SoK: Modeling for Large S-boxes Oriented to Differential Probabilities and Linear Correlations

Ling Sun and Meiqin Wang(✉)

{lingsun, mqwang}@sdu.edu.cn

Shandong University, Jinan & Qingdao, China

FSE 2023 @ March, 2023

Outline

- **Motivation & Contributions.**
- MILP Modeling Progress for Large S-boxes.
- SAT/SMT Modeling Progress for S-boxes.
- Fast SAT Models for Large S-boxes.
- New Findings with the New SAT Models.
- Conclusion.

SHANDONG UNIVERSITY

Motivation

- Automatic methods for differential and linear characteristic search are well-established.
  - Mixed-integer linear programming (MILP).
  - Boolean satisfiability problem or satisfiability modulo theories (SAT/SMT).
- Searching for actual differential & linear characteristics for large S-boxes is not conclusive.
- How to efficiently create SAT models of large S-boxes?

Motivation & Contributions

Motivation

- Automatic methods for differential and linear characteristic search are well-established.
  - Mixed-integer linear programming (MILP).
  - Boolean satisfiability problem or satisfiability modulo theories (SAT/SMT).
- Searching for actual differential & linear characteristics for large S-boxes is not conclusive.
- How to efficiently create SAT models of large S-boxes?

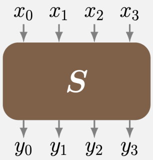
Contributions

- Three strategies are proposed.
  - ① Utilising the option of the ESPRESSO logic minimizer.
  - ② Dividing the description of a large S-box into two steps.
  - ③ Simplifying by partitioning method.
- Upper bound on the differential probability for 14 rounds of `SKINNY-128` is determined.
- Related-key differential properties of both versions of PIPO are investigated.
- Seven `AES`-based constructions `C1` - `C7` are analysed.

Outline

- Motivation & Contributions.
- **MILP Modeling Progress for Large S-boxes.**
- SAT/SMT Modeling Progress for S-boxes.
- Fast SAT Models for Large S-boxes.
- New Findings with the New SAT Models.
- Conclusion.

MILP Modeling Progress for Large S-boxes



DDT

Δ_{in} \ Δ_{out}	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	16															
0x1				4				4		4				4		
0x2				2		4	2				2		2	2	2	
0x3		2		2	2		4	2			2	2				
0x4						4	2	2		2	2		2		2	
0x5		2			2					2	2	2	4	2		
0x6			2				2		2			4	2			4
0x7		4	2				2		2				2			4
0x8				2				2		2		4		2		4
0x9			2		4		2		2				2		4	
0xa			2	2		4			2		2			2	2	
0xb		2			2				4	2	2	2		2		
0xc			2			4		2	2	2	2				2	
0xd		2	4	2	2			2			2	2				
0xe			2	2			2	2	2	2			2	2		
0xf		4			4										4	4

*-DDT

Δ_{in} \ Δ_{out}	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	1															
0x1				1				1		1				1		
0x2				1		1	1				1		1	1	1	
0x3		1		1	1		1	1			1	1				
0x4						1	1	1		1	1		1		1	
0x5		1			1					1	1	1	1	1		
0x6			1				1		1			1	1			1
0x7		1	1				1		1				1			1
0x8				1				1		1		1		1		1
0x9			1		1		1		1				1		1	
0xa			1	1		1			1		1			1	1	
0xb		1			1				1	1	1	1		1		
0xc			1			1		1	1	1	1				1	
0xd		1	1	1	1			1			1	1				
0xe			1	1			1	1	1	1			1	1		
0xf		1			1										1	1

$$\mathcal{F} = \{\boldsymbol{x}\|\boldsymbol{y} \mid \boldsymbol{x} \to \boldsymbol{y} \text{ is a } \textbf{possible} \text{ propagation}, \boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_2^n\}$$

$$\mathcal{I} = \{\boldsymbol{x}\|\boldsymbol{y} \mid \boldsymbol{x} \to \boldsymbol{y} \text{ is an } \textbf{impossible} \text{ propagation}, \boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_2^n\}$$

MILP Modeling Progress for Large S-boxes

SHANDONG UNIVERSITY

First Bit-Oriented Model for S-boxes
Sun *et al.* @ ASIACRYPT 2014

Modeling for Large S-boxes
Abdelkhalek *et al.* @ FSE 2018

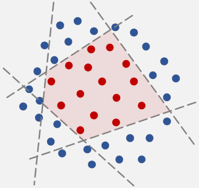
Finding Smallest MILP Models
Li and Sun @ FSE 2023, Udovenko @ Epring

2014 — 2017 — 2018 — 2021 — 2022

Reduction Algorithm for Small S-boxes
Sasaki and Todo @ SecITC 2017

Efficient Modeling for Large S-boxes
Boura and Coggia @ FSE 2021

Approach 1: H-representation of the Convex Hull



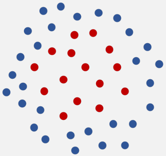
$$\sum_{j=0}^{n-1} a_j^1 \cdot x_j + \sum_{j=0}^{n-1} a_{j+n}^1 \cdot y_j + c^1 \geqslant 0$$

$\cdots\ \cdots$

$$\sum_{j=0}^{n-1} a_j^m \cdot x_j + \sum_{j=0}^{n-1} a_{j+n}^m \cdot y_j + c^m \geqslant 0$$

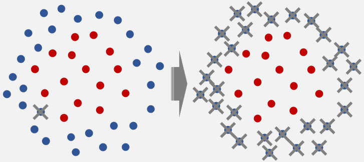
Convex hull ⊳ H-representation

sage.geometry.polyhedron class (SageMath)



- **Possible**
- **Impossible**

Approach 2: Logical Condition Modeling



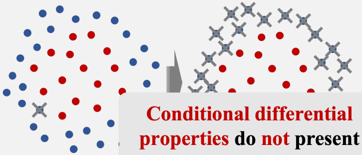
$1001 \nrightarrow 0001$

$$-x_0 + x_1 + x_2 - x_3 + y_0 + y_1 + y_2 - y_3 + 2 \geqslant 0$$

MILP Modeling Progress for Large S-boxes

- 2014 — **First Bit-Oriented Model for S-boxes** — Sun *et al.* @ ASIACRYPT 2014
- 2017 — **Reduction Algorithm for Small S-boxes** — Sasaki and Todo @ SecITC 2017
- 2018 — **Modeling for Large S-boxes** — Abdelkhalek *et al.* @ FSE 2018
- 2021 — **Efficient Modeling for Large S-boxes** — Boura and Coggia @ FSE 2021
- 2022 — **Finding Smallest MILP Models** — Li and Sun @ FSE 2023, Udovenko @ Epring

Approach 2: Logical Condition Modeling



Conditional differential properties do not present in all S-boxes

1001 $\nrightarrow$ ∗∗∗1

$$-x_0 + x_1 + x_2 - x_3 - y_3 + 2 \geqslant 0$$

Modeling of Large S-boxes

- A $2n$-bit Boolean function f is built.
- $f(\boldsymbol{x}\|\boldsymbol{y}) = 1$ if and only if $\boldsymbol{x}\|\boldsymbol{y} \in \mathcal{F} = \mathbb{F}_2^{2n} \setminus \mathcal{I}$.
- The canonical POS form of f is

$$f(\boldsymbol{x}\|\boldsymbol{y}) = \bigwedge_{\boldsymbol{a}\|\boldsymbol{b}\in\mathcal{I}} \left(\bigvee_{i=0}^{n-1} (x_i \oplus a_i) \vee \bigvee_{i=0}^{n-1} (y_i \oplus b_i) \right)$$

- 1-bit XOR $x_i \oplus a_i$ can be represented as $x_i + a_i - 2 \cdot x_i \cdot a_i$.
- Lowering the number of inequalities is akin to simplifying the POS form of f.
- The Quine-McCluskey algorithm can be used to determine the minimum POS.
- Reducing a 16-bit function corresponding to the ∗-DDT of AES is infeasible.
- Heuristic algorithm ESPRESSO was suggested for large-scale functions.

MILP Modeling Progress for Large S-boxes

SHANDONG UNIVERSITY

First Bit-Oriented Model for S-boxes
Sun *et al.* @ ASIACRYPT 2014

Modeling for Large S-boxes
Abdelkhalek *et al.* @ FSE 2018

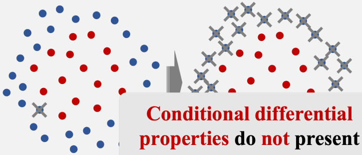
Finding Smallest MILP Models
Li and Sun @ FSE 2023, Udovenko @ Epring

2014 — 2017 — 2018 — 2021 — 2022

Reduction Algorithm for Small S-boxes
Sasaki and Todo @ SecITC 2017

Efficient Modeling for Large S-boxes
Boura and Coggia @ FSE 2021

Approach 2: Logical Condition Modeling



Conditional differential properties do not present in all S-boxes

1001 $\nrightarrow$ ***1

$-x_0 + x_1 + x_2 - x_3 - y_3 + 2 \geqslant 0$

Modeling of Large S-boxes

- A $2n$-bit Boolean function f is built.
- $f(\boldsymbol{x}\|\boldsymbol{y}) = 1$ if and only if $\boldsymbol{x}\|\boldsymbol{y} \in \mathcal{F} = \mathbb{F}_2^{2n} \setminus \mathcal{I}$.
- The canonical POS form of f is

$$f(\boldsymbol{x}\|\boldsymbol{y}) = \bigwedge_{\boldsymbol{a}\|\boldsymbol{b}\in\mathcal{I}} \left(\bigvee_{i=0}^{n-1} (x_i \oplus a_i) \vee \bigvee_{i=0}^{n-1} (y_i \oplus b_i) \right)$$

- 1-bit XOR $x_i \oplus a_i$ can be represented as $x_i + a_i - 2 \cdot x_i \cdot a_i$.
- Lowering the number of inequalities is akin to simplifying the POS form of f.
- The Quine-McCluskey algorithm can be used to determine the minimum POS.
- Reducing a 16-bit function corresponding to the $*$-DDT of AES is infeasible.
- Heuristic algorithm ESPRESSO was suggested for large-scale functions.

MILP Modeling Progress for Large S-boxes

- **2014** — First Bit-Oriented Model for S-boxes — **Sun *et al.* @ ASIACRYPT 2014**
- **2017** — Reduction Algorithm for Small S-boxes — **Sasaki and Todo @ SecITC 2017**
- **2018** — Modeling for Large S-boxes — **Abdelkhalek *et al.* @ FSE 2018**
- **2021** — Efficient Modeling for Large S-boxes — **Boura and Coggia @ FSE 2021**
- **2022** — Finding Smallest MILP Models — **Li and Sun @ FSE 2023, Udovenko @ Epring**

- Minimising the number of inequalities does not always reduce the runtime of the MILP optimiser.
- Many subsequent studies continue to seek a breakthrough on the number of inequalities.
- Improved MILP models for the S-boxes of `AES` and `SKINNY-128` were not employed to analyse the differential characteristics of these ciphers.
- This problem is of theoretical importance in its own right.

Outline

- Motivation & Contributions.
- MILP Modeling Progress for Large S-boxes.
- **SAT/SMT Modeling Progress for S-boxes.**
- Fast SAT Models for Large S-boxes.
- New Findings with the New SAT Models.
- Conclusion.

SAT/SMT Modeling Progress for S-boxes

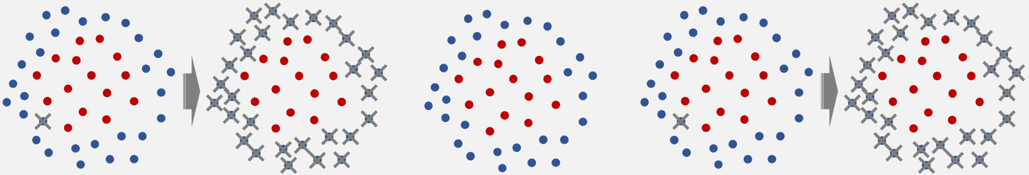
SHANDONG UNIVERSITY

SAT/SMT Modeling Progress for S-boxes

- **2013** — Models for Active S-boxes — **Mouha and Preneel @ Eprint**
- **2015 & 2016** — Search Oriented to ARX Ciphers — **Kölbl *et al.* @ CRYPTO 2015, Liu *et al.* @ ACNS 2016, …**
- **2018** — Logical Condition Modeling — **Ankele and Kölbl @ SAC 2018**
- **2018** — Logical Condition Modeling Using Simplification — **Sun *et al.* @ ToSC 2018**
- **2019** — SMT Modeling for Large S-boxes — **Liu *et al.* @ Epring**

Logical Condition Modeling in MILP

Logical Condition Modeling in SAT



$1001 \nrightarrow 0001$

$-x_0 + x_1 + x_2 - x_3 + y_0 + y_1 + y_2 - y_3 + 2 \geqslant 0$

- **Possible**
- **Impossible**

$1001 \nrightarrow 0001$

$\overline{x_0} \vee x_1 \vee x_2 \vee \overline{x_3} \vee y_0 \vee y_1 \vee y_2 \vee \overline{y_3} = 1$

SAT/SMT Modeling Progress for S-boxes

2013 — Models for Active S-boxes
Mouha and Preneel @ Eprint

2015 & 2016 — Search Oriented to ARX Ciphers
Kölbl *et al.* @ CRYPTO 2015, Liu *et al.* @ ACNS 2016, ...

2018 — Logical Condition Modeling
Ankele and Kölbl @ SAC 2018

2018 — Logical Condition Modeling Using Simplification
Sun *et al.* @ ToSC 2018

2019 — SMT Modeling for Large S-boxes
Liu *et al.* @ Epring

SAT/SMT Modeling Progress for S-boxes

SHANDONG UNIVERSITY

- 2013 — Models for Active S-boxes — **Mouha and Preneel @ Eprint**
- 2015 & 2016 — Search Oriented to ARX Ciphers — **Kölbl *et al.* @ CRYPTO 2015, Liu *et al.* @ ACNS 2016, …**
- 2018 — Logical Condition Modeling — **Ankele and Kölbl @ SAC 2018**
- 2018 — Logical Condition Modeling Using Simplification — **Sun *et al.* @ ToSC 2018**
- 2019 — SMT Modeling for Large S-boxes — **Liu *et al.* @ Epring**

Modeling Oriented to Active S-boxes [Sun *et al.* @ ToSC 2018]

- Auxiliary Boolean variable w.

$$\mathcal{F}_{\langle n,n,1\rangle} = \left\{ \boldsymbol{x}\|\boldsymbol{y}\|w \;\middle|\; \begin{array}{l} \boldsymbol{x},\boldsymbol{y} \in \mathbb{F}_2^n, w \in \mathbb{F}_2, \boldsymbol{x} \to \boldsymbol{y} \text{ is a possible propagation} \\ w = \begin{cases} 0, & \text{if } \Pr(\boldsymbol{x} \to \boldsymbol{y}) = 1 \\ 1, & \text{if } \Pr(\boldsymbol{x} \to \boldsymbol{y}) < 1 \end{cases} \end{array} \right\}.$$

- The number of clauses in the SAT problem will be extremely high if $|\mathbb{F}_2^{2n+1} \backslash \mathcal{F}_{\langle n,n,1\rangle}|$ is enormous.

$$f_{\langle n,n,1\rangle}(\boldsymbol{x}\|\boldsymbol{y}\|w) = \begin{cases} 1, & \text{if } \boldsymbol{x}\|\boldsymbol{y}\|w \in \mathcal{F}_{\langle n,n,1\rangle} \\ 0, & \text{otherwise} \end{cases}.$$

Quine-McCluskey and ESPRESSO algorithms [Abdelkhalek *et al.* @ FSE 2018]

SHANDONG UNIVERSITY

Modeling Oriented to Differential Probabilities and Linear Correlations

- Additional auxiliary variables are required to encode probability information.
- The weight of a possible propagation is $-\log_2(p)$ and can take on non-integer values.
  - Integral portion: μ variables $(u_0, u_1, \ldots, u_{\mu-1}) \triangleq \boldsymbol{u}$.
  - Decimal portion: ν variables $(v_0, v_1, \ldots, v_{\nu-1}) \triangleq \boldsymbol{v}$.

SAT/SMT Modeling Progress for S-boxes

SHANDONG UNIVERSITY

Modeling Oriented to Differential Probabilities and Linear Correlations

- Additional auxiliary variables are required to encode probability information.
- The weight of a possible propagation is $-\log_2(p)$ and can take on non-integer values.
  - Integral portion: μ variables $(u_0, u_1, \ldots, u_{\mu-1}) \triangleq \boldsymbol{u}$.
  - Decimal portion: ν variables $(v_0, v_1, \ldots, v_{\nu-1}) \triangleq \boldsymbol{v}$.
- Consider a 4-bit S-box whose DDT contains the values 0, 2, 4, 6, and 16.
  - The set of probability for all feasible differential propagations is $\{2^{-3}, 2^{-2}, 2^{-1.415}, 1\}$.
  - $(u_0, u_1, u_2) \triangleq \boldsymbol{u}$ to represent the integral portion and v_0 to represent the decimal portion.
  - The optional set of possible values for $\boldsymbol{x}\|\boldsymbol{y}\|\boldsymbol{u}\|v_0$ is

$$\left\{ \boldsymbol{x}\|\boldsymbol{y}\|\boldsymbol{u}\|v_0 \;\middle|\; \begin{array}{l} \boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_2^4, \boldsymbol{u} \in \mathbb{F}_2^3, v_0 \in \mathbb{F}_2, \boldsymbol{x} \to \boldsymbol{y} \text{ is a possible propagation} \\ \boldsymbol{u}\|v_0 = \begin{cases} 1\|1\|1\|0, & \text{if } \Pr(\boldsymbol{x} \to \boldsymbol{y}) = 2^{-3} \\ 0\|1\|1\|0, & \text{if } \Pr(\boldsymbol{x} \to \boldsymbol{y}) = 2^{-2} \\ 0\|0\|1\|1, & \text{if } \Pr(\boldsymbol{x} \to \boldsymbol{y}) = 2^{-1.415} \\ 0\|0\|0\|0, & \text{if } \Pr(\boldsymbol{x} \to \boldsymbol{y}) = 1 \end{cases} \end{array} \right\}.$$

  - The vector in the set confirms $u_0 + u_1 + u_2 + 0.415 \cdot v_0 = -\log_2(p)$.
- The SAT model for differential probabilities can be derived by simplifying the canonical POS form.

Outline

- Motivation & Contributions.
- MILP Modeling Progress for Large S-boxes.
- SAT/SMT Modeling Progress for S-boxes.
- **Fast SAT Models for Large S-boxes.**
- New Findings with the New SAT Models.
- Conclusion.

SHANDONG UNIVERSITY

Model 1: Trade-off Between Level of Simplification and Time

- ESPRESSO provides multiple options and commands for minimisation.
- These create a trade-off between simplification level and execution time.

SHANDONG UNIVERSITY

Model 1: Trade-off Between Level of Simplification and Time

- ESPRESSO provides multiple options and commands for minimisation.
- These create a trade-off between simplification level and execution time.
- Listed below are several options that may reduce the runtime.
  - `-efast` This option stops ESPRESSO after the first [`Expand`] and [`Irredundant Cover`] operations and prevents it from iterating over the solution.
  - `-eness` With this setting, essential prime implicants will not be identified.
  - `-enirr` With this option, the result will not necessarily be made irredundant in the last step which removes redundant literals.
  - `-eonset` This option recalculates the support of the input function prior to minimisation, which is advantageous when the canonical POS form includes a large number of maxterms.
- ESPRESSO is used to conduct the simplification of $f_{\langle 8,8,10\rangle}$ with the four options.
- The simplification is only accomplished with the option `-eonset`.
- There are 820 clauses in the output, and the total execution time is 3521.42 seconds.

SHANDONG UNIVERSITY

Model 2: Two-Step Encoding Method

- The complexity of simplification increases exponentially with the number of input variables.
- The main idea is dividing the encoding phase for an n-bit S-box into two steps.

SHANDONG UNIVERSITY

Model 2: Two-Step Encoding Method

- The complexity of simplification increases exponentially with the number of input variables.
- The main idea is dividing the encoding phase for an n-bit S-box into two steps.
- In addition to the auxiliary variables $\boldsymbol{u}$ and $\boldsymbol{v}$, we claim a set of *chaining variables* $\boldsymbol{z}$.
- 8-bit S-box $\mathcal{S}_8$ of `SKINNY-128` [Beierle *et al.* @ CRYPTO 2016]
  - $\{2^{-7}, 2^{-6}, 2^{-5.415}, 2^{-5}, 2^{-4.415}, 2^{-4}, 2^{-3.678}, 2^{-3.415}, 2^{-3.193}, 2^{-3}, 2^{-2.678}, 2^{-2.415}, 2^{-2}, 1\}$.

$x_0\ x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7$ — 8 variables for the input difference; $y_0\ y_1\ y_2\ y_3\ y_4\ y_5\ y_6\ y_7$ — 8 variables for the output difference; $u_0\ u_1\ u_2\ u_3\ u_4\ u_5\ u_6$ — 7 variables for integral; $v_0\ v_1\ v_2$ — 3 variables for decimal: 26-bit Boolean function

20-bit Boolean function

$x_0\ x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7$ — 8 variables for the input difference; $y_0\ y_1\ y_2\ y_3\ y_4\ y_5\ y_6\ y_7$ — 8 variables for the output difference; $z_0\ z_1\ z_2\ z_3$ — 4 chaining variables

Step 1

$$\mathcal{F}^{(1)}_{\langle 8,8,4\rangle} = \left\{ \boldsymbol{x}\|\boldsymbol{y}\|\boldsymbol{z} \;\middle|\; \begin{array}{l} \boldsymbol{x},\boldsymbol{y} \in \mathbb{F}_2^8, \boldsymbol{z} \in \mathbb{F}_2^4, \boldsymbol{x} \to \boldsymbol{y} \text{ is a possible propagation} \\ \boldsymbol{z} = \begin{cases} 1\|1\|0\|1, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-7} \\ 1\|1\|0\|0, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-6} \\ 1\|0\|1\|1, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-5.415} \\ 1\|0\|1\|0, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-5} \\ 1\|0\|0\|1, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-4.415} \\ 1\|0\|0\|0, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-4} \\ 0\|1\|1\|1, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-3.678} \\ 0\|1\|1\|0, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-3.415} \\ 0\|1\|0\|1, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-3.193} \\ 0\|1\|0\|0, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-3} \\ 0\|0\|1\|1, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-2.678} \\ 0\|0\|1\|0, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-2.415} \\ 0\|0\|0\|1, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-2} \\ 0\|0\|0\|0, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 1 \end{cases} \end{array} \right\}.$$

14-bit Boolean function

$z_0\ z_1\ z_2\ z_3$ — 4 chaining variables; $u_0\ u_1\ u_2\ u_3\ u_4\ u_5\ u_6$ — 7 variables for integral; $v_0\ v_1\ v_2$ — 3 variables for decimal

Step 2

$$\mathcal{F}^{(2)}_{\langle 4,10\rangle} = \left\{ \boldsymbol{z}\|\boldsymbol{u}\|\boldsymbol{v} \;\middle|\; \begin{array}{l} \boldsymbol{z} \in \mathbb{F}_2^4, \boldsymbol{u} \in \mathbb{F}_2^7, \boldsymbol{v} \in \mathbb{F}_2^3 \\ \boldsymbol{u}\|\boldsymbol{v} = \begin{cases} 1\|1\|1\|1\|1\|1\|0\|0\|0, & \text{if } \boldsymbol{z} = 1\|1\|0\|1 \\ 0\|1\|1\|1\|1\|1\|0\|0\|0, & \text{if } \boldsymbol{z} = 1\|1\|0\|0 \\ 0\|0\|1\|1\|1\|1\|0\|1\|0, & \text{if } \boldsymbol{z} = 1\|0\|1\|1 \\ 0\|0\|1\|1\|1\|1\|0\|0\|0, & \text{if } \boldsymbol{z} = 1\|0\|1\|0 \\ 0\|0\|0\|1\|1\|1\|0\|1\|0, & \text{if } \boldsymbol{z} = 1\|0\|0\|1 \\ 0\|0\|0\|1\|1\|1\|0\|0\|0, & \text{if } \boldsymbol{z} = 1\|0\|0\|0 \\ 0\|0\|0\|0\|1\|1\|1\|0\|0, & \text{if } \boldsymbol{z} = 0\|1\|1\|1 \\ 0\|0\|0\|0\|1\|1\|0\|1\|0, & \text{if } \boldsymbol{z} = 0\|1\|1\|0 \\ 0\|0\|0\|0\|1\|1\|0\|0\|1, & \text{if } \boldsymbol{z} = 0\|1\|0\|1 \\ 0\|0\|0\|0\|1\|1\|0\|0\|0, & \text{if } \boldsymbol{z} = 0\|1\|0\|0 \\ 0\|0\|0\|0\|0\|1\|1\|0\|0, & \text{if } \boldsymbol{z} = 0\|0\|1\|1 \\ 0\|0\|0\|0\|0\|1\|0\|1\|0, & \text{if } \boldsymbol{z} = 0\|0\|1\|0 \\ 0\|0\|0\|0\|0\|1\|0\|0\|0, & \text{if } \boldsymbol{z} = 0\|0\|0\|1 \\ 0\|0\|0\|0\|0\|0\|0\|0\|0, & \text{if } \boldsymbol{z} = 0\|0\|0\|0 \end{cases} \end{array} \right\}.$$

SHANDONG UNIVERSITY

Model 2: Two-Step Encoding Method

- The complexity of simplification increases exponentially with the number of input variables.
- The main idea is dividing the encoding phase for an n-bit S-box into two steps.
- In addition to the auxiliary variables $\boldsymbol{u}$ and $\boldsymbol{v}$, we claim a set of *chaining variables* $\boldsymbol{z}$.
- 8-bit S-box $\mathcal{S}_8$ of `SKINNY-128` [Beierle *et al.* @ CRYPTO 2016]
  - $\{2^{-7}, 2^{-6}, 2^{-5.415}, 2^{-5}, 2^{-4.415}, 2^{-4}, 2^{-3.678}, 2^{-3.415}, 2^{-3.193}, 2^{-3}, 2^{-2.678}, 2^{-2.415}, 2^{-2}, 1\}$.

$x_0\ x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7$ — 8 variables for the input difference; $y_0\ y_1\ y_2\ y_3\ y_4\ y_5\ y_6\ y_7$ — 8 variables for the output difference; $u_0\ u_1\ u_2\ u_3\ u_4\ u_5\ u_6$ — 7 variables for integral; $v_0\ v_1\ v_2$ — 3 variables for decimal. 26-bit Boolean function

20-bit Boolean function: $x_0\ x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7$ — 8 variables for the input difference; $y_0\ y_1\ y_2\ y_3\ y_4\ y_5\ y_6\ y_7$ — 8 variables for the output difference; $z_0\ z_1\ z_2\ z_3$ — 4 chaining variables

14-bit Boolean function: $z_0\ z_1\ z_2\ z_3$ — 4 chaining variables; $u_0\ u_1\ u_2\ u_3\ u_4\ u_5\ u_6$ — 7 variables for integral; $v_0\ v_1\ v_2$ — 3 variables for decimal

Step 1

$$\mathcal{F}^{(1)}_{\langle 8,8,4\rangle} = \left\{ \boldsymbol{x}\|\boldsymbol{y}\|\boldsymbol{z} \;\middle|\; \begin{array}{l} \boldsymbol{x},\boldsymbol{y} \in \mathbb{F}_2^8, \boldsymbol{z} \in \mathbb{F}_2^4, \boldsymbol{x} \to \boldsymbol{y} \text{ is a possible propagation} \\ \boldsymbol{z} = \begin{cases} 1\|1\|0\|1, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-7} \\ 1\|1\|0\|0, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-6} \\ 1\|0\|1\|1, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-5.415} \\ 1\|0\|1\|0, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-5} \\ 1\|0\|0\|1, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-4.415} \\ 1\|0\|0\|0, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-4} \\ 0\|1\|1\|1, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-3.678} \\ 0\|1\|1\|0, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-3.415} \\ 0\|1\|0\|1, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-3.193} \\ 0\|1\|0\|0, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-3} \\ 0\|0\|1\|1, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-2.678} \\ 0\|0\|1\|0, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-2.415} \\ 0\|0\|0\|1, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 2^{-2} \\ 0\|0\|0\|0, & \text{if } \Pr(\boldsymbol{x}\to\boldsymbol{y}) = 1 \end{cases} \end{array} \right\}.$$

Step 2

$$\mathcal{F}^{(2)}_{\langle 4,10\rangle} = \left\{ \boldsymbol{z}\|\boldsymbol{u}\|\boldsymbol{v} \;\middle|\; \begin{array}{l} \boldsymbol{z} \in \mathbb{F}_2^4, \boldsymbol{u} \in \mathbb{F}_2^7, \boldsymbol{v} \in \mathbb{F}_2^3 \\ \boldsymbol{u}\|\boldsymbol{v} = \begin{cases} 1\|1\|1\|1\|1\|1\|0\|0\|0, & \text{if } \boldsymbol{z} = 1\|1\|0\|1 \\ 0\|1\|1\|1\|1\|1\|0\|0\|0, & \text{if } \boldsymbol{z} = 1\|1\|0\|0 \\ 0\|0\|1\|1\|1\|1\|0\|1\|0, & \text{if } \boldsymbol{z} = 1\|0\|1\|1 \\ 0\|0\|1\|1\|1\|1\|0\|0\|0, & \text{if } \boldsymbol{z} = 1\|0\|1\|0 \\ 0\|0\|0\|1\|1\|1\|0\|1\|0, & \text{if } \boldsymbol{z} = 1\|0\|0\|1 \\ 0\|0\|0\|1\|1\|1\|0\|0\|0, & \text{if } \boldsymbol{z} = 1\|0\|0\|0 \\ 0\|0\|0\|0\|1\|1\|1\|0\|0, & \text{if } \boldsymbol{z} = 0\|1\|1\|1 \\ 0\|0\|0\|0\|1\|1\|0\|1\|0, & \text{if } \boldsymbol{z} = 0\|1\|1\|0 \\ 0\|0\|0\|0\|1\|1\|0\|0\|1, & \text{if } \boldsymbol{z} = 0\|1\|0\|1 \\ 0\|0\|0\|0\|1\|1\|0\|0\|0, & \text{if } \boldsymbol{z} = 0\|1\|0\|0 \\ 0\|0\|0\|0\|0\|1\|1\|0\|0, & \text{if } \boldsymbol{z} = 0\|0\|1\|1 \\ 0\|0\|0\|0\|0\|1\|0\|1\|0, & \text{if } \boldsymbol{z} = 0\|0\|1\|0 \\ 0\|0\|0\|0\|0\|1\|0\|0\|0, & \text{if } \boldsymbol{z} = 0\|0\|0\|1 \\ 0\|0\|0\|0\|0\|0\|0\|0\|0, & \text{if } \boldsymbol{z} = 0\|0\|0\|0 \end{cases} \end{array} \right\}.$$

Model 2: Two-Step Encoding Method - Application

Option	$f^{(1)}_{\langle 8,8,4\rangle}$		$f^{(2)}_{\langle 4,10\rangle}$	
	The number of clauses	Runtime	The number of clauses	Runtime
`Null`	757	87359.76s	30	1.39s
`-efast`	839	98018.76s	32	1.37s
`-eness`	757	95035.71s	30	1.46s
`-enirr`	757	92729.09s	30	1.4s
`-eonset`	757	98.83s	30	0.14s
`-estrong`	730	101050.85s	28	1.45s
`-Dexact`	-	>60 days	28	0.16s

`Null`: There is no option used in the implementation of ESPRESSO.

- The two-step encoding approach is still highly efficient when the total time is comprised of the simplifications for the two functions. (98.97s Vs 3521.42s)
- The amount of clauses for the two-step method is 787. (787 clauses Vs 820 clauses)

SHANDONG UNIVERSITY

Main Observation of Model 3

- The simplification of a large-scale function is not difficult if the number of clauses in the function is not excessively huge.

Fast SAT Models for Large S-boxes

Main Observation of Model 3

The simplification of a large-scale function is not difficult if the number of clauses in the function is not excessively huge.

Definition

- Given a set $\mathcal{X}$, a family of sets Ψ is a *partition* of $\mathcal{X}$ if and only if the following conditions are met.
  - The family Ψ does not contain the empty set.
  - $\mathcal{X}$ is equal to the union of the sets contained in Ψ .
  - In Ψ, the intersection of any two different sets is empty set.

SHANDONG UNIVERSITY

Main Observation of Model 3

The simplification of a large-scale function is not difficult if the number of clauses in the function is not excessively huge.

Definition

- Given a set $\mathcal{X}$, a family of sets Ψ is a *partition* of $\mathcal{X}$ if and only if the following conditions are met.
  - The family Ψ does not contain the empty set.
  - $\mathcal{X}$ is equal to the union of the sets contained in Ψ .
  - In Ψ, the intersection of any two different sets is empty set.

Model 3: Simplifying by Partition and Iteration

$$f(\boldsymbol{x}) = \bigwedge_{\boldsymbol{u}\in\overline{\mathrm{supp}(f)}} M_{\boldsymbol{u}}(\boldsymbol{x}) = \bigwedge_{i=0}^{\ell-1} \bigwedge_{\boldsymbol{u}\in\psi_i} M_{\boldsymbol{u}}(\boldsymbol{x}) = \bigwedge_{i=0}^{\ell-1} f_i(\boldsymbol{x}).$$

- $\Psi = \{\psi_0, \psi_1, \ldots, \psi_{\ell-1}\}$ is a partition of the set $\overline{\mathrm{supp}(f)}$.
- If a simplification $\tilde{f}_i$ can be found for each f_i, then $\bigwedge_{i=0}^{\ell-1} \tilde{f}_i$ yields a simplified form of f.

SHANDONG UNIVERSITY

General Method of Partition

- Quine-McCluskey technique: grouping clauses by the Hamming weight.
  - The simplification could be simpler if the clauses in a given set share as many bit values as possible.

Fast SAT Models for Large S-boxes

General Method of Partition

- Quine-McCluskey technique: grouping clauses by the Hamming weight.
  - The simplification could be simpler if the clauses in a given set share as many bit values as possible.
  - A partition of the set $\mathbb{F}_2^n$.
    - $\mathbb{F}_2^n[s|\mathring{x}]$, where $0 < s \leqslant n$ and $\mathring{x} \in \mathbb{F}_2^s$.

	s-bit							$(n-s)$-bit					
$\mathbb{F}_2^n[s\|0]$	0	0	0	$\cdots$	0	0	0	$*$	$*$	$\cdots$	$*$	$*$
$\mathbb{F}_2^n[s\|1]$	0	0	0	$\cdots$	0	0	1	$*$	$*$	$\cdots$	$*$	$*$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathbb{F}_2^n[s\|2^s-1]$	1	1	1	$\cdots$	1	1	1	$*$	$*$	$\cdots$	$*$	$*$

  - The family of sets $\Psi^n_{\langle s \rangle} = \left\{ \mathbb{F}_2^n[s|\mathring{x}] \mid \mathring{x} \in \mathbb{F}_2^s \right\}$ constitutes a partition of $\mathbb{F}_2^n$ with 2^s sets.

Fast SAT Models for Large S-boxes

SHANDONG UNIVERSITY

General Method of Partition

- Quine-McCluskey technique: grouping clauses by the Hamming weight.
  - The simplification could be simpler if the clauses in a given set share as many bit values as possible.
  - A partition of the set $\mathbb{F}_2^n$.
    - $\mathbb{F}_2^n[s|\mathring{x}]$, where $0 < s \leqslant n$ and $\mathring{x} \in \mathbb{F}_2^s$.

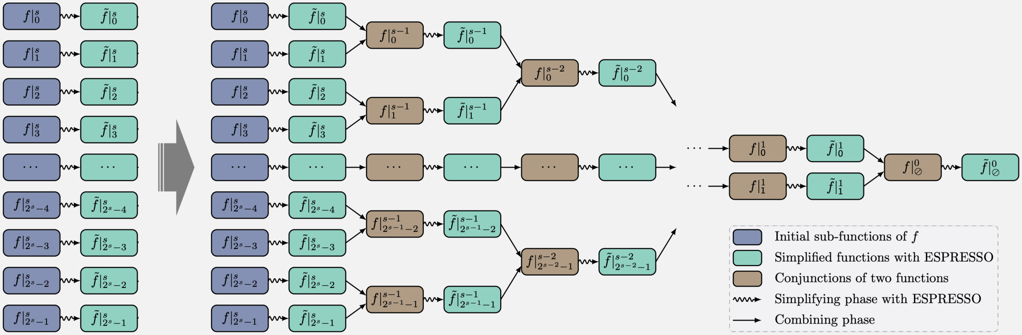
	s-bit							$(n-s)$-bit				
$\mathbb{F}_2^n[s\vert 0]$	0	0	0	$\cdots$	0	0	0	*	*	$\cdots$	*	*
$\mathbb{F}_2^n[s\vert 1]$	0	0	0	$\cdots$	0	0	1	*	*	$\cdots$	*	*
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathbb{F}_2^n[s\vert 2^s-1]$	1	1	1	$\cdots$	1	1	1	*	*	$\cdots$	*	*

    - The family of sets $\Psi_{\langle s\rangle}^n = \left\{\mathbb{F}_2^n[s|\mathring{x}] \mid \mathring{x} \in \mathbb{F}_2^s\right\}$ constitutes a partition of $\mathbb{F}_2^n$ with 2^s sets.
  - The partition $\Psi_{\langle s\rangle}^n$ restricted on the set $\Psi_{\langle s\rangle}^n \cap \overline{\mathrm{supp}(f)}$ turns into a partition of $\overline{\mathrm{supp}(f)}$.

SHANDONG UNIVERSITY

Iterative Simplification Method

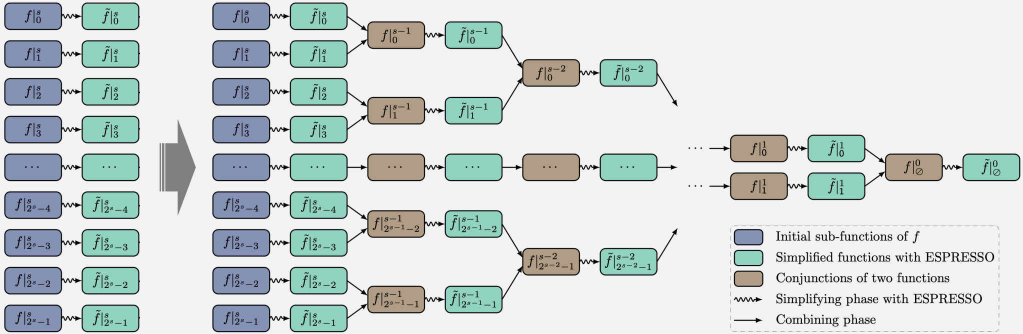
- The partition $\Psi^n_{\langle s \rangle}\big|_f$ permits the decomposition of the function f into 2^s sub-functions.
- The number of clauses in the simplified form with one time of simplification is typically quite high.



Fast SAT Models for Large S-boxes

Iterative Simplification Method

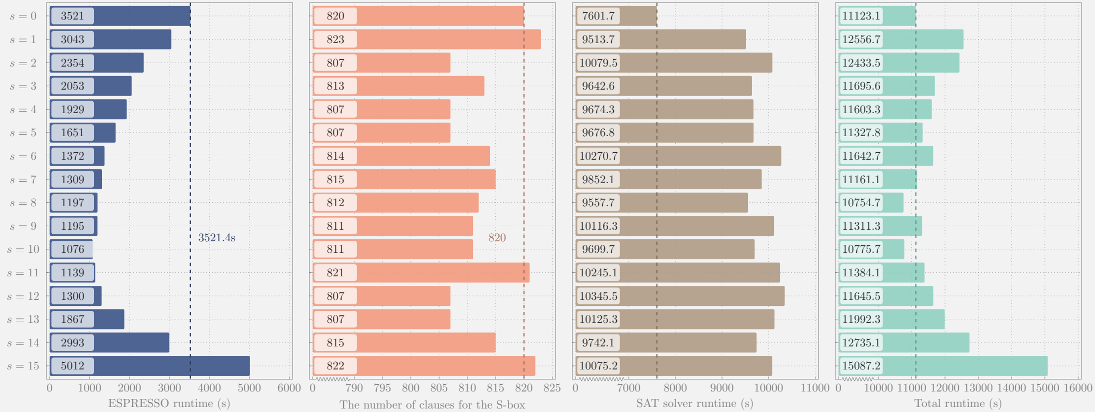
- The partition $\Psi^n_{\langle s\rangle}\big|_f$ permits the decomposition of the function f into 2^s sub-functions.
- The number of clauses in the simplified form with one time of simplification is typically quite high.



- It can be imaged that the level of simplification of the final output and the runtime are affected by the number of components 2^s in the initial partition $\Psi^n_{\langle s\rangle}\big|_f$.

Model 3: Simplifying by Partition and Iteration - Application

- Iterative simplification for the 26-bit Boolean function regarding $\mathcal{S}_8$ of `SKINNY-128`.

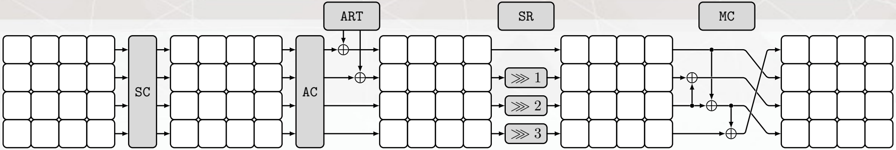


(a) Test results regarding the `-eonset` option.

Outline

- Motivation & Contributions.
- MILP Modeling Progress for Large S-boxes.
- SAT/SMT Modeling Progress for S-boxes.
- Fast SAT Models for Large S-boxes.
- **New Findings with the New SAT Models.**
- Conclusion.

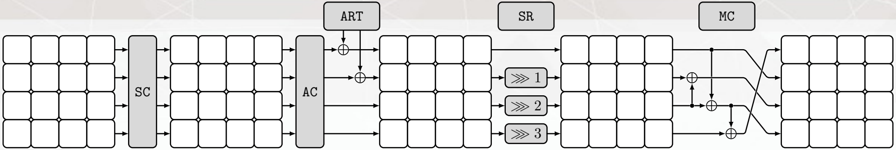
Tight Probability Bound for 14 Rounds of SKINNY-128



Previous Results [Beierle *et al.* @ CRYPTO 2016, Abdelkhalek *et al.* @ FSE 2018]

- The designers of SKINNY-128 gave only lower bounds for the number of differential active S-boxes.
- Abdelkhalek *et al.* attempted to get tight upper bounds for the probability with MILP model.
  - The task was completed up to 13 rounds, and the search on 13 rounds took 16 days.
  - For 14-round, they merely demonstrated that no characteristic had a probability greater than 2^{-128}.

Tight Probability Bound for 14 Rounds of SKINNY-128



Previous Results [Beierle *et al.* @ CRYPTO 2016, Abdelkhalek *et al.* @ FSE 2018]

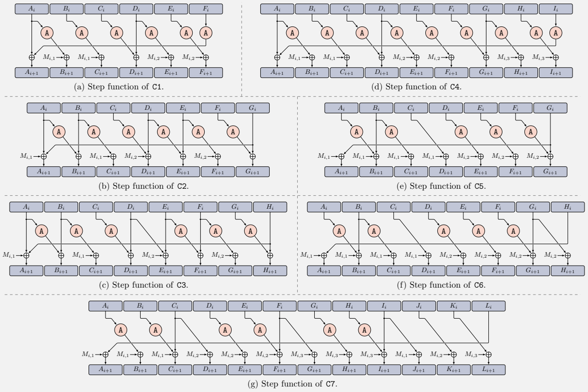
- The designers of SKINNY-128 gave only lower bounds for the number of differential active S-boxes.
- Abdelkhalek *et al.* attempted to get tight upper bounds for the probability with MILP model.
  - The task was completed up to 13 rounds, and the search on 13 rounds took 16 days.
  - For 14-round, they merely demonstrated that no characteristic had a probability greater than 2^{-128}.

New Finding for SKINNY-128

Round	1	2	3	4	5	6	7
$-\log_2(p)$	2	4	10	16	24	32	52
Round	8	9	10	11	12	13	14
$-\log_2(p)$	72	86	96	104	112	123	131

AES-Based Constructions

- [Jean and Nikolić @ FSE 2016] suggested seven AES-based constructions.
- These constructions can be utilised as building blocks for MAC and AE.
- The security is determined by the number of active S-boxes required to create an internal collision.



(a) Step function of C1.
(d) Step function of C4.
(b) Step function of C2.
(e) Step function of C5.
(c) Step function of C3.
(f) Step function of C6.
(g) Step function of C7.

SHANDONG UNIVERSITY

New Findings for AES-Based Constructions

C1		C2		C3		C4		C5		C6		C7		Ref.
n_s	#S	n_s	#S	n_s	#S	n_s	#S	n_s	#S	n_s	#S	n_s	#S	
-	22	-	25	-	34	-	25	-	22	-	23	-	25	FSE 2016
3-7	22	-	-	-	-	-	-	4-7	24	-	-	-	-	FSE 2018
2	✗	2	✗	2	✗	2	✗	2	✗	2	✗	2	48	Our results
3	22	3	50	3	47	3	33	3	40	3	48	3	48	
4	22	4	25	4	47	4	25	4	25	4	> 41	4	> 37	
5	22	5	25	5	36	5	25	5	25	5	23	5	28	
6	22	6	25	6	36	6	25	6	25	6	23	6	28	
7	22	7	25	7	36	7	25	7	25	7	23	7	> 24	
8	22	8	25	8	36	8	25	8	25	8	23	8	> 24	

n_s: The number of step functions. #S: The number of active S-boxes. -: No information is provided.

✗: There is no differential characteristic with the specified number of step functions.

Outline

SHANDONG UNIVERSITY

Contribution

- Three strategies to create SAT models for large S-boxes are proposed.
  - ① Utilising the option of the ESPRESSO logic minimizer.
  - ② Dividing the description of a big S-box into two steps.
  - ③ Simplifying by partitioning method.
- Upper bound on the differential probability for 14 rounds of SKINNY-128 is determined.
- Related-key differential properties of both versions of PIPO are investigated.
- Seven AES-based constructions C1 - C7 devised by Jean and Nikolić are analysed.

Thank you for your attention!

Thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the paper.