
  - Misterious property:
    - Positive & negative connotations
    - For a long time: Not formally defined
  - First formal definition at CRYPTO'21[2]
  - Informally, alignment means that two rounds decompose with at least two S-boxes (referred to as super-boxes)
  - Investigate: Definition & impact of alignment

[1] A. Baksi, S. Bhasin, J. Breier, M. Khairallah, T. Peyrin, S. Sarkar, and S. M. Sim at ASIACRYPT'21

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

Uniqueness of Decompositions

- Example without unique decomposition: DEFAULT[1]
- Have to be careful if S-boxes with maximal differential uniformity and linearity are/can be used!
- One such case: Alignment
  - Misterious property:
    - Positive & negative connotations
    - For a long time: Not formally defined
  - First formal definition at CRYPTO'21[2]
  - Informally, alignment means that two rounds decompose with at least two S-boxes (referred to as super-boxes)
  - Investigate: Definition & impact of alignment

[1] A. Baksi, S. Bhasin, J. Breier, M. Khairallah, T. Peyrin, S. Sarkar, and S. M. Sim at ASIACRYPT'21

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

Uniqueness of Decompositions

- Example without unique decomposition: DEFAULT[1]
- Have to be careful if S-boxes with maximal differential uniformity and linearity are/can be used!
- One such case: Alignment
  - Misterious property:
    - Positive & negative connotations
    - For a long time: Not formally defined
  - First formal definition at CRYPTO'21[2]
  - Informally, alignment means that two rounds decompose with at least two S-boxes (referred to as super-boxes)
  - Investigate: Definition & impact of alignment

[1] A. Baksi, S. Bhasin, J. Breier, M. Khairallah, T. Peyrin, S. Sarkar, and S. M. Sim at ASIACRYPT'21
[2] By Nicolas Bordes, Joan Daemen, Daniël Kuijsters, and Gilles Van Assche

Uniqueness of Decompositions

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- Example without unique decomposition: DEFAULT[1]
- Have to be careful if S-boxes with maximal differential uniformity and linearity are/can be used!
- One such case: Alignment
  - Misterious property:
    - Positive & negative connotations
    - For a long time: Not formally defined
  - First formal definition at CRYPTO'21[2]
  - Informally, alignment means that two rounds decompose with at least two S-boxes (referred to as super-boxes)
  - Investigate: Definition & impact of alignment

[1] A. Baksi, S. Bhasin, J. Breier, M. Khairallah, T. Peyrin, S. Sarkar, and S. M. Sim at ASIACRYPT'21
[2] By Nicolas Bordes, Joan Daemen, Daniël Kuijsters, and Gilles Van Assche

Uniqueness of Decompositions

- Example without unique decomposition: DEFAULT[1]
- Have to be careful if S-boxes with maximal differential uniformity and linearity are/can be used!
- One such case: Alignment
  - Misterious property:
    - Positive & negative connotations
    - For a long time: Not formally defined
  - First formal definition at CRYPTO'21[2]
  - Informally, alignment means that two rounds decompose with at least two S-boxes (referred to as super-boxes)
  - Investigate: Definition & impact of alignment

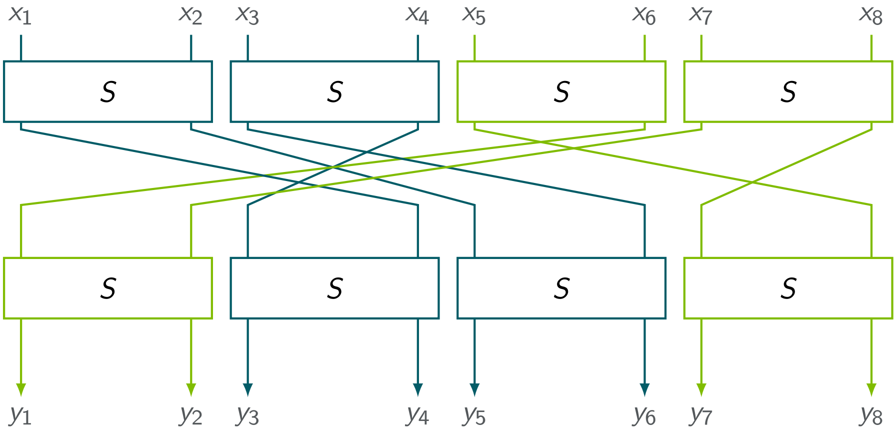
[1] A. Baksi, S. Bhasin, J. Breier, M. Khairallah, T. Peyrin, S. Sarkar, and S. M. Sim at ASIACRYPT'21
[2] By Nicolas Bordes, Joan Daemen, Daniël Kuijsters, and Gilles Van Assche

Uniqueness of Decompositions

- Example without unique decomposition: DEFAULT[1]
- Have to be careful if S-boxes with maximal differential uniformity and linearity are/can be used!
- One such case: Alignment
  - Misterious property:
    - Positive & negative connotations
    - For a long time: Not formally defined
  - First formal definition at CRYPTO'21[2]
  - Informally, alignment means that two rounds decompose with at least two S-boxes (referred to as super-boxes)
  - Investigate: Definition & impact of alignment

[1] A. Baksi, S. Bhasin, J. Breier, M. Khairallah, T. Peyrin, S. Sarkar, and S. M. Sim at ASIACRYPT'21
[2] By Nicolas Bordes, Joan Daemen, Daniël Kuijsters, and Gilles Van Assche

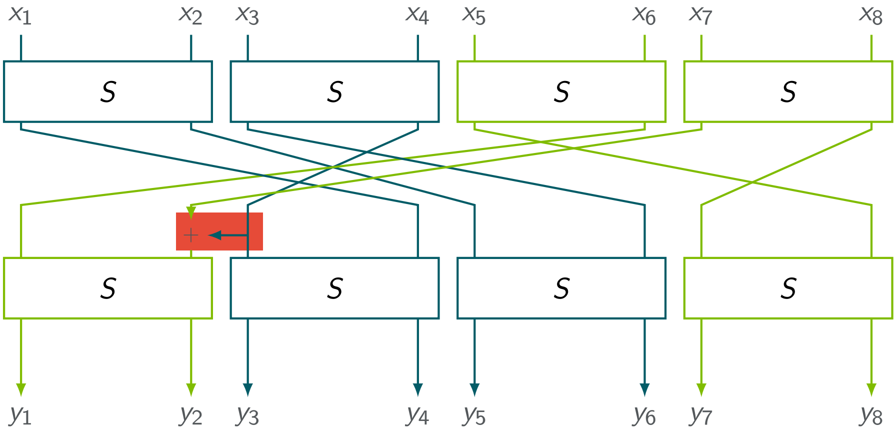
Alignment and Non-Unique Decompositions



- Function aligned

Alignment and Non-Unique Decompositions

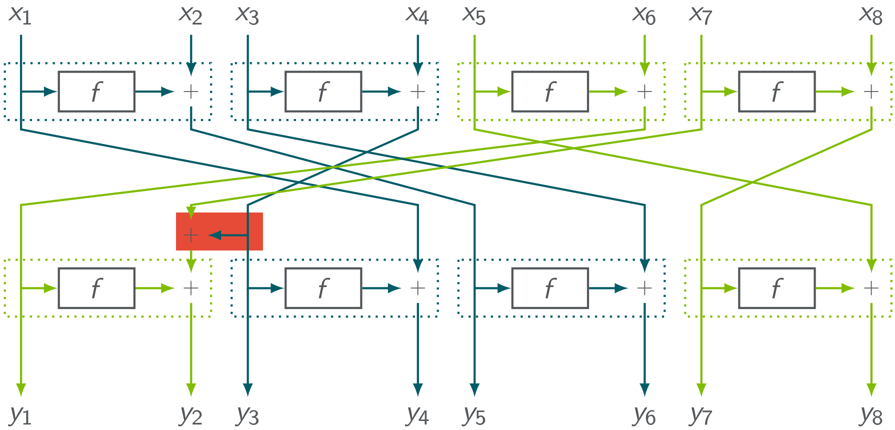
CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES



- Function unaligned

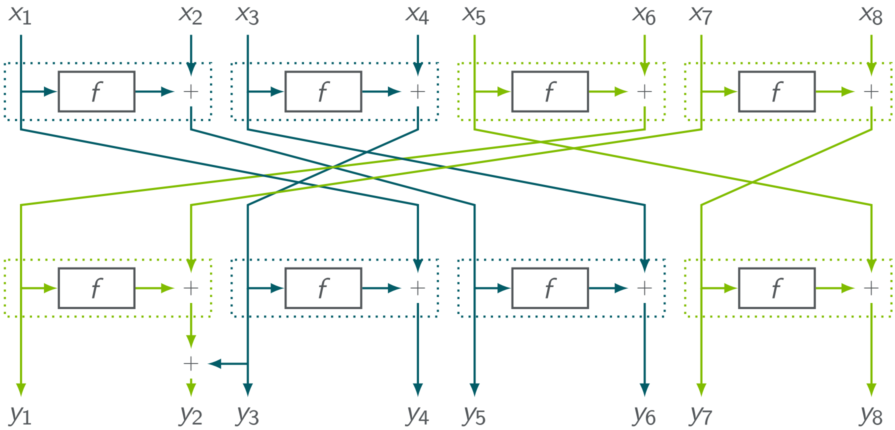
Alignment and Non-Unique Decompositions

CASA
Cyber Security in the Age of Large-Scale Adversaries



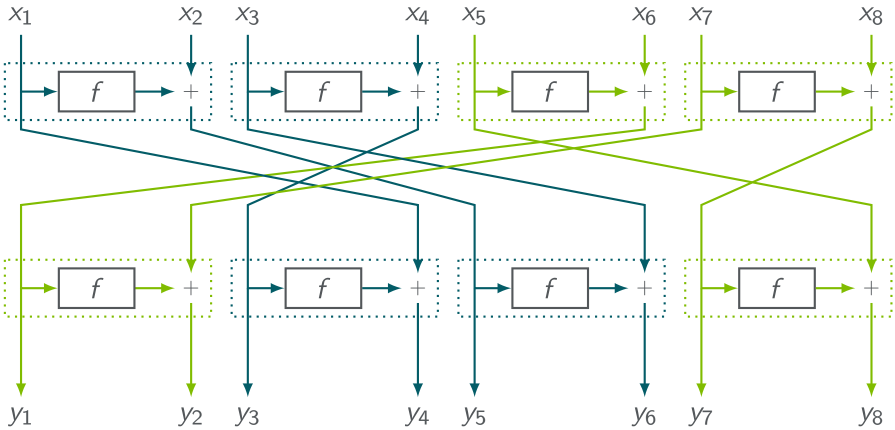
- Function unaligned

Alignment and Non-Unique Decompositions



- Function unaligned

Alignment and Non-Unique Decompositions



- Function unaligned, but also aligned?

Alignment – Impact

- (CRYPTO'21) compared aligned and unaligned ciphers
- Infer that alignment might lead to bigger clustering effects
- Question: Results due to alignment or due to other disparities?
- Idea: Change bit-permutation of PRESENT
  - Produce variants that are aligned and ones that are unaligned
  - Preserve full diffusion after 3 round
  - Preserve all 1-to-1 linear trails

Alignment – Impact

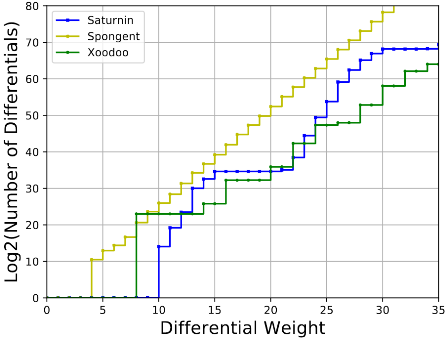
- (CRYPTO'21) compared aligned and unaligned ciphers
- Infer that alignment might lead to bigger clustering effects
- Question: Results due to alignment or due to other disparities?
- Idea: Change bit-permutation of PRESENT
  - Produce variants that are aligned and ones that are unaligned
  - Preserve full diffusion after 3 round
  - Preserve all 1-to-1 linear trails

Alignment – Impact

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- (CRYPTO'21) compared aligned and unaligned ciphers
- Infer that alignment might lead to bigger clustering effects
- Question: Results due to alignment or due to other disparities?
- Idea: Change bit-permutation of PRESENT
  - Produce variants that are aligned and ones that are unaligned
  - Preserve full diffusion after 3 round
  - Preserve all 1-to-1 linear trails

Cumulative histogram of the number of differentials of a given weight over 2 rounds

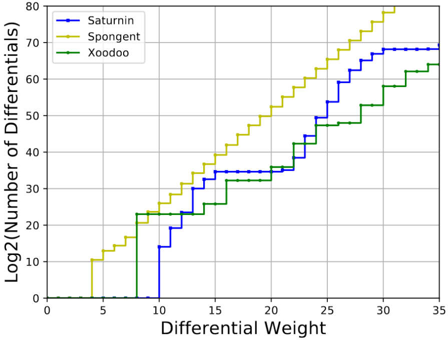


Saturnin, Spongent and Xoodoo (CRYPTO'21)

Alignment – Impact

- (CRYPTO'21) compared aligned and unaligned ciphers
- Infer that alignment might lead to bigger clustering effects
- Question: Results due to alignment or due to other disparities?
- Idea: Change bit-permutation of PRESENT
  - Produce variants that are aligned and ones that are unaligned
  - Preserve full diffusion after 3 round
  - Preserve all 1-to-1 linear trails

Cumulative histogram of the number of differentials of a given weight over 2 rounds

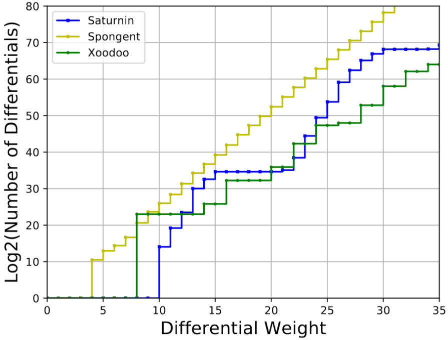


Saturnin, Spongent and Xoodoo (CRYPTO'21)

Alignment – Impact

- (CRYPTO'21) compared aligned and unaligned ciphers
- Infer that alignment might lead to bigger clustering effects
- Question: Results due to alignment or due to other disparities?
- Idea: Change bit-permutation of PRESENT
  - Produce variants that are aligned and ones that are unaligned
  - Preserve full diffusion after 3 round
  - Preserve all 1-to-1 linear trails

Cumulative histogram of the number of differentials of a given weight over 2 rounds



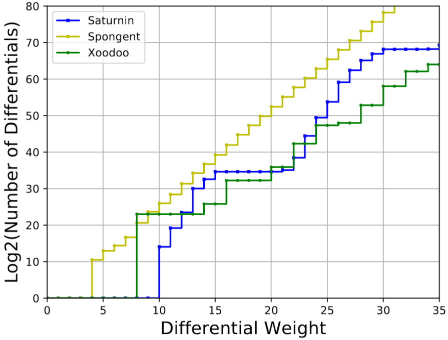
Saturnin, Spongent and Xoodoo (CRYPTO'21)

Alignment – Impact

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- (CRYPTO'21) compared aligned and unaligned ciphers
- Infer that alignment might lead to bigger clustering effects
- Question: Results due to alignment or due to other disparities?
- Idea: Change bit-permutation of PRESENT
  - Produce variants that are aligned and ones that are unaligned
  - Preserve full diffusion after 3 round
  - Preserve all 1-to-1 linear trails

Cumulative histogram of the number of differentials of a given weight over 2 rounds



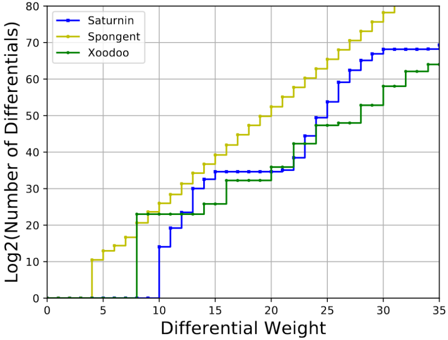
Saturnin, Spongent and Xoodoo (CRYPTO'21)

Alignment – Impact

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- (CRYPTO'21) compared aligned and unaligned ciphers
- Infer that alignment might lead to bigger clustering effects
- Question: Results due to alignment or due to other disparities?
- Idea: Change bit-permutation of PRESENT
  - Produce variants that are aligned and ones that are unaligned
  - Preserve full diffusion after 3 round
  - Preserve all 1-to-1 linear trails

Cumulative histogram of the number of differentials of a given weight over 2 rounds

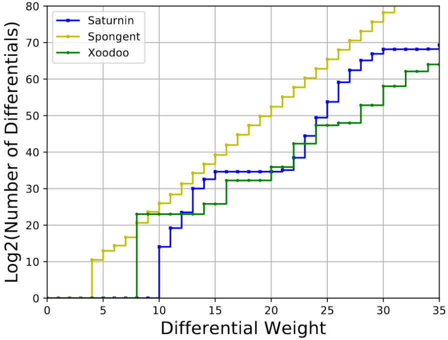


Saturnin, Spongent and Xoodoo (CRYPTO'21)

Alignment – Impact

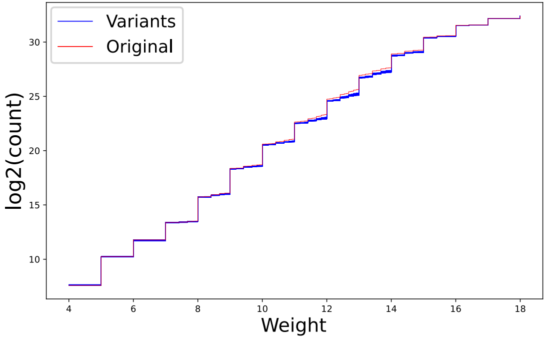
- (CRYPTO'21) compared aligned and unaligned ciphers
- Infer that alignment might lead to bigger clustering effects
- Question: Results due to alignment or due to other disparities?
- Idea: Change bit-permutation of PRESENT
  - Produce variants that are aligned and ones that are unaligned
  - Preserve full diffusion after 3 round
  - Preserve all 1-to-1 linear trails

Cumulative histogram of the number of differentials of a given weight over 2 rounds

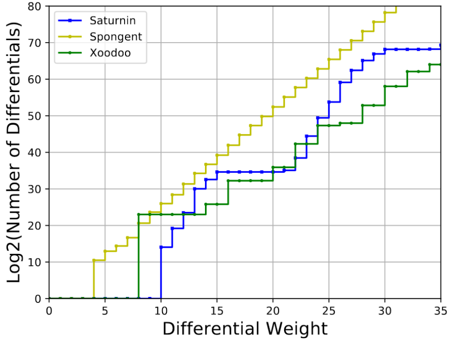


Saturnin, Spongent and Xoodoo (CRYPTO'21)

Cumulative histogram of the number of differentials of a given weight over 2 rounds



Variants of PRESENT
(original aligned, variants unaligned)

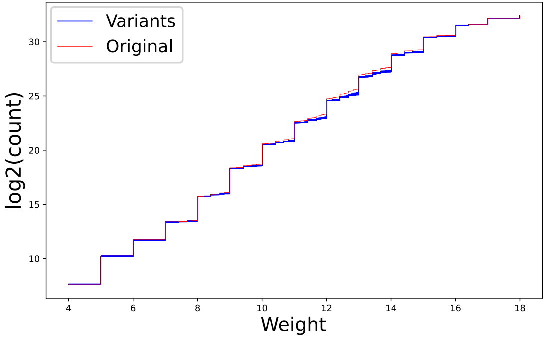


Saturnin, Spongent and Xoodoo
(CRYPTO'21)

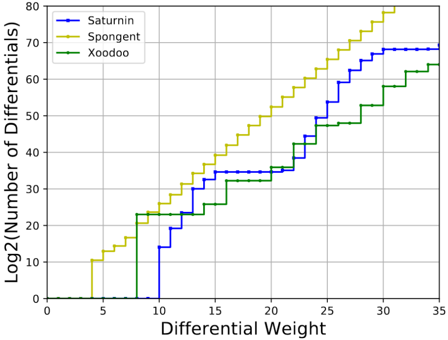
- Overall result: PRESENT variants behave very similar in all aspects

Cumulative histogram of the number of differentials of a given weight over 2 rounds

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES



Variants of PRESENT
(original aligned, variants unaligned)



Saturnin, Spongent and Xoodoo
(CRYPTO'21)

- <u>Overall result:</u> PRESENT variants behave very similar in all aspects

Conclusion

- Under some mild conditions decomposition is unique
- Good, as it allows to base security arguments on the unique decomposition
- Still, have to be careful if conditions are not met

- Impact of alignment on clustering may be overestimated
- Benefits of alignment may outweigh this impact

Thank you for your attention!

Conclusion

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- Under some mild conditions decomposition is unique
- Good, as it allows to base security arguments on the unique decomposition
- Still, have to be careful if conditions are not met

- Impact of alignment on clustering may be overestimated
- Benefits of alignment may outweigh this impact

Thank you for your attention!

Conclusion

CASA
Cyber Security in the Age of Large-Scale Adversaries

- Under some mild conditions decomposition is unique
- Good, as it allows to base security arguments on the unique decomposition
- Still, have to be careful if conditions are not met

- Impact of alignment on clustering may be overestimated
- Benefits of alignment may outweigh this impact

Thank you for your attention!

Conclusion

- Under some mild conditions decomposition is unique
- Good, as it allows to base security arguments on the unique decomposition
- Still, have to be careful if conditions are not met

- Impact of alignment on clustering may be overestimated
- Benefits of alignment may outweigh this impact

Thank you for your attention!

Conclusion

- Under some mild conditions decomposition is unique
- Good, as it allows to base security arguments on the unique decomposition
- Still, have to be careful if conditions are not met

- Impact of alignment on clustering may be overestimated
- Benefits of alignment may outweigh this impact

Thank you for your attention!

Conclusion

- Under some mild conditions decomposition is unique
- Good, as it allows to base security arguments on the unique decomposition
- Still, have to be careful if conditions are not met

- Impact of alignment on clustering may be overestimated
- Benefits of alignment may outweigh this impact

Thank you for your attention!