Convexity of division property transitions: theory, algorithms and compact models

Aleksei Udovenko

CryptoExperts

ASIACRYPT 2021,
December 10th

CRYPTO EXPERTS

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.)

[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 $O(n2^{2n})$, 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]

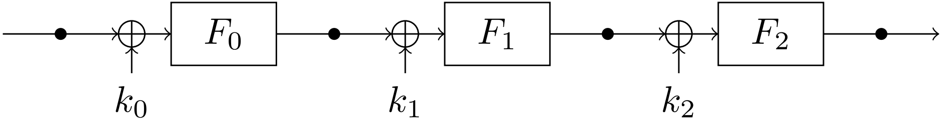
Contributions

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 $O(n2^{2n})$, even less for "heavy" S-boxes
3. Application to LED: Super-Sbox model does **not** yield 8-round distinguishers (Q unsolved by [DF20][2])

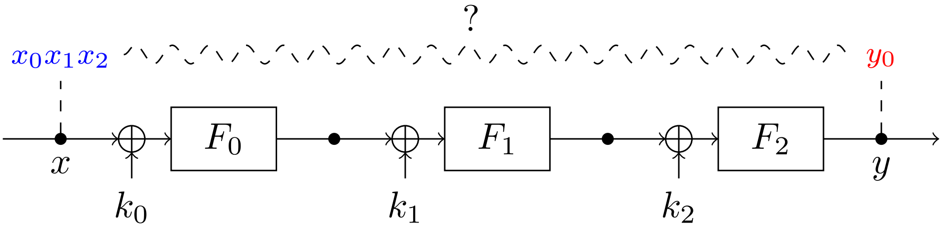
[1] (EUROCRYPT'15) Yosuke Todo. Structural evaluation by generalized integral property
[2] (ToSC'20) Derbez, Fouque. Increasing precision of division property

Plan

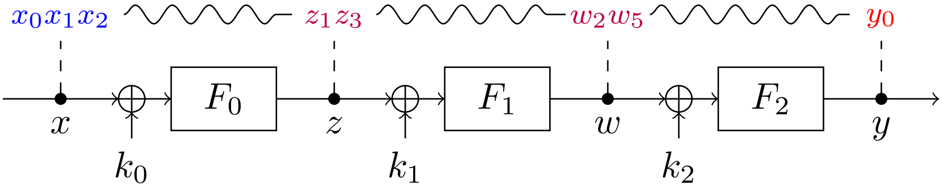
Division property



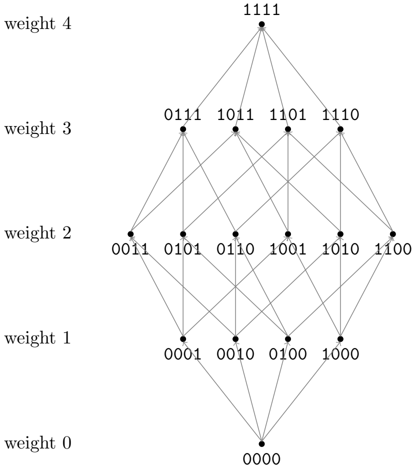
Division property



Division property

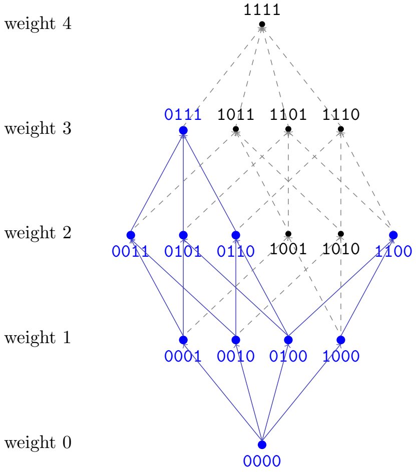


Monotonicity and convexity on $\mathbb{F}_2^n$ - definitions



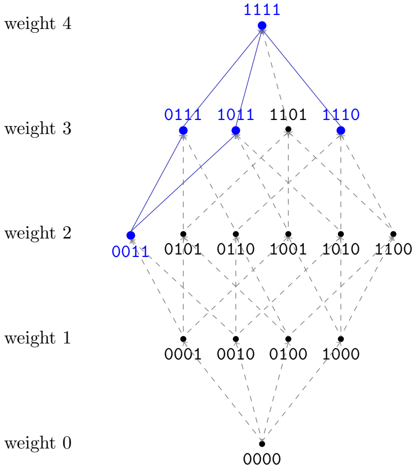
- **partial order** on $\mathbb{F}_2^n$:
  $u \preceq v$ iff $\forall i \quad u_i \leq v_i$

Monotonicity and convexity on $\mathbb{F}_2^n$ - definitions



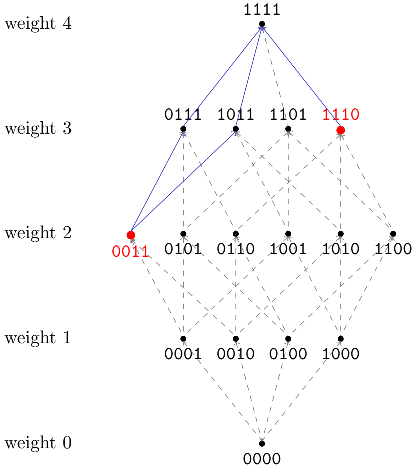
- **partial order** on $\mathbb{F}_2^n$:
  $u \preceq v$ iff $\forall i \quad u_i \leq v_i$
- lower set: $u \notin X \not\preceq v \in X$

Monotonicity and convexity on $\mathbb{F}_2^n$ - definitions



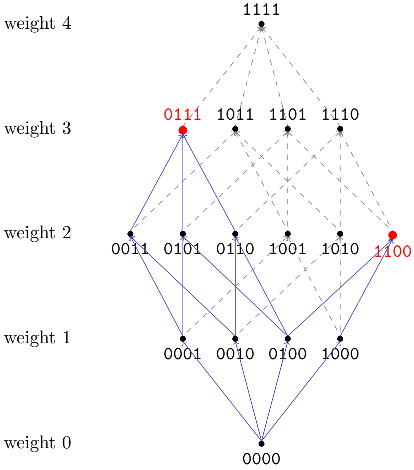
- **partial order** on $\mathbb{F}_2^n$:
  $u \preceq v$ iff $\forall i \quad u_i \leq v_i$
- lower set: $u \notin X \not\preceq v \in X$
- upper set: $u \in X \not\preceq v \notin X$

Monotonicity and convexity on $\mathbb{F}_2^n$ - definitions



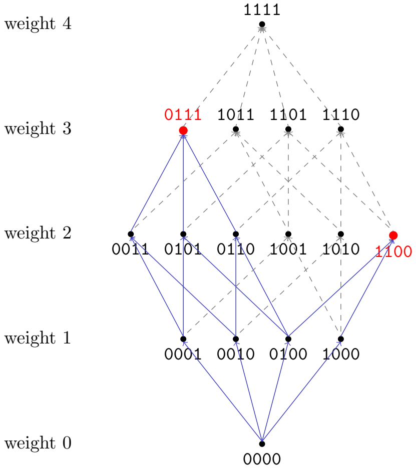
- **partial order** on $\mathbb{F}_2^n$:
  $u \preceq v$ iff $\forall i \quad u_i \leq v_i$
- lower set: $u \notin X \not\preceq v \in X$
- upper set: $u \in X \not\preceq v \notin X$
- extreme elements
  (resp. maximal/minimal)
  form a compact representation:
  {**11, 111*}

Monotonicity and convexity on $\mathbb{F}_2^n$ - definitions



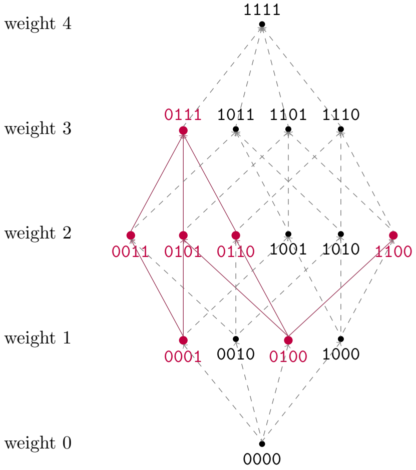
- **partial order** on $\mathbb{F}_2^n$:
  $u \preceq v$ iff $\forall i \ \ u_i \leq v_i$
- lower set: $u \notin X \not\preceq v \in X$
- upper set: $u \in X \not\preceq v \notin X$
- extreme elements
  (resp. maximal/minimal)
  form a compact representation:
  {**11, 111*}
  {0***, **00}

Monotonicity and convexity on $\mathbb{F}_2^n$ - definitions



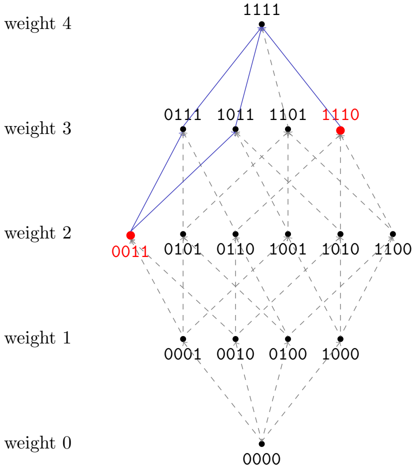
- **partial order** on $\mathbb{F}_2^n$:
  $u \preceq v$ iff $\forall i \;\; u_i \leq v_i$
- lower set: $u \notin X \not\preceq v \in X$
- upper set: $u \in X \not\preceq v \notin X$
- extreme elements
  (resp. maximal/minimal)
  form a compact representation:
  {∗∗11, 111∗}
  {0∗∗∗, ∗∗00}
- (resp. upper and lower bounds)

Monotonicity and convexity on $\mathbb{F}_2^n$ - definitions



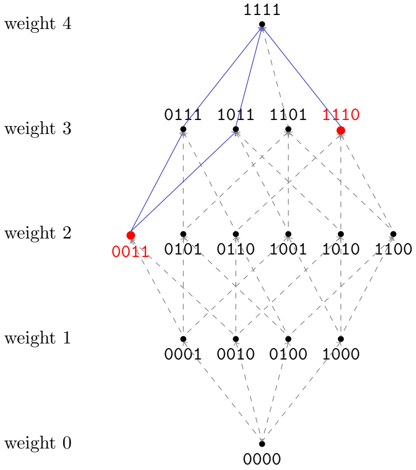
- **partial order** on $\mathbb{F}_2^n$:
  $u \preceq v$ iff $\forall i \; u_i \leq v_i$
- lower set: $u \notin X \not\preceq v \in X$
- upper set: $u \in X \not\preceq v \notin X$
- extreme elements
  (resp. maximal/minimal)
  form a compact representation:
  {**11, 111*}
  {0***, **00}
- (resp. upper and lower bounds)
- 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

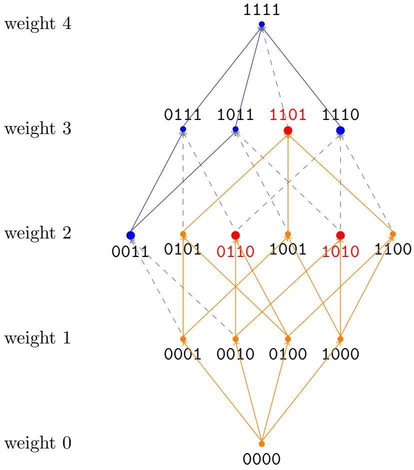


modeling an **upper** set $X \subseteq \mathbb{F}_2^n$:

- monotone DNF (from the min-set):

$$\underbrace{(x_2 \wedge x_3)}_{0011} \vee \underbrace{(x_0 \wedge x_1 \wedge x_2)}_{1110}$$

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



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

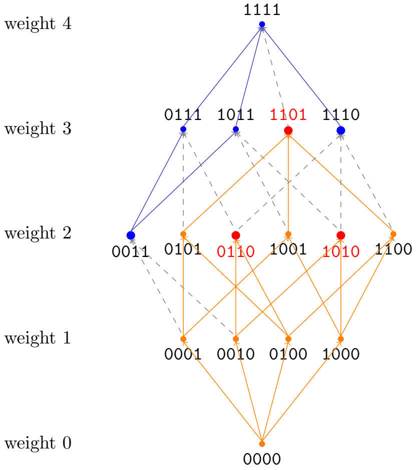
- monotone DNF (from the min-set):

$$\underbrace{(x_2 \wedge x_3)}_{0011} \vee \underbrace{(x_0 \wedge x_1 \wedge x_2)}_{1110}$$

- monotone CNF (from the max-set of the complement):

$$\underbrace{(x_0 \vee x_3)}_{0110} \wedge \underbrace{(x_2)}_{1101} \wedge \underbrace{(x_1 \vee x_3)}_{1010}$$

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):

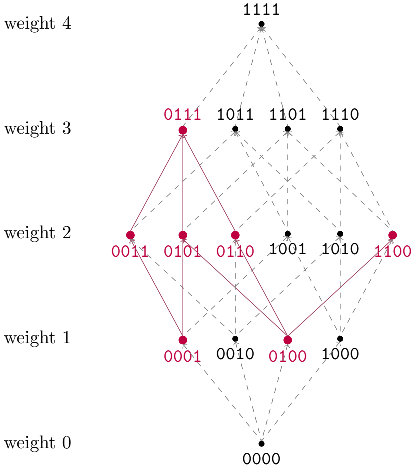
$$\underbrace{(x_2 \wedge x_3)}_{0011} \vee \underbrace{(x_0 \wedge x_1 \wedge x_2)}_{1110}$$

- monotone CNF (from the max-set of the complement):

$$\underbrace{(x_0 \vee x_3)}_{0110} \wedge \underbrace{(x_2)}_{1101} \wedge \underbrace{(x_1 \vee x_3)}_{1010}$$

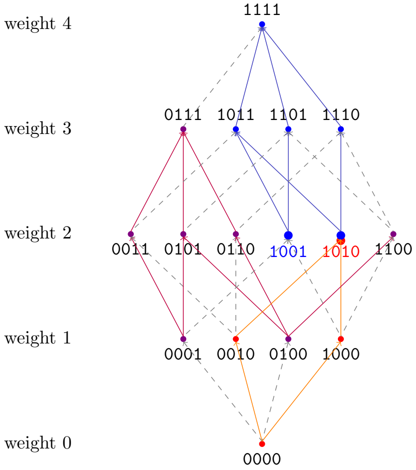
note: CNF-DNF size gap can be exponential!

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



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

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:

$$\underbrace{(\neg x_0 \vee \neg x_3)}_{1001} \wedge \underbrace{(\neg x_0 \vee \neg x_2)}_{1010} \wedge \underbrace{(x_1 \vee x_3)}_{1010}$$

Parity sets: formalization of division property

Definition ([BC16])

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

$$\mathrm{ParitySet}(X) = \left\{ u \in \mathbb{F}_2^n \;\middle|\; \bigoplus_{x \in X} x^u = 1 \right\}$$

Parity sets: formalization of division property

Definition ([BC16])

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

$$\mathrm{ParitySet}(X) = \left\{ u \in \mathbb{F}_2^n \;\middle|\; \bigoplus_{x \in X} x^u = 1 \right\}$$

Definition ([Tod15])

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

$$\mathrm{ParitySet}(X) \subseteq \mathrm{UpperClosure}(\mathbb{K})$$

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

Parity sets: formalization of division property

Definition ([BC16])

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

$$\mathrm{ParitySet}(X) = \left\{ u \in \mathbb{F}_2^n \;\middle|\; \bigoplus_{x \in X} x^u = 1 \right\}$$

Definition ([Tod15])

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

$$\mathrm{ParitySet}(X) \subseteq \mathrm{UpperClosure}(\mathbb{K})$$

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

Proposition

$u \in \mathrm{ParitySet}(X)$

if and only if

the ANF of $\mathbb{1}_{\neg X}$ *contains* $x^{\neg u}$

$\Rightarrow$ 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

$$\mathrm{ParitySet}(X) = \left\{ u \in \mathbb{F}_2^n \;\middle|\; \bigoplus_{x \in X} x^u = 1 \right\}$$

Definition ([Tod15])

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

$$\mathrm{ParitySet}(X) \subseteq \mathrm{UpperClosure}(\mathbb{K})$$

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

Proposition

$u \in \mathrm{ParitySet}(X)$
if and only if
the ANF of $\mathbb{1}_{\neg X}$ *contains* $x^{\neg u}$

$\Rightarrow$ parity set is equivalent to the indicator's ANF up to negations!

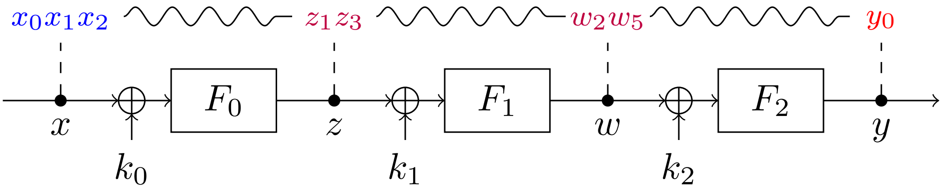
The takeaway

$\Rightarrow$ division property of a set defines **upper bounds** on monomials in the indicator's ANF

Propagation of division property

Proposition (Propagation rule)

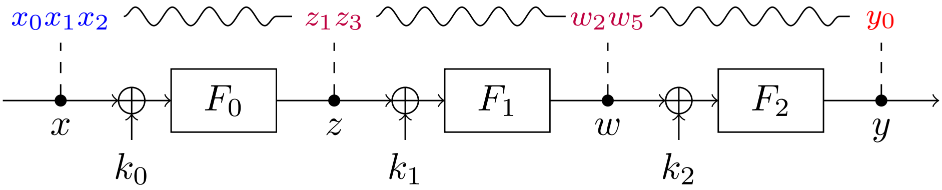
Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, $u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m$. *If* $F^{v'}(x)$ *contains monomial* $x^{u'}$ *for some* $v' \preceq v, u' \succeq u$, *then* $u \xrightarrow{F} v$ *is a valid division property transition through* F.



Propagation of division property

Proposition (Propagation rule)

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, $u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m$. 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.



e.g. $z_1 = (F_0(x))_1$ contains $x_0x_1x_2x_5$

Plan

New characterizations of transitions

Definition

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

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

[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 $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ 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* Γ_F *(i.e.,* $\mathrm{UpperClosure}(\mathrm{ParitySet}(\Gamma_F))$*)*
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.

Compact representation

Definition

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

$$\mathrm{DivCore}(F) = \mathrm{MinSet}(\mathrm{ParitySet}(\Gamma_F)) \quad \text{i.e., the division property of } \Gamma_F$$

Equivalently:

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

Compact representation

Definition

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

$$\mathrm{DivCore}(F) = \mathrm{MinSet}(\mathrm{ParitySet}(\Gamma_F)) \quad \text{i.e., the division property of } \Gamma_F$$

Equivalently:

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

- Classic propagation of division property focuses on minimal/reduced transitions $u \xrightarrow[\text{min.}]{F} v$, which only require that v is minimal.
- $\mathrm{DivCore}$ 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 $\mathrm{DivCore}(F)$:

Theorem

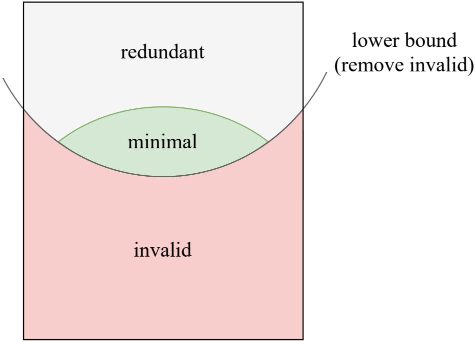
Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$*. Then,*

1. $u \xrightarrow{F} v \quad \Leftrightarrow \quad (\neg u, v) \in \mathrm{UpperClosure}(\mathrm{DivCore}(F))$
2. $u \xrightarrow[\text{min.}]{F} v \quad \Leftrightarrow \quad (\neg u, v) \in \mathrm{MinSet}_v(\mathrm{UpperClosure}(\mathrm{DivCore}(F)))$

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

4. $v \xrightarrow{F^{-1}} u \quad \Leftrightarrow \quad (u, \neg v) \in \mathrm{UpperClosure}(\mathrm{DivCore}(F))$
5. $v \xrightarrow[\text{min.}]{F^{-1}} u \quad \Leftrightarrow \quad (u, \neg v) \in \mathrm{MinSet}_u(\mathrm{UpperClosure}(\mathrm{DivCore}(F)))$

Convexity of minimal transitions

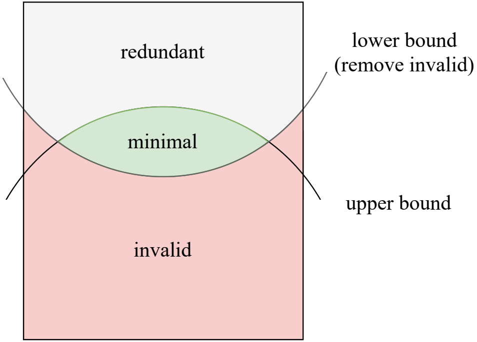


partition of $\mathbb{F}_2^n \times \mathbb{F}_2^m$
into transition classes
$\neg u \xrightarrow[?]{F} v$

Modeling:

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

Convexity of minimal transitions

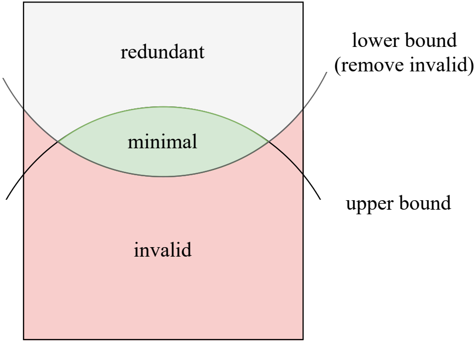


partition of $\mathbb{F}_2^n \times \mathbb{F}_2^m$
into transition classes
$\neg u \xrightarrow[?]{F} v$

Modeling:

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

Convexity of minimal transitions



partition of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ into transition classes $\neg u \xrightarrow[?]{F} v$

Modeling:

- removing invalid transitions is sufficient
- however, removing redundant transitions aids solvers
- $\Rightarrow$ 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 DivCore

Model sizes for some (Super)S-boxes

Modeling only minimal transitions: (convex)

function	n	#min.trans.	CNF (our)	CNF (optimal)
AES	8	2001	361	234
Misty S7	7	1779	1363	607
Misty S9	9	27 626	21 988	10 403-11 819

Modeling valid transitions: (upper)

function	n	#min.trans.	CNF (our)
Midori-64 Super-Sbox (all keys)	16	14 714 723	1 912 088
LED Super-Sbox (all keys)	16	8 458 909	319 606
LED MixColumn (linear)	16	177 643 913	33 412
Randomly gen. 32-bit S-box	32	?	2958

Plan

Algorithmic framework

function $\mathrm{Transform}_f(X \in \mathbb{F}_2^{2^n})$ ▷ 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**

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

Algorithmic framework

function $\mathrm{Transform}_f(X \in \mathbb{F}_2^{2^n})$ ▷ 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**
      $(X_{j-2^i}, X_j) \leftarrow f(X_{j-2^i}, X_j)$

function f	$f(a, b)$	effect of $\mathrm{Transform}_f$
XOR-up	$(a, b \oplus a)$	compute ANF (involution)

Algorithmic framework

function $\mathrm{Transform}_f(X \in \mathbb{F}_2^{2^n})$ ▷ 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**
      $(X_{j-2^i}, X_j) \leftarrow f(X_{j-2^i}, X_j)$

function f	$f(a,b)$	effect of $\mathrm{Transform}_f$
XOR-up	$(a, b \oplus a)$	compute ANF (involution)
XOR-down	$(a \oplus b, b)$	compute $\mathrm{ParitySet}$ (involution)

Algorithmic framework

function $\mathrm{Transform}_f(X \in \mathbb{F}_2^{2^n})$ ▷ Complexity: $O(n2^n)$
  for all $i \in \{0, \dots, n-1\}$ **do**
    for all $j \in \{0, \dots, 2^n - 1\}$, s.t. j has $(n-1-i)$-th bit set **do**
      $(X_{j-2^i}, X_j) \leftarrow f(X_{j-2^i}, X_j)$

function f	$f(a, b)$	effect of $\mathrm{Transform}_f$
XOR-up	$(a, b \oplus a)$	compute ANF (involution)
XOR-down	$(a \oplus b, b)$	compute $\mathrm{ParitySet}$ (involution)
OR-up	$(a, b \vee a)$	compute $\mathrm{UpperClosure}$
OR-down	$(a \vee b, b)$	compute $\mathrm{LowerClosure}$

Algorithmic framework

function $\mathrm{Transform}_f(X \in \mathbb{F}_2^{2^n})$ ▷ 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**
      $(X_{j-2^i}, X_j) \leftarrow f(X_{j-2^i}, X_j)$

function f	$f(a,b)$	effect of $\mathrm{Transform}_f$
XOR-up	$(a, b \oplus a)$	compute ANF (involution)
XOR-down	$(a \oplus b, b)$	compute $\mathrm{ParitySet}$ (involution)
OR-up	$(a, b \vee a)$	compute $\mathrm{UpperClosure}$
OR-down	$(a \vee b, b)$	compute $\mathrm{LowerClosure}$
LESS-up	$(a, b \wedge \neg a)$	compute MinSet (after $\mathrm{Transform}_{\text{OR-up}}$)
MORE-down	$(a \wedge \neg b, b)$	compute MaxSet (after $\mathrm{Transform}_{\text{OR-down}}$)

Algorithmic framework

function $\mathrm{Transform}_f(X \in \mathbb{F}_2^{2^n})$ ▷ 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**

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

function $\mathrm{MinDPPT}(F : \mathbb{F}_2^n \to \mathbb{F}_2^m$: a lookup table) ▷ Complexity: $O((n+m)2^{n+m})$

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

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

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

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

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

Algorithmic framework

function $\mathrm{Transform}_f(X \in \mathbb{F}_2^{2^n})$ ▷ 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**
      $(X_{j-2^i}, X_j) \leftarrow f(X_{j-2^i}, X_j)$

function $\mathrm{MinDPPT}(F : \mathbb{F}_2^n \to \mathbb{F}_2^m$: a lookup table) ▷ Complexity: $O((n+m)2^{n+m})$
  $D \leftarrow$ indicator vector of Γ_F $(\in \mathbb{F}_2^{2^{n+m}})$
  $D \leftarrow \mathrm{Transform}_{\text{XOR-down}}(D)$
  $D \leftarrow \mathrm{Transform}_{\text{OR-up}}(D)$
  $D \leftarrow \mathrm{Transform}_{\text{LESS-up}}(D)$, only with $i < n$ in the first loop
  return $\{(\neg u, v) \mid (u, v) \in D\}$

DPPT, DivCore, etc. for $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ in $O(n2^{2n})$

Plan

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.

[4] (ToSC'20) Hu, Wang, Wang. Finding bit-based division property for ciphers with complex linear layers.

[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)

---

[4] (ToSC'20) Hu, Wang, Wang. Finding bit-based division property for ciphers with complex linear layers.

[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

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

1^{15} $\langle \alpha, x \rangle^{\perp}$			
	1111	1111	1111
	1111	1111	1111
	1111	1111	1111
	1111	1111	1111

SuperSbox →

1111	1111	1111	1111
0010	1111	1111	1111
1111	1111	1111	1111
0110	1111	1111	1111

$\mathsf{SR} \circ \mathsf{MC} \circ \mathsf{SR}$ →

1111	1011	1111	1101
1111	1111	1101	1111
1111	1111	1111	1111
1101	1111	1101	1111

SuperSbox →

0100	0011	1000	1000
0001	1111	0100	1111
1111	0001	0100	1010
1111	1111	0110	0100

$\mathsf{SR} \circ \mathsf{MC} \circ \mathsf{SR}$ →

0000	0000	1111	0000
0111	1011	0000	0011
1011	1101	1010	1101
0011	1101	0111	0111

SuperSbox →

0000	0000	0100	0000
1010	0000	0000	0100
0000	0000	0000	0000
0000	0010	0010	0000

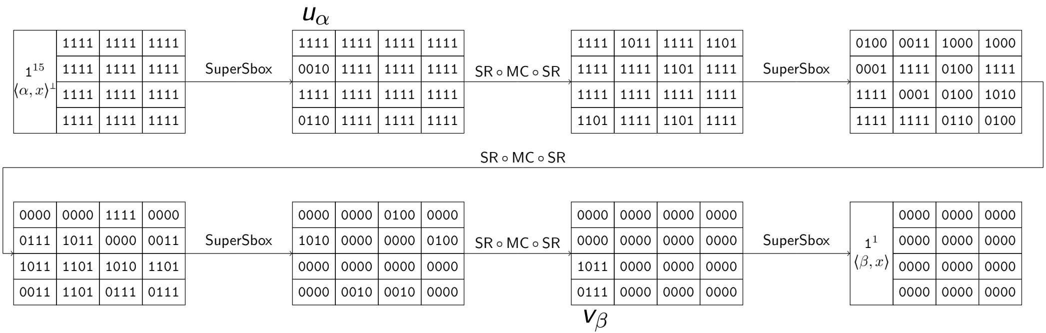
$\mathsf{SR} \circ \mathsf{MC} \circ \mathsf{SR}$ →

0000	0000	0000	0000
0000	0000	0000	0000
1011	0000	0000	0000
0111	0000	0000	0000

SuperSbox →

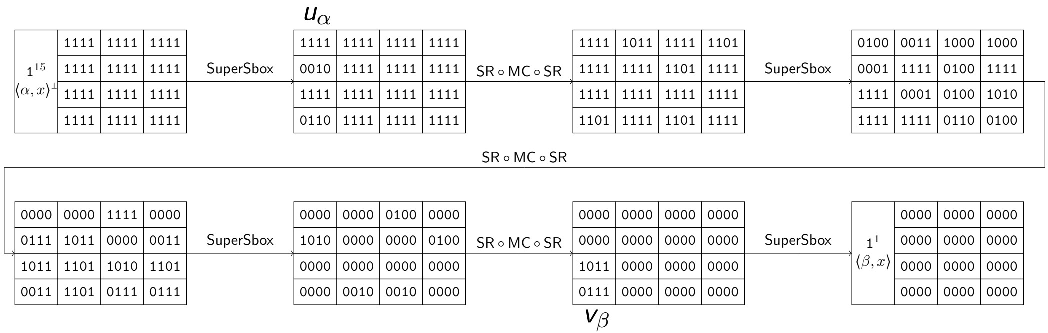
1^{1} $\langle \beta, x \rangle$			
	0000	0000	0000
	0000	0000	0000
	0000	0000	0000
	0000	0000	0000

An example LED trail



- 255 columns u_α to cover all possible $\alpha \neq 0$
- 255 columns v_β to cover all possible $\beta \neq 0$

An example LED trail



- 255 columns u_α to cover all possible $\alpha \neq 0$
- 255 columns v_β to cover all possible $\beta \neq 0$
- on practice, ≈30 trails are sufficient to cover all (u_α, v_β) pairs (per each of the input/output Super-Sbox positions)

The End

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*, volume 9814 of *LNCS*, pages 654–682. Springer, Heidelberg, 2016.

[Car20] Claude Carlet.
Graph indicators of vectorial functions and bounds on the algebraic degree of composite functions.
IEEE Transactions on Information Theory, pages 1–1, 2020.

[DF20] Patrick Derbez and Pierre-Alain Fouque.
Increasing precision of division property.
IACR Trans. Symm. Cryptol., 2020(4):173–194, 2020.

[GPPR11] Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew J. B. Robshaw.
The LED block cipher.

In Bart Preneel and Tsuyoshi Takagi, editors, *CHES 2011*, volume 6917 of *LNCS*, pages 326–341. Springer, Heidelberg, 2011.

[HWW20] Kai Hu, Qingju Wang, and Meiqin Wang.
IACR transactions class documentation.
IACR Trans. Symm. Cryptol., 2020(1):396–424, 2020.

[Tod15] Yosuke Todo.
Structural evaluation by generalized integral property.
In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 287–314. Springer, Heidelberg, 2015.