Overview

This work focuses on traditional/conventional bit-based (2-subset) division property [Tod15].

Contributions

1. New insights on the theory:
   - close links of div. prop. propagation with the function’s graph
   - new compact representation, suitable for modeling (CNF/MILP/etc.)

---

1. (EUROCRYPT’15) Yosuke Todo. Structural evaluation by generalized integral property
2. (ToSC’20) Derbez, Fouque. Increasing precision of division property
Overview

This work focuses on traditional/conventional bit-based (2-subset) division property [Tod15]

Contributions

1. New insights on the theory:
   - close links of div. prop. propagation with the function’s graph
   - new compact representation, suitable for modeling (CNF/MILP/etc.)

2. New algorithms: DPPT/compact repr. in $O(n2^n)$, even less for “heavy” S-boxes

1 (EUROCRYPT’15) Yosuke Todo. Structural evaluation by generalized integral property
2 (ToSC’20) Derbez, Fouque. Increasing precision of division property
Overview

This work focuses on traditional/conventional bit-based (2-subset) division property [Tod15]¹

Contributions

1. New insights on the theory:
   - close links of div. prop. propagation with the function’s graph
   - new compact representation, suitable for modeling (CNF/MILP/etc.)

2. New algorithms: DPPT/compact repr. in $O(n2^n)$, even less for “heavy” S-boxes

3. Application to LED: Super-Sbox model does not yield 8-round distinguishers (Q unsolved by [DF20]²)

¹(EUROCRYPT’15) Yosuke Todo. Structural evaluation by generalized integral property
²(ToSC’20) Derbez, Fouque. Increasing precision of division property
Plan

1 Introduction
   - Division property
   - Monotonicity and convexity on $\mathbb{F}_2^n$
   - Parity sets: formalization of division property

2 New insights
   - New characterizations of transitions
   - Compact representation
   - Completeness and the symmetry of the division core
   - Convexity of minimal transitions

3 Algorithms

4 Application to LED
Division property
Division property

\[ x_0 x_1 x_2 \]

\[ \begin{array}{c}
 F_0 \quad k_0 \\
 F_1 \quad k_1 \\
 F_2 \quad k_2 \\
\end{array} \]

\[ x_0 x_1 x_2 \quad ? \quad y_0 \]
Division property
Monotonicity and convexity on $\mathbb{F}_2^n$ - definitions

- partial order on $\mathbb{F}_2^n$: $u \preceq v$ iff $\forall i \ u_i \leq v_i$
Monotonicity and convexity on $\mathbb{F}_2^n$ - definitions

- **Partial order** on $\mathbb{F}_2^n$: $u \preceq v$ iff $\forall i \ u_i \leq v_i$

- **Lower set:** $u \notin X \not\preceq v \in X$

![Diagram showing the partial order and lower set on $\mathbb{F}_2^n$]
Monotonicity and convexity on $\mathbb{F}_2^n$ - definitions

- **partial order** on $\mathbb{F}_2^n$: $u \preceq v$ iff $\forall i \ u_i \leq v_i$

- **lower set**: $u \notin X \Rightarrow v \in X$

- **upper set**: $u \in X \Rightarrow v \notin X$

**Convex set**: lower set $\cap$ upper set (two-sided bound)
Monotonicity and convexity on $\mathbb{F}_2^n$ - definitions

- **Partial order** on $\mathbb{F}_2^n$: 
  $u \preceq v$ iff $\forall i \ u_i \leq v_i$

- **Lower set**: $u \not\in X \preceq v \in X$

- **Upper set**: $u \in X \not\preceq v \not\in X$

- **Extreme elements** (resp. maximal/minimal)
  form a compact representation:
  $\{**11, 111*\}$
Monotonicity and convexity on $\mathbb{F}_2^n$ - definitions

- **partial order** on $\mathbb{F}_2^n$:
  \[ u \preceq v \text{ iff } \forall i \ u_i \leq v_i \]

- lower set: \( u \notin X \preceq v \in X \)

- upper set: \( u \in X \preceq v \notin X \)

- **extreme elements**
  (resp. maximal/minimal)
  form a compact representation:
  \[
  \{**11, 111*\}
  \{0***, **00\}
  \]
Monotonicity and convexity on $\mathbb{F}_2^n$ - definitions

- **partial order** on $\mathbb{F}_2^n$: 
  $u \preceq v$ iff $\forall i \ u_i \leq v_i$

- lower set: $u \notin X \preceq v \in X$

- upper set: $u \in X \preceq v \notin X$

- extreme elements
  (resp. maximal/minimal)
  form a **compact** representation:
  $\{**11, 111*\}$
  $\{0***, **00\}$

- (resp. upper and lower bounds)
Monotonicity and convexity on $\mathbb{F}_2^n$ - definitions

- **Partial order** on $\mathbb{F}_2^n$:
  \[ u \preceq v \text{ iff } \forall i \ u_i \leq v_i \]

- **Lower set**: \( u \notin X \preceq v \in X \)

- **Upper set**: \( u \in X \preceq v \notin X \)

- **Extreme elements** (resp. maximal/minimal)
  form a compact representation:
  \[ \{**11, 111*\} \]
  \[ \{0***, **00\} \]

- **Convex set**: lower set $\cap$ upper set
  (two-sided bound)
Monotonicity and convexity on $\mathbb{F}_2^n$ - modeling upper/lower sets

modeling an upper set $X \subseteq \mathbb{F}_2^n$:
Monotonicity and convexity on $\mathbb{F}_2^n$ - modeling upper/lower sets

modeling an upper set $X \subseteq \mathbb{F}_2^n$:

- monotone DNF (from the min-set):

$$(x_2 \land x_3) \lor (x_0 \land x_1 \land x_2)$$

- weight 4
  
  - 1111
  
  - 0111, 1011, 1101, 1110

- weight 3
  
  - 0110, 1100
  
  - 0101, 1010
  
  - 0100, 1001
  
  - 0011, 1110

- weight 2
  
  - 0010, 1001
  
  - 0100, 1010
  
  - 0011, 1110

- weight 1
  
  - 0001, 0100, 1000

- weight 0
  
  - 0000
Monotonicity and convexity on $\mathbb{F}_2^n$ - modeling upper/lower sets

modeling an **upper** set $X \subseteq \mathbb{F}_2^n$:

- monotone DNF (from the min-set):
  $$(x_2 \land x_3) \lor (x_0 \land x_1 \land x_2)$$
  0011 1110

- monotone CNF (from the max-set of the complement):
  $$(x_0 \lor x_3) \land (x_2) \land (x_1 \lor x_3)$$
  0110 1101 1010
Monotonicity and convexity on $\mathbb{F}_2^n$ - modeling upper/lower sets

modeling an upper set $X \subseteq \mathbb{F}_2^n$:
- monotone DNF (from the min-set):
  \[
  (x_2 \land x_3) \lor (x_0 \land x_1 \land x_2)
  \]
- monotone CNF (from the max-set of the complement):
  \[
  (x_0 \lor x_3) \land (x_2) \land (x_1 \lor x_3)
  \]

note: CNF-DNF size gap can be exponential!
Monotonicity and convexity on $\mathbb{F}_2^n$ - modeling convex sets

modeling an convex set $X \subseteq \mathbb{F}_2^n$: 

weight 4

weight 3

weight 2

weight 1

weight 0
Monotonicity and convexity on $\mathbb{F}_2^n$ - modeling convex sets

modeling an convex set $X \subseteq \mathbb{F}_2^n$:

- combined CNF

  of the upper/lower bounds:

\[
(\neg x_0 \lor \neg x_3) \land (\neg x_0 \lor \neg x_2) \land (x_1 \lor x_3)
\]
Parity sets: formalization of division property

Definition ([BC16])
Let $X \subseteq \mathbb{F}_2^n$. Define

$$\text{ParitySet}(X) = \left\{ u \in \mathbb{F}_2^n \mid \bigoplus_{x \in X} x^u = 1 \right\}$$
Parity sets: formalization of division property

Definition ([BC16])

Let $X \subseteq \mathbb{F}_2^n$. Define

\[
\text{ParitySet}(X) = \left\{ u \in \mathbb{F}_2^n \mid \bigoplus_{x \in X} x^u = 1 \right\}
\]

Definition ([Tod15])

$X$ satisfies division property $K \subseteq \mathbb{F}_2^n$ if

\[
\text{ParitySet}(X) \subseteq \text{UpperClosure}(K)
\]

(i.e., ParitySet($X$) is lower bounded by $K$)
Parity sets: formalization of division property

Definition ([BC16])

Let \( X \subseteq \mathbb{F}_2^n \). Define

\[
\text{ParitySet}(X) = \left\{ u \in \mathbb{F}_2^n \mid \bigoplus_{x \in X} x^u = 1 \right\}
\]

Definition ([Tod15])

\( X \) satisfies division property \( K \subseteq \mathbb{F}_2^n \) if

\[
\text{ParitySet}(X) \subseteq \text{UpperClosure}(K)
\]

(i.e., \( \text{ParitySet}(X) \) is lower bounded by \( K \))

Proposition

\[
u \in \text{ParitySet}(X) \text{ if and only if the ANF of } 1 \mathbf{^X} \text{ contains } x^{\sim u}
\]

\( \Rightarrow \) parity set is equivalent to the indicator’s ANF up to negations!
Parity sets: formalization of division property

Definition ([BC16])

Let \( X \subseteq \mathbb{F}_2^n \). Define

\[
\text{ParitySet}(X) = \left\{ u \in \mathbb{F}_2^n \mid \bigoplus_{x \in X} x^u = 1 \right\}
\]

Definition ([Tod15])

\( X \) satisfies division property \( K \subseteq \mathbb{F}_2^n \) if

\[
\text{ParitySet}(X) \subseteq \text{UpperClosure}(K)
\]

(i.e., \( \text{ParitySet}(X) \) is lower bounded by \( K \))

Proposition

\[
u \in \text{ParitySet}(X) \text{ if and only if } \exists \text{ ANF of } 1 \neg X \text{ contains } x^{\neg u}
\]

\( \Rightarrow \) parity set is equivalent to the indicator’s ANF up to negations!

The takeaway

\( \Rightarrow \) division property of a set defines upper bounds on monomials in the indicator’s ANF
**Proposition (Propagation rule)**

Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$, $u \in \mathbb{F}_2^n$, $v \in \mathbb{F}_2^m$. If $F^v(x)$ contains monomial $x^{u'}$ for some $v' \preceq v$, $u' \succeq u$, then $u \xrightarrow{F} v$ is a valid division property transition through $F$. 
**Proposition (Propagation rule)**

Let \( F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m, u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m \). If \( F^{v'}(x) \) contains monomial \( x^{u'} \) for some \( v' \preceq v, u' \succeq u \), then \( u \xrightarrow{F} v \) is a valid division property transition through \( F \).

For example, \( z_1 = (F_0(x))_1 \) contains \( x_0x_1x_2x_5 \).
Plan

1. Introduction
   - Division property
   - Monotonicity and convexity on $\mathbb{F}_2^n$
   - Parity sets: formalization of division property

2. New insights
   - New characterizations of transitions
   - Compact representation
   - Completeness and the symmetry of the division core
   - Convexity of minimal transitions

3. Algorithms

4. Application to LED
New characterizations of transitions

Definition

The graph of $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ is defined as

$$\Gamma_F = \{(x, y) \mid y = F(x)\} \quad (|\Gamma_F| = 2^n)$$

Theorem

The following statements are equivalent:

1. Transition $u \xrightarrow{F} v$ is valid
2. $(\neg u, v)$ belongs to the division property of $\Gamma_F$ (i.e., $\text{UpperClosure}(\text{ParitySet}(\Gamma_F))$
3. The graph indicator of $F$ contains a monomial multiple of $x^u y^\neg v$ (links to [Car20] 3)

---

3 ([IEEE TIT 2020] Carlet. Graph indicators of vectorial functions and bounds on the algebraic degree of composite functions.)
New characterizations of transitions

Definition
The graph of \( F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m \) is defined as
\[
\Gamma_F = \{(x, y) \mid y = F(x)\} \quad (|\Gamma_F| = 2^n)
\]

Theorem
The following statements are equivalent:
1. transition \( u \xrightarrow{F} v \) is valid
2. \((\neg u, v)\) belongs to the division property of \( \Gamma_F \) (i.e., \( \text{UpperClosure}(\text{ParitySet}(\Gamma_F)) \))
3. the graph indicator of \( F \) contains a monomial multiple of \( x^u y^{\neg v} \) (links to [Car20])

\( ^3 \) (IEEE TIT 2020) Carlet. Graph indicators of vectorial functions and bounds on the algebraic degree of composite functions.
Compact representation

**Definition**

Define the **division core** of $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ as

$$\text{DivCore}(F) = \text{MinSet}(\text{ParitySet}(\Gamma_F))$$

i.e., the division property of $\Gamma_F$

Equivalently:

- $\text{DivCore}(F) = \left\{ (-u, \nu) \mid u \xrightarrow{F} \nu, u \text{ is maximal, } \nu \text{ is minimal} \right\}$
- $\text{DivCore}(F) = \left\{ (-u, -\nu) \mid x^u y^\nu \text{ is a maximal monomial in the ANF of } \Gamma_F \right\}$

Classic propagation of division property focuses on minimal/reduced transitions $u \xrightarrow{F} \min. \nu$, which only require that $\nu$ is minimal.

DivCore in addition requires that $u$ is maximal.
Define the division core of $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ as

$$\text{DivCore}(F) = \text{MinSet}(\text{ParitySet}(\Gamma_F))$$

i.e., the division property of $\Gamma_F$

Equivalently:

- $\text{DivCore}(F) = \{- (u, v) \mid u \overset{F}{\rightarrow} v, u \text{ is maximal, } v \text{ is minimal}\}$
- $\text{DivCore}(F) = \{(-u, -v) \mid x^u y^v \text{ is a maximal monomial in the ANF of } \Gamma_F\}$

- Classic propagation of division property focuses on minimal/reduced transitions $u \overset{F}{\rightarrow}_{\text{min.}} v$, which only require that $v$ is minimal.
- DivCore in addition requires that $u$ is maximal.
Completeness and the symmetry of the division core

All sets of transitions, both for $F$ and $F^{-1}$ can be derived from $\text{DivCore}(F)$:

**Theorem**

Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$. Then,

1. $u \xrightarrow{F} v \iff (-u, v) \in \text{UpperClosure}(\text{DivCore}(F))$
2. $u \xrightarrow{\text{min.}} v \iff (-u, v) \in \text{MinSet}_v(\text{UpperClosure}(\text{DivCore}(F)))$

If, in addition, $n = m$ and $F$ is bijective:

4. $v \xrightarrow{F^{-1}} u \iff (u, -v) \in \text{UpperClosure}(\text{DivCore}(F))$
5. $v \xrightarrow{\text{min.}} u \iff (u, -v) \in \text{MinSet}_u(\text{UpperClosure}(\text{DivCore}(F)))$
Convexity of minimal transitions

Modeling:

- removing invalid transitions is sufficient
- however, removing redundant transitions aids solvers
- ⇒ modeling a convex set (e.g. removing monotone invalid and redundant sets)

Partition of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ into transition classes

$\neg u \xrightarrow{F} v$
Convexity of minimal transitions

Modeling:
- removing invalid transitions is sufficient
- however, removing redundant transitions aids solvers
  ⇒ modeling a convex set (e.g. removing monotone invalid and redundant sets)
- alternative: removing above upper bound, often is more compact

partition of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ into transition classes
$\neg u \xrightarrow{F} v$
Convexity of minimal transitions

Modeling:
- removing invalid transitions is sufficient
- however, removing redundant transitions aids solvers
  \[ \Rightarrow \text{modeling a convex set (e.g. removing monotone invalid and redundant sets)} \]
- alternative: removing above upper bound, often is more compact
- all the relevant sets can be computed from \text{DivCore}

\[
\text{partition of } \mathbb{F}_2^n \times \mathbb{F}_2^m \text{ into transition classes}
\neg u \xrightarrow{F} v
\]
Model sizes for some (Super)S-boxes

### Modeling only minimal transitions: (convex)

<table>
<thead>
<tr>
<th>function</th>
<th>n</th>
<th>#min.trans.</th>
<th>CNF (our)</th>
<th>CNF (optimal)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>8</td>
<td>2001</td>
<td>361</td>
<td>234</td>
</tr>
<tr>
<td>Misty S7</td>
<td>7</td>
<td>1779</td>
<td>1363</td>
<td>607</td>
</tr>
<tr>
<td>Misty S9</td>
<td>9</td>
<td>27626</td>
<td>21988</td>
<td>10403-11819</td>
</tr>
</tbody>
</table>

### Modeling valid transitions: (upper)

<table>
<thead>
<tr>
<th>function</th>
<th>n</th>
<th>#min.trans.</th>
<th>CNF (our)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Midori-64 Super-Sbox (all keys)</td>
<td>16</td>
<td>14714723</td>
<td>1912088</td>
</tr>
<tr>
<td>LED Super-Sbox (all keys)</td>
<td>16</td>
<td>8458909</td>
<td>319606</td>
</tr>
<tr>
<td>LED MixColumn (linear)</td>
<td>16</td>
<td>177643913</td>
<td>33412</td>
</tr>
<tr>
<td>Randomly gen. 32-bit S-box</td>
<td>32</td>
<td>?</td>
<td>2958</td>
</tr>
</tbody>
</table>
Plan

1 Introduction
   ■ Division property
   ■ Monotonicity and convexity on $\mathbb{F}_2^n$
   ■ Parity sets: formalization of division property

2 New insights
   ■ New characterizations of transitions
   ■ Compact representation
   ■ Completeness and the symmetry of the division core
   ■ Convexity of minimal transitions

3 Algorithms

4 Application to LED
Algorithmic framework

\[
\text{function } \text{Transform}_f(X \in \mathbb{F}_2^{2^n}) \quad \triangleright \text{ Complexity: } O(n2^n)
\]

\[
\text{for all } i \in \{0, \ldots, n - 1\} \text{ do}
\]

\[
\text{for all } j \in \{0, \ldots, 2^n - 1\}, \text{ s.t. } j \text{ has } (n - 1 - i)\text{-th bit set do}
\]

\[
(X_{j-2^i}, X_j) \leftarrow f(X_{j-2^i}, X_j)
\]
Algorithmic framework

function \( \text{Transform}_f(X \in \mathbb{F}_2^n) \)

\[
\text{for all } i \in \{0, \ldots, n - 1\} \text{ do}
\]

\[
\text{for all } j \in \{0, \ldots, 2^n - 1\}, \text{ s.t. } j \text{ has } (n - 1 - i)\text{-th bit set do}
\]

\[
(X_{j-2^i}, X_j) \leftarrow f(X_{j-2^i}, X_j)
\]

function \( f(a, b) \) effect of \( \text{Transform}_f \)

| XOR-up       | \((a, b \oplus a)\) | compute ANF (involution) | Complexity: \( O(n2^n) \) |
Algorithmic framework

$$\text{function } \text{Transform}_f(X \in \mathbb{F}_2^n)$$

$$\text{for all } i \in \{0, \ldots, n-1\} \text{ do}$$

$$\text{for all } j \in \{0, \ldots, 2^n - 1\}, \text{ s.t. } j \text{ has } (n - 1 - i)\text{-th bit set } \text{do}$$

$$(X_{j-2^i}, X_j) \leftarrow f(X_{j-2^i}, X_j)$$

$$\text{function } f$$

$$f(a, b)$$

$$\text{effect of } \text{Transform}_f$$

<table>
<thead>
<tr>
<th>Function</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>XOR-up</td>
<td>$a, b \oplus a$</td>
</tr>
<tr>
<td>XOR-down</td>
<td>$(a \oplus b, b)$</td>
</tr>
</tbody>
</table>

compute ANF (involution)

compute ParitySet (involution)
Algorithmic framework

function \text{Transform}_f(X \in \mathbb{F}_2^{2^n})\quad \triangleright \text{Complexity: } O(n2^n)

for all \(i \in \{0, \ldots, n - 1\}\) do

\hspace{1em} for all \(j \in \{0, \ldots, 2^n - 1\}\), s.t. \(j\) has \((n - 1 - i)\)-th bit set do

\hspace{2em} \(X_{j-2i}, X_j\) \leftarrow f(X_{j-2i}, X_j)

function \(f\)\hspace{2em} f(a, b) \hspace{2em} \text{effect of } \text{Transform}_f

\begin{tabular}{|l|l|l|}
\hline
XOR-up & \(a, b \oplus a\) & compute ANF (involution) \\
XOR-down & \(a \oplus b, b\) & compute ParitySet (involution) \\
OR-up & \(a, b \lor a\) & compute UpperClosure \\
OR-down & \(a \lor b, b\) & compute LowerClosure \\
\hline
\end{tabular}
Algorithmic framework

\textbf{function} \text{Transform}_f(X \in \mathbb{F}_2^n) \quad \triangleright \text{Complexity: } O(n2^n)

\begin{align*}
\text{for all } i \in \{0, \ldots, n-1\} \text{ do} \\
\quad \text{for all } j \in \{0, \ldots, 2^n - 1\}, \text{ s.t. } j \text{ has } (n-1-i)\text{-th bit set} \text{ do} \\
\quad \quad (X_{j-2^i}, X_j) \leftarrow f(X_{j-2^i}, X_j)
\end{align*}

\begin{tabular}{lll}
\textbf{function} & \textbf{Effect} & \textbf{Effect of} \\
\hline
XOR-up & \(a, b \oplus a\) & \text{compute ANF (involution)} \\
XOR-down & \(a \oplus b, b\) & \text{compute ParitySet (involution)} \\
OR-up & \(a, b \lor a\) & \text{compute UpperClosure} \\
OR-down & \(a \lor b, b\) & \text{compute LowerClosure} \\
LESS-up & \(a, b \land \neg a\) & \text{compute MinSet (after TransformOR-up)} \\
MORE-down & \(a \land \neg b, b\) & \text{compute MaxSet (after TransformOR-down)}
\end{tabular}
Algorithmic framework

**function** Transform\(_f(X \in \mathbb{F}_2^n)\) \hspace{1cm} ▷ Complexity: \(O(n2^n)\)

for all \(i \in \{0, \ldots, n - 1\}\) do

for all \(j \in \{0, \ldots, 2^n - 1\}\), s.t. \(j\) has \((n - 1 - i)\)-th bit set do

\((X_{j-2i}, X_j) \leftarrow f(X_{j-2i}, X_j)\)

**function** MinDPPT\((F : \mathbb{F}_2^n \to \mathbb{F}_2^m : \text{a lookup table}) \hspace{1cm} ▷ Complexity: O((n + m)2^{n+m})\)

\(D \leftarrow \text{indicator vector of } \Gamma_F (\in \mathbb{F}_2^{2^n+m})\)

\(D \leftarrow \text{Transform}_{\text{XOR-down}}(D)\)

\(D \leftarrow \text{Transform}_{\text{OR-up}}(D)\)

\(D \leftarrow \text{Transform}_{\text{LESS-up}}(D), \text{ only with } i < n \text{ in the first loop}\)

return \(\{(\neg u, v) \mid (u, v) \in D\}\)
Algorithmic framework

\textbf{function} \ Transform_f(X \in \mathbb{F}_2^n) \quad \triangleright \text{ Complexity: } O(n2^n)

\textbf{for all} i \in \{0, \ldots, n-1\} \ \textbf{do}

\textbf{for all} j \in \{0, \ldots, 2^n - 1\}, \text{ s.t. } j \text{ has } (n-1-i)\text{-th bit set} \ \textbf{do}

\hspace{1cm} (X_{j-2^i}, X_j) \leftarrow f(X_{j-2^i}, X_j)

\textbf{function} \ \text{MinDPPT}(F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m : \text{a lookup table}) \quad \triangleright \text{ Complexity: } O((n + m)2^{n+m})

\hspace{1cm} D \leftarrow \text{indicator vector of } \Gamma_F (\in \mathbb{F}_2^{2^n+m})

\hspace{1cm} D \leftarrow \text{Transform\text{\_}XOR\text{-down}}(D)

\hspace{1cm} D \leftarrow \text{Transform\text{\_}OR\text{-up}}(D)

\hspace{1cm} D \leftarrow \text{Transform\text{\_}LESS\text{-up}}(D), \text{ only with } i < n \text{ in the first loop}

\textbf{return} \ \{(\neg u, v) \mid (u, v) \in D\}

DPPT, DivCore, etc. for \(F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n\) in \(O(n2^n)\)
Plan

1. Introduction
   - Division property
   - Monotonicity and convexity on $\mathbb{F}_2^n$
   - Parity sets: formalization of division property

2. New insights
   - New characterizations of transitions
   - Compact representation
   - Completeness and the symmetry of the division core
   - Convexity of minimal transitions

3. Algorithms

4. Application to LED
Integral distinguishers for LED

- LED [GPPR11] is a lightweight 64-bit block cipher
- Best integral distinguisher is on 7 rounds due to [HWW20]⁴, using an SMT solver on S-box model with precise model for the linear layer.

---

⁵(ToSC’20) Derbez, Fouque. Increasing precision of division property.
Integral distinguishers for LED

- LED [GPPR11] is a lightweight 64-bit block cipher.
- Best integral distinguisher is on 7 rounds due to [HWW20]⁴, using an SMT solver on S-box model with precise model for the linear layer.
- [DF20]⁵ applied ad-hoc division property search on Super-Sbox models with linear combinations of Midori, SKINNY, and HIGHT, but for LED the running time was not reasonable.
- The hardness lies in the complex MixColumns (MDS) layer of LED, which creates a lot of transitions (177M).

---

⁵(ToSC’20) Derbez, Fouque. Increasing precision of division property.
Application to LED

With our compact modeling:

- one MixColumn can be modeled by <40k CNF clauses (vs 177M minimal transitions)
- one Super-Sbox can be modeled by <400k CNF clauses (vs 8.5M minimal transitions)
- using Kissat solver, the Super-Sbox model with linear combinations of 8-round LED can be solved in about 1 minute

...exhausting all linear combinations showed NO integral distinguishers...

existence of 8-round integral distinguisher for LED remains open, but one has to go beyond the Super-Sbox model or use perfect variants of division property to progress
Application to LED

With our compact modeling:

- one MixColumn can be modeled by <40k CNF clauses (vs 177M minimal transitions)
- one Super-Sbox can be modeled by <400k CNF clauses (vs 8.5M minimal transitions)
- using Kissat solver, the Super-Sbox model with linear combinations of 8-round LED can be solved in about 1 minute
- exhausting all linear combinations showed NO integral distinguishers...
- existence of 8-round integral distinguisher for LED remains open, but one has to go beyond the Super-Sbox model or use perfect variants of division property to progress
An example LED trail

\( \alpha, x \rightarrow \beta, x \)

<table>
<thead>
<tr>
<th>( (\alpha, x) )</th>
<th>SuperSbox</th>
<th>( \alpha, x )</th>
<th>SuperSbox</th>
<th>( (\beta, x) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1111 1111 1111</td>
<td>1111 1111 1111 1111</td>
<td>1111 1011 1111 1101</td>
<td>0100 0011 1000 1000</td>
<td>0001 1111 0100 1111</td>
</tr>
<tr>
<td>1111 1111 1111</td>
<td>1111 1111 1111 1111</td>
<td>1111 1111 1111 1111</td>
<td>1111 0001 0100 1010</td>
<td>1111 1111 0110 0100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( (\alpha, x) )</th>
<th>SuperSbox</th>
<th>( \alpha, x )</th>
<th>SuperSbox</th>
<th>( (\beta, x) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000 0000 1111 0000</td>
<td>0000 0000 0100 0000</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
</tr>
<tr>
<td>0111 1011 0000 0011</td>
<td>1010 0000 0000 0100</td>
<td>0000 0000 0000 0000</td>
<td>1011 0000 0000 0000</td>
<td>0111 0000 0000 0000</td>
</tr>
<tr>
<td>1011 1101 1010 1101</td>
<td>0000 0000 0000 0000</td>
<td>0000 0010 0010 0000</td>
<td>0111 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
</tr>
<tr>
<td>0011 1101 0111 0111</td>
<td>0000 0000 0000 0000</td>
<td>0111 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
</tr>
</tbody>
</table>

For practice, \( \approx 30 \) trails are sufficient to cover all \((u, v)\) pairs (per each of the input/output Super-Sbox positions).
An example LED trail

<table>
<thead>
<tr>
<th>$\alpha$</th>
<th>$\beta$</th>
<th>$u_\alpha$</th>
<th>$v_\beta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1111</td>
<td>1111</td>
<td>0000</td>
<td>0000</td>
</tr>
<tr>
<td>1111</td>
<td>1111</td>
<td>0100</td>
<td>0000</td>
</tr>
<tr>
<td>1111</td>
<td>1111</td>
<td>0100</td>
<td>0000</td>
</tr>
<tr>
<td>1111</td>
<td>1111</td>
<td>0100</td>
<td>0000</td>
</tr>
</tbody>
</table>

255 columns $u_\alpha$ to cover all possible $\alpha \neq 0$

255 columns $v_\beta$ to cover all possible $\beta \neq 0$
An example LED trail

255 columns \( u_\alpha \) to cover all possible \( \alpha \neq 0 \)
255 columns \( v_\beta \) to cover all possible \( \beta \neq 0 \)

on practice, \( \approx 30 \) trails are sufficient to cover all \((u_\alpha, v_\beta)\) pairs (per each of the input/output Super-Sbox positions)
More in the paper:
1 advanced algorithm for computing division core for “heavy” S-boxes (up to 32 bits)

Open problems:
1 compressing CNF models into compact MILP models
2 existence of 8-round integral distinguisher for LED (still open)
3 more applications?

Implementation: github.com/CryptoExperts/AC21-divprop-convexity
1 Python bindings for a C++ implementation
2 Reproducing/verifying results
3 Random 32-bit S-box modeling

ia.cr/2021/1285
[BC16] Christina Boura and Anne Canteaut.  
Another view of the division property.  
In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part I*,  

[Car20] Claude Carlet.  
Graph indicators of vectorial functions and bounds on the algebraic degree  
of composite functions.  

Increasing precision of division property.  

The LED block cipher.