# On Division Property and Degree Bounds

Aleksei Udovenko

*based on joint work with* Gregor Leander and Phil Hebborn

BFA 2023, September 4$^{th}$

SnT, University of Luxembourg

# Plan

Problem formulation

Degree bounds

Division property

Perfect division property and degree lower bounds

Conclusions

# Algebraic Normal Form (ANF)

**ANF:** $f : \mathbb{F}_2^n \to \mathbb{F}_2$

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{u} \in \mathbb{F}_2^n} \lambda_{\boldsymbol{u}} \prod_{1 \le j \le n} x_j^{u_j} \qquad \lambda_{\boldsymbol{u}} \in \mathbb{F}_2$$

# Algebraic Normal Form (ANF)

**ANF:** $f : \mathbb{F}_2^n \to \mathbb{F}_2$

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{u} \in \mathbb{F}_2^n} \lambda_{\boldsymbol{u}} \prod_{1 \leq j \leq n} x_j^{u_j} = \boxed{\sum_{\boldsymbol{u} \in \mathbb{F}_2^n} \lambda_{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{u}}} \qquad \lambda_{\boldsymbol{u}} \in \mathbb{F}_2$$

# Algebraic Normal Form (ANF)

**ANF:** $f : \mathbb{F}_2^n \to \mathbb{F}_2$

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{u} \in \mathbb{F}_2^n} \lambda_{\boldsymbol{u}} \prod_{1 \le j \le n} x_j^{u_j} = \boxed{\sum_{\boldsymbol{u} \in \mathbb{F}_2^n} \lambda_{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{u}}} \qquad \lambda_{\boldsymbol{u}} \in \mathbb{F}_2$$

**Partial order:** $\boldsymbol{u} \preceq \boldsymbol{v} \quad \Leftrightarrow \quad \forall i \ u_i \le v_i$

# Algebraic Normal Form (ANF)

**ANF:** $f : \mathbb{F}_2^n \to \mathbb{F}_2$

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{u} \in \mathbb{F}_2^n} \lambda_{\boldsymbol{u}} \prod_{1 \leq j \leq n} x_j^{u_j} = \boxed{\sum_{\boldsymbol{u} \in \mathbb{F}_2^n} \lambda_{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{u}}} \qquad \lambda_{\boldsymbol{u}} \in \mathbb{F}_2$$

**Partial order:** $\boldsymbol{u} \preceq \boldsymbol{v} \quad \Leftrightarrow \quad \forall i \; u_i \leq v_i \quad \Leftrightarrow \quad \boldsymbol{x}^{\boldsymbol{u}} \mid \boldsymbol{x}^{\boldsymbol{v}}$

# Algebraic Normal Form (ANF)

**ANF:** $f : \mathbb{F}_2^n \to \mathbb{F}_2$

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{u} \in \mathbb{F}_2^n} \lambda_{\boldsymbol{u}} \prod_{1 \leq j \leq n} x_j^{u_j} = \boxed{\sum_{\boldsymbol{u} \in \mathbb{F}_2^n} \lambda_{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{u}}} \qquad \lambda_{\boldsymbol{u}} \in \mathbb{F}_2$$

**Partial order:** $\boldsymbol{u} \preceq \boldsymbol{v} \quad \Leftrightarrow \quad \forall i \; u_i \leq v_i \quad \Leftrightarrow \quad \boldsymbol{x}^{\boldsymbol{u}} \mid \boldsymbol{x}^{\boldsymbol{v}} \quad \Leftrightarrow \quad \boldsymbol{v}^{\boldsymbol{u}} = 1$

# Algebraic Normal Form (ANF)

**ANF:** $f : \mathbb{F}_2^n \to \mathbb{F}_2$

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{u} \in \mathbb{F}_2^n} \lambda_{\boldsymbol{u}} \prod_{1 \le j \le n} x_j^{u_j} = \boxed{\sum_{\boldsymbol{u} \in \mathbb{F}_2^n} \lambda_{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{u}}} \qquad \lambda_{\boldsymbol{u}} \in \mathbb{F}_2$$

**Partial order:** $\boldsymbol{u} \preceq \boldsymbol{v} \Leftrightarrow \forall i \; u_i \le v_i \Leftrightarrow \boldsymbol{x}^{\boldsymbol{u}} \mid \boldsymbol{x}^{\boldsymbol{v}} \Leftrightarrow \boldsymbol{v}^{\boldsymbol{u}} = 1$

**Inversion:** $\boxed{\lambda_{\boldsymbol{u}} = \sum_{\boldsymbol{x} \preceq \boldsymbol{u}} f(\boldsymbol{x})}$

# Algebraic Normal Form (ANF)

**ANF:** $f : \mathbb{F}_2^n \to \mathbb{F}_2$

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{u} \in \mathbb{F}_2^n} \lambda_{\boldsymbol{u}} \prod_{1 \le j \le n} x_j^{u_j} = \boxed{\sum_{\boldsymbol{u} \in \mathbb{F}_2^n} \lambda_{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{u}}} \qquad \lambda_{\boldsymbol{u}} \in \mathbb{F}_2$$

**Partial order:** $\boldsymbol{u} \preceq \boldsymbol{v} \quad \Leftrightarrow \quad \forall i \; u_i \le v_i \quad \Leftrightarrow \quad \boldsymbol{x}^{\boldsymbol{u}} \mid \boldsymbol{x}^{\boldsymbol{v}} \quad \Leftrightarrow \quad \boldsymbol{v}^{\boldsymbol{u}} = 1$

**Inversion:** $\boxed{\lambda_{\boldsymbol{u}} = \sum_{\boldsymbol{x} \preceq \boldsymbol{u}} f(\boldsymbol{x})} \qquad f(\boldsymbol{x}) = \sum_{\boldsymbol{u} \preceq \boldsymbol{x}} \lambda_{\boldsymbol{u}}$

# Problem (Degree)

**ANF:** $f(\boldsymbol{x}) = \sum_{\boldsymbol{u} \in \mathbb{F}_2^n} \lambda_{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{u}}$

**Algebraic degree:** $\deg f = \max_{\boldsymbol{u} \colon \lambda_{\boldsymbol{u}} = 1} \mathrm{wt}(\boldsymbol{u})$

# Problem (Degree)

**ANF:** $$f(\boldsymbol{x}) = \sum_{\boldsymbol{u} \in \mathbb{F}_2^n} \lambda_{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{u}}$$

**Algebraic degree:** $$\deg f = \max_{\boldsymbol{u} \colon \lambda_{\boldsymbol{u}} = 1} \mathrm{wt}(\boldsymbol{u})$$

$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ $$\deg F = \max_i \deg F_i$$ (min also makes sense)

# Problem (Degree)

**ANF:** $$f(\boldsymbol{x}) = \sum_{\boldsymbol{u} \in \mathbb{F}_2^n} \lambda_{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{u}}$$

**Algebraic degree:** $$\deg f = \max_{\boldsymbol{u} \colon \lambda_{\boldsymbol{u}} = 1} \mathrm{wt}(\boldsymbol{u})$$

$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ $$\deg F = \max_i \deg F_i$$ (min also makes sense)

**Problem**

*Given $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ (in some form), determine or bound its algebraic degree*

*Typically: $F = G^{(r)} \circ G^{(r-1)} \circ \ldots \circ G^{(1)}$ with explicit $G^{(i)}$*

# Finer Problem (Monomials)

**Example**

Let $F(\boldsymbol{x}, \boldsymbol{y}) = G(\boldsymbol{x}) + H(\boldsymbol{y}) : \mathbb{F}_2^{2n} \to \mathbb{F}_2^{n}$ with $\deg G = \deg H = n - 1$. Then:

- $\deg F = n - 1$

# Finer Problem (Monomials)

**Example**

Let $F(\boldsymbol{x}, \boldsymbol{y}) = G(\boldsymbol{x}) + H(\boldsymbol{y}) : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$ with $\deg G = \deg H = n - 1$. Then:

- $\deg F = n - 1$
- $F$ does not contain any of the monomials $x_i y_j$ for all pairs $(i, j)$

# Finer Problem (Monomials)

**Example**

Let $F(\boldsymbol{x}, \boldsymbol{y}) = G(\boldsymbol{x}) + H(\boldsymbol{y}) : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$ with $\deg G = \deg H = n - 1$. Then:

- $\deg F = n - 1$
- $F$ does not contain any of the monomials $x_i y_j$ for all pairs $(i, j)$
- in fact, $F$ does not contain *any multiple* of those

# Finer Problem (Monomials)

**Example**

Let $F(\boldsymbol{x}, \boldsymbol{y}) = G(\boldsymbol{x}) + H(\boldsymbol{y}) : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$ with $\deg G = \deg H = n - 1$. Then:

- $\deg F = n - 1$
- $F$ does not contain any of the monomials $x_i y_j$ for all pairs $(i, j)$
- in fact, $F$ does not contain *any multiple* of those
- $\Rightarrow \quad F(a, b) + F(a + \delta, b) + F(a, b + \delta') + F(a + \delta, b + \delta') = 0 \quad \forall a, b, \delta, \delta'$

# Finer Problem (Monomials)

**Example**

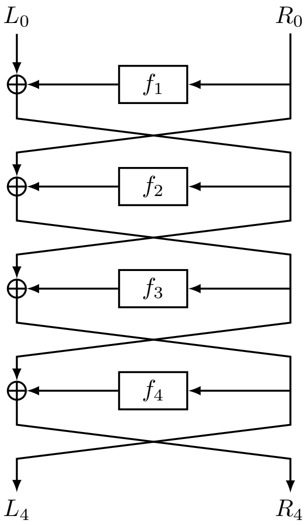
Let $F(\boldsymbol{x}, \boldsymbol{y}) = G(\boldsymbol{x}) + H(\boldsymbol{y}) : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$ with $\deg G = \deg H = n - 1$. Then:

- $\deg F = n - 1$
- $F$ does not contain any of the monomials $x_i y_j$ for all pairs $(i, j)$
- in fact, $F$ does not contain *any multiple* of those
- $\Rightarrow \quad F(a, b) + F(a + \delta, b) + F(a, b + \delta') + F(a + \delta, b + \delta') = 0 \quad \forall a, b, \delta, \delta'$

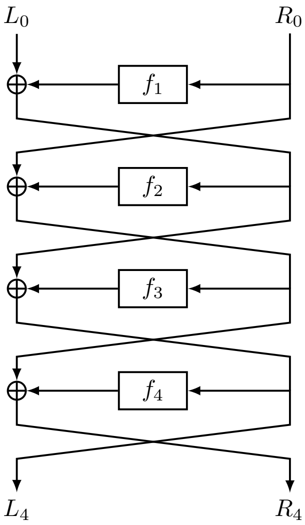
Applications: integral cryptanalysis, cube attacks

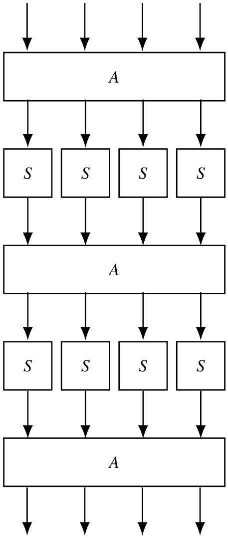
Important: ciphers are very structured, we want to catch any such deficiencies

# Iterated Structures

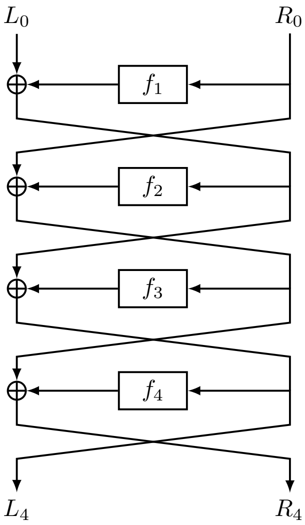


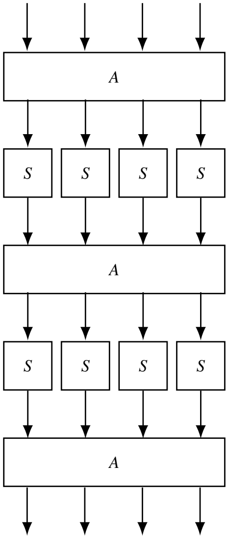
# Iterated Structures

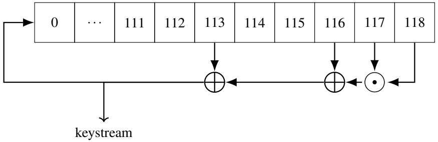


# Iterated Structures



# Plan

Problem formulation

Degree bounds

- Classic bounds
- Bound unification and comparison
- Bound summary

Division property

Perfect division property and degree lower bounds

Conclusions

# Plan

Problem formulation

Degree bounds

- Classic bounds
- Bound unification and comparison
- Bound summary

Division property

Perfect division property and degree lower bounds

Conclusions

# Naive bound

**Proposition (Naive bound)**

*Let* $f = g \circ H$. *Then,*

$$\boxed{\deg f \;\leq\; \deg g \;\times\; \deg H}$$

# Naive bound

## Proposition (Naive bound)

*Let* $f = g \circ H$. *Then,*

$$\boxed{\deg f \;\leq\; \deg g \;\times\; \deg H}$$

## Example

Say $g(\boldsymbol{x}) = x_1 x_2 x_3$. Then,

$$f(\boldsymbol{x}) = g(H(\boldsymbol{x})) = \underbrace{\underbrace{H_1(x)}_{\leq \deg H} \cdot \underbrace{H_2(x)}_{\leq \deg H} \cdot \underbrace{H_3(x)}_{\leq \deg H}}_{\deg g \ \text{times}}$$

# Naive bound

**Proposition (Naive bound)**

*Let $f = g \circ H$. Then,*

$$\boxed{\deg f \;\le\; \deg g \;\times\; \deg H}$$

**Example**

Say $g(\boldsymbol{x}) = x_1 x_2 x_3$. Then,

$$f(\boldsymbol{x}) = g(H(\boldsymbol{x})) = \underbrace{\underbrace{H_1(x)}_{\le \deg H} \cdot \underbrace{H_2(x)}_{\le \deg H} \cdot \underbrace{H_3(x)}_{\le \deg H}}_{\deg g \text{ times}}$$

Important idea: $g$ a *monomial function* covers a lot of cases

# Boura-Canteaut bound (Boura and Canteaut 2013)

**Theorem (Boura and Canteaut 2013; Boura, Canteaut, and De Cannière 2011)**

*Let* $f = g \circ H$ *with* $H$ *a bijection. Then,*

$$\boxed{\deg f \;\leq\; n - \left\lceil \frac{n - \deg g}{\deg H^{-1}} \right\rceil}$$

# Boura-Canteaut bound (Boura and Canteaut 2013)

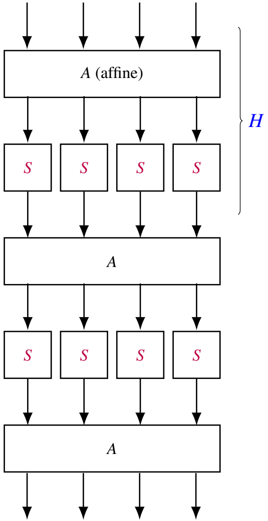
**Theorem (Boura and Canteaut 2013; Boura, Canteaut, and De Cannière 2011)**

*Let $f = g \circ H$ with $H$ a bijection. Then,*

$$\boxed{\deg f \;\le\; n - \left\lceil \frac{n - \deg g}{\deg H^{-1}} \right\rceil}$$

Degree deficit can not drop by a factor more than $\deg H^{-1}$ when pre-composing $H$

# Boura-Canteaut bound - example (SPN)




$H : \mathbb{F}_2^n \to \mathbb{F}_2^n$ (one SPN round)
$S : \mathbb{F}_2^m \to \mathbb{F}_2^m$ (an S-box)
$\deg H = \deg S \leq m - 1$
$\deg H^{-1} = \deg S^{-1} \leq m - 1$

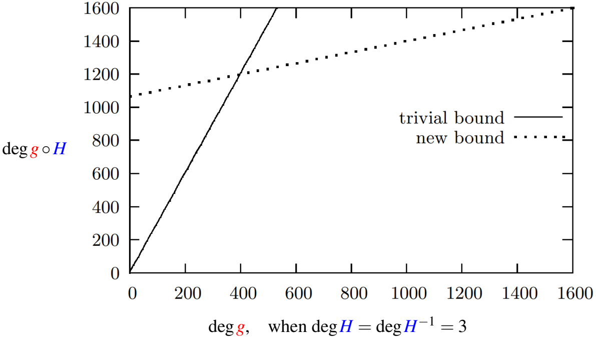



*Figure from (Boura-Canteaut-DeCannière, FSE 2011)*

# Carlet bound

**Theorem (Carlet 2020)**

*Let $f = g \circ H$, where $H : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Then,*

$$\boxed{\deg f \leq \deg g + \deg \mathbb{1}_{\Gamma_H} - m}$$

*where*

- $\Gamma_H = \{(\boldsymbol{x}, H(\boldsymbol{x})) \mid \boldsymbol{x} \in \mathbb{F}_2^n\}$
- $\mathbb{1}_{\Gamma_H} : \mathbb{F}_2^{n+m} \to \mathbb{F}_2 : (\boldsymbol{x}, \boldsymbol{y}) \mapsto \begin{cases} 1 & \text{if } H(\boldsymbol{x}) = \boldsymbol{y}, \\ 0 & \text{otherwise} \end{cases}$

# Plan


Problem formulation

Degree bounds

- Classic bounds
- Bound unification and comparison
- Bound summary

Division property

Perfect division property and degree lower bounds

Conclusions

# Bound unification 1

For $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ define (Boura and Canteaut 2013)

$$\boxed{\delta_k(F) = \max_{\alpha \in \mathbb{F}_2^n,\, \mathrm{wt}\,\alpha \leq k} \deg F^\alpha}$$

# Bound unification 1

For $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ define (Boura and Canteaut 2013)

$$\boxed{\delta_k(F) = \max_{\alpha \in \mathbb{F}_2^n,\, \mathrm{wt}\,\alpha \leq k} \deg F^\alpha} = \max_{g : \mathbb{F}_2^m \to \mathbb{F}_2,\, \deg g \leq k} \deg\,(g \circ F)$$

# Bound unification 1

For $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ define (Boura and Canteaut 2013)

$$\boxed{\delta_k(F) = \max_{\alpha \in \mathbb{F}_2^n,\, \mathrm{wt}\,\alpha \le k} \deg F^\alpha} = \max_{g : \mathbb{F}_2^m \to \mathbb{F}_2,\, \deg g \le k} \deg (g \circ F)$$

Essentially a "precomputed" answer to the problem (example):

| $k$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $\delta_k$ | 3 | 4 | 6 | 7 | 7 | 7 | 7 | 8 |

# Bound unification 1

For $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ define (Boura and Canteaut 2013)

$$\boxed{\delta_k(F) = \max_{\alpha \in \mathbb{F}_2^n,\, \mathrm{wt}\, \alpha \le k} \deg F^{\alpha}} = \max_{g : \mathbb{F}_2^m \to \mathbb{F}_2,\, \deg g \le k} \deg (g \circ F)$$

Essentially a "precomputed" answer to the problem (example):

| $k$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $\delta_k$ | 3 | 4 | 6 | 7 | 7 | 7 | 7 | 8 |

Question: how does it relate to the previous bounds?

# Bound unification 2

**Theorem (Boura and Canteaut 2013)**

$\delta_\ell(F^{-1}) < n - k \quad \Leftrightarrow \quad \delta_k(F) < n - \ell$

# Bound unification 2

**Theorem (Boura and Canteaut 2013)**

$\delta_\ell(F^{-1}) < n - k \quad \Leftrightarrow \quad \delta_k(F) < n - \ell$

$\Rightarrow$ knowing $d = \deg F^{-1} = \delta_1(F^{-1})$ yields $\delta_{n-d-1}(F) < n - 1$

# Bound unification 2

**Theorem (Boura and Canteaut 2013)**

$\delta_\ell(F^{-1}) < n - k \quad \Leftrightarrow \quad \delta_k(F) < n - \ell$

$\Rightarrow$ knowing $d = \deg F^{-1} = \delta_1(F^{-1})$ yields $\delta_{n-d-1}(F) < n - 1$

$\Rightarrow$ knowing $\delta(F)$ is equivalent to knowing $\delta(F^{-1})$

# Bound unification 2

**Theorem (Boura and Canteaut 2013)**

$\delta_\ell(F^{-1}) < n - k \quad \Leftrightarrow \quad \delta_k(F) < n - \ell$

$\Rightarrow$ knowing $d = \deg F^{-1} = \delta_1(F^{-1})$ yields $\delta_{n-d-1}(F) < n - 1$

$\Rightarrow$ knowing $\delta(F)$ is equivalent to knowing $\delta(F^{-1})$

**Theorem (Udovenko 2021)**

*The following are equivalent:*

- $\delta_v(F) \geq u$
- $\exists$ *monomial* $\boldsymbol{x}^\alpha \boldsymbol{y}^\beta$ *in* $\mathbb{1}_{\Gamma_F}(\boldsymbol{x}, \boldsymbol{y})$ *with*
  - $\deg_{\boldsymbol{x}} \boldsymbol{x}^\alpha \boldsymbol{y}^\beta = \mathrm{wt}\,\alpha \geq u$, *and*
  - $\deg_{\boldsymbol{y}} \boldsymbol{x}^\alpha \boldsymbol{y}^\beta = \mathrm{wt}\,\beta \geq m - v$

# Bound unification 2

**Theorem (Boura and Canteaut 2013)**

$\delta_\ell(F^{-1}) < n - k \quad \Leftrightarrow \quad \delta_k(F) < n - \ell$

$\Rightarrow$ knowing $d = \deg F^{-1} = \delta_1(F^{-1})$ yields $\delta_{n-d-1}(F) < n - 1$

$\Rightarrow$ knowing $\delta(F)$ is equivalent to knowing $\delta(F^{-1})$

**Theorem (Udovenko 2021)**

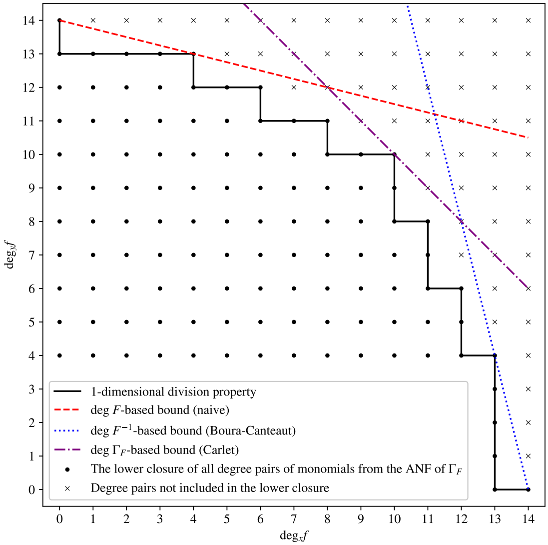
*The following are equivalent:*

- $\delta_v(F) = u$ *with minimal such* $v$ *(i.e.,* $\delta_{v-1}(F) < u$*)*
- $\exists$ *maximal monomial* $\boldsymbol{x}^\alpha \boldsymbol{y}^\beta$ *in* $\mathbb{1}_{\Gamma_F}(\boldsymbol{x}, \boldsymbol{y})$ *with* $\mathrm{wt}\,\alpha = u, \mathrm{wt}\,\beta = m - v$

# Bound comparison

$$F : (\mathbb{F}_{2^7})^2 \to (\mathbb{F}_{2^7})^2 : (x_L, x_R) \mapsto (x_L^3, x_R^{1/3})$$

$$\deg F = \deg F^{-1} = 4, \ \deg \mathbb{1}_{\Gamma_F} = 20$$

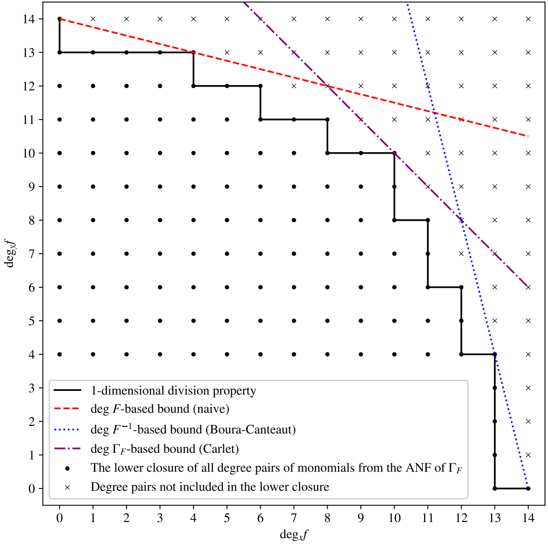


# Bound comparison

$F : (\mathbb{F}_{2^7})^2 \to (\mathbb{F}_{2^7})^2 : (x_L, x_R) \mapsto (x_L^3, x_R^{1/3})$

$\deg F = \deg F^{-1} = 4, \ \deg \mathbb{1}_{\Gamma_F} = 20$

- naive bound
- Boura-Canteaut bound ($\deg F^{-1}$)
- Carlet bound ($\deg \mathbb{1}_{\Gamma_F}$)
- **maximal degree pairs of $\mathbb{1}_{\Gamma_F}$ / extremal $\delta(F)$ values**



# Plan

Problem formulation

Degree bounds

Classic bounds

Bound unification and comparison

Bound summary

Division property

Perfect division property and degree lower bounds

Conclusions

# Bound summary

Degree bounds:

- Naive bound ($\deg F$)
- Boura-Canteaut ($\deg F^{-1}$)
- Carlet ($\deg \mathbb{1}_{\Gamma_F}$)
- Full $\delta(F)$ = state-based division property

Monomial bounds:

- word-based division property
- bit-based division property
- perfect division property (bit-based)

precision

information used

computations

# Plan

Problem formulation

Degree bounds

Division property

- From state-based to bit-based
- On bit-based division property
- Computational aspects

Perfect division property and degree lower bounds

Conclusions

# Plan


Problem formulation

Degree bounds

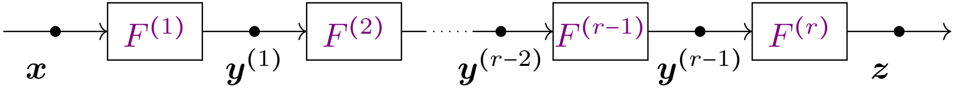
Division property

- From state-based to bit-based
- On bit-based division property
- Computational aspects

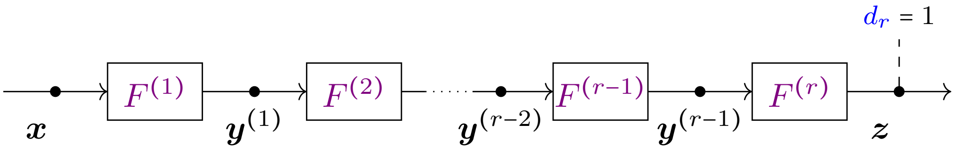
Perfect division property and degree lower bounds

Conclusions

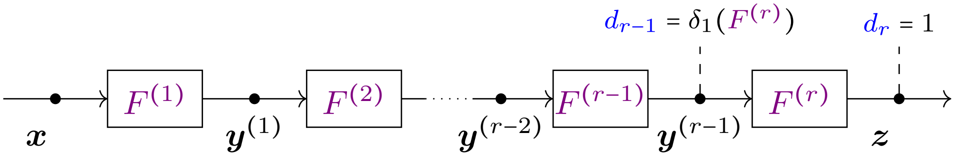
# Multi-round usage of $\delta(F)$



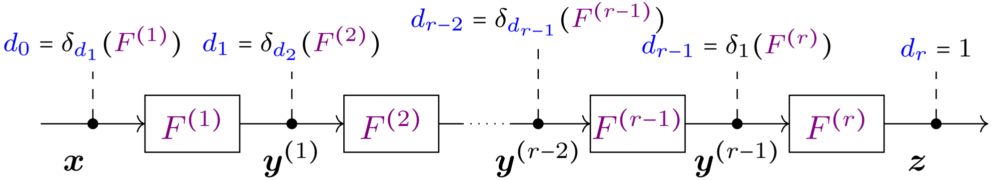
# Multi-round usage of $\delta(F)$



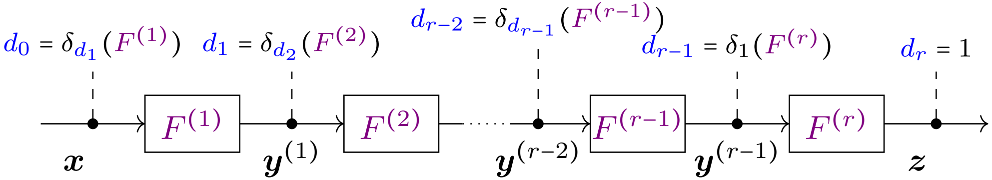
# Multi-round usage of $\delta(F)$



# Multi-round usage of $\delta(F)$



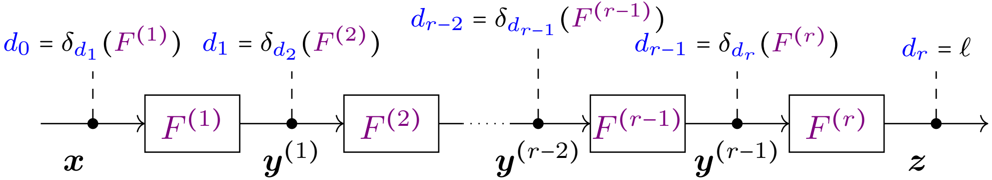
# Multi-round usage of $\delta(F)$




**Proposition**

$\deg F^{(r)} \circ F^{(r-1)} \circ \ldots \circ F^{(2)} \circ F^{(1)} \leq d_0$

# Multi-round usage of $\delta(F)$



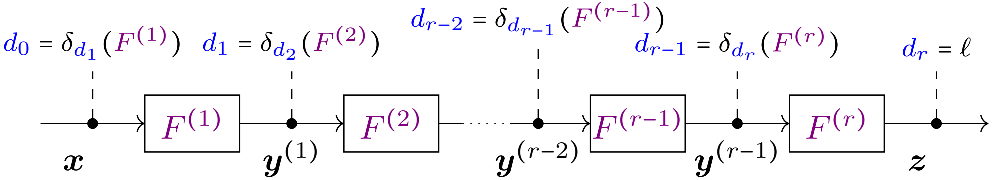

**Proposition**

$\deg F^{(r)} \circ F^{(r-1)} \circ \ldots \circ F^{(2)} \circ F^{(1)} \ \leq \ d_0$

**Proposition**

$\delta_\ell(F^{(r)} \circ F^{(r-1)} \circ \ldots \circ F^{(2)} \circ F^{(1)}) \ \leq \ d_0$ *by starting from* $d_n = \ell$

# Multi-round usage of $\delta(F)$




**Proposition**

$\deg F^{(r)} \circ F^{(r-1)} \circ \ldots \circ F^{(2)} \circ F^{(1)} \ \leq \ d_0$

**Proposition**

$\delta_\ell(F^{(r)} \circ F^{(r-1)} \circ \ldots \circ F^{(2)} \circ F^{(1)}) \ \leq \ d_0$ *by starting from* $d_n = \ell$

Going from the left requires initial guess on the degree ($d_0$)

# Word-based division property

## Definition

Let $F : (\mathbb{F}_2^n)^2 \to (\mathbb{F}_2^n)^2 : (\boldsymbol{x}_L, \boldsymbol{x}_R) \mapsto (F_L(\boldsymbol{x}_L, \boldsymbol{x}_R), F_R(\boldsymbol{x}_L, \boldsymbol{x}_R))$.

- take a product of at most $k_L$ outputs of $F_L$ and at most $k_R$ outputs of $F_R$

# Word-based division property

**Definition**

Let $F : (\mathbb{F}_2^n)^2 \to (\mathbb{F}_2^n)^2 : (\boldsymbol{x}_L, \boldsymbol{x}_R) \mapsto (F_L(\boldsymbol{x}_L, \boldsymbol{x}_R), F_R(\boldsymbol{x}_L, \boldsymbol{x}_R))$.

- take a product of at most $k_L$ outputs of $F_L$ and at most $k_R$ outputs of $F_R$
- what are the maximal degree pairs in the two input parts that can be achieved?

# Word-based division property

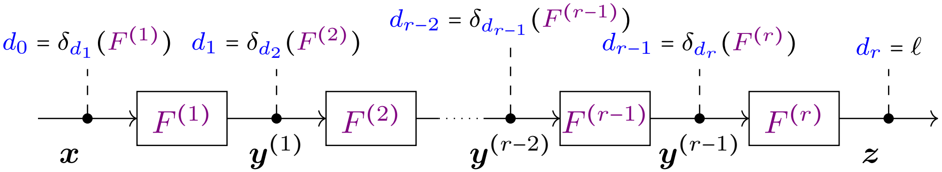
**Definition**

Let $F : (\mathbb{F}_2^n)^2 \to (\mathbb{F}_2^n)^2 : (\boldsymbol{x}_L, \boldsymbol{x}_R) \mapsto (F_L(\boldsymbol{x}_L, \boldsymbol{x}_R), F_R(\boldsymbol{x}_L, \boldsymbol{x}_R))$.

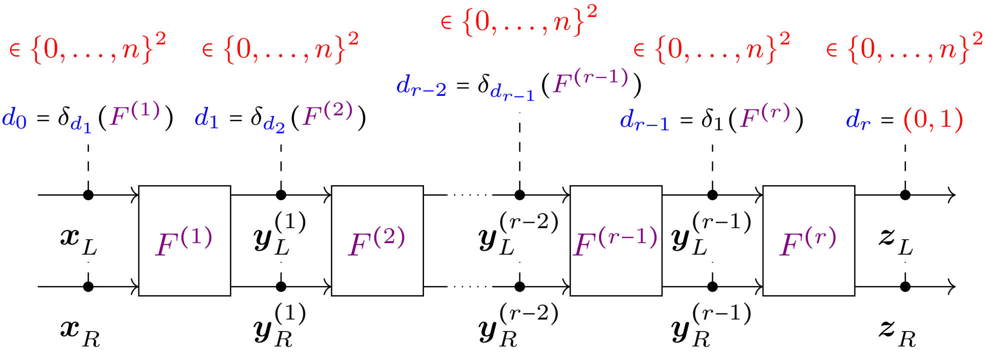
- take a product of at most $k_L$ outputs of $F_L$ and at most $k_R$ outputs of $F_R$
- what are the maximal degree pairs in the two input parts that can be achieved?

$$\begin{aligned}\delta_{k_L,k_R}(F) = \mathrm{MaxSet}\{ \ & (\mathsf{wt}\,\alpha_1, \mathsf{wt}\,\alpha_2) \\ & \mid (\beta_L, \beta_R) \in (\mathbb{F}_2^n)^2,\ \mathsf{wt}\,\beta_L \le k_L,\ \mathsf{wt}\,\beta_R \le k_R, \\ & F(\boldsymbol{x}_L, \boldsymbol{x}_R)^{\beta_L \| \beta_R} \text{ contains } x_L^{\alpha_L} x_R^{\alpha_R} \ \}\end{aligned}$$

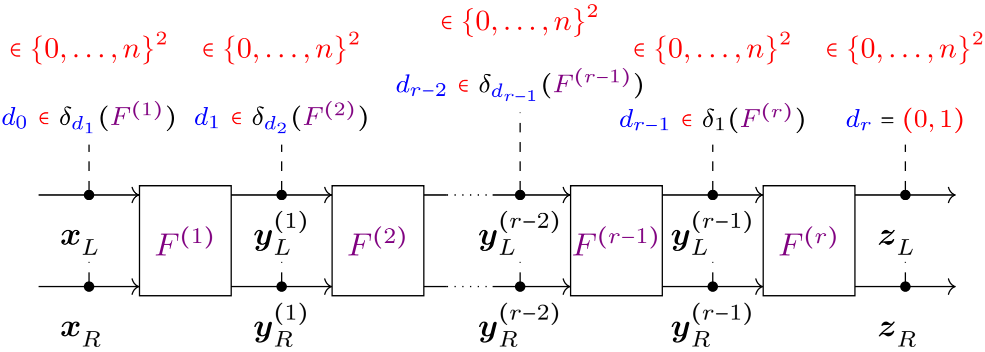
# Word-based division property - Trails



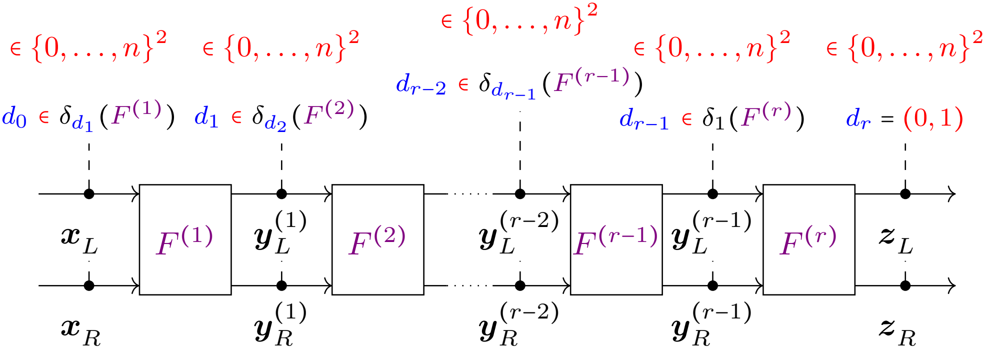
# Word-based division property - Trails



# Word-based division property - Trails



# Word-based division property - Trails

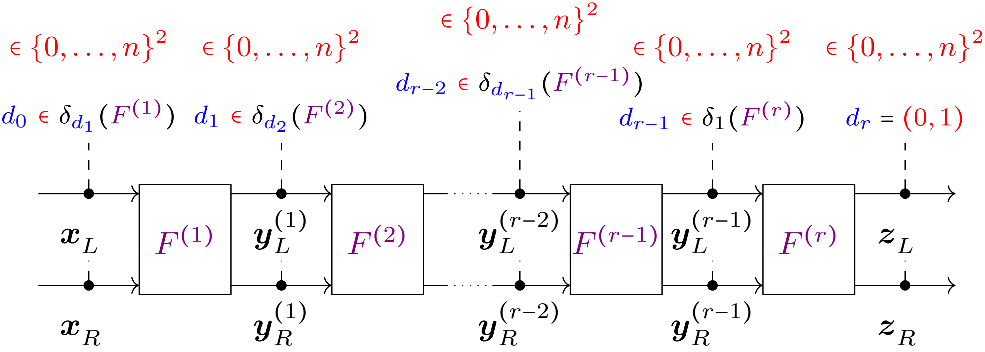



**Proposition (analogy to 1D)**

$d_0 = (k_L, k_R)$ *is a maximal reachable pair (from* $d_r = (0,1)$*)*

$\Rightarrow (F^{(r)})_R \circ F^{(r-1)} \circ \dots)(\boldsymbol{x}_L, \boldsymbol{x}_R)$ *may not contain monomials* $\boldsymbol{x}_L^{\alpha_L}\boldsymbol{x}_R^{\alpha_R}$ *with* $(\mathrm{wt}\,\alpha_L, \mathrm{wt}\,\alpha_R) \succ (k_L, k_R)$

# Word-based division property - Trails

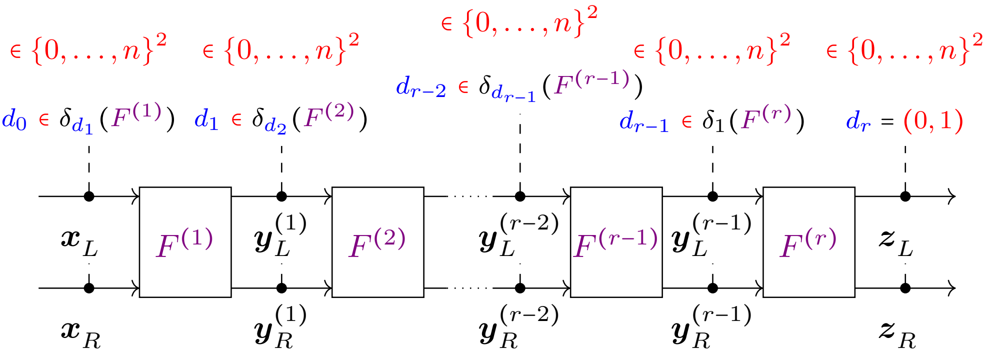



**Proposition (better phrased)**

$d_0 = (k_L, k_R)$ *can* ***NOT*** *be reached (from* $d_r = (0,1)$*)*

$\Rightarrow (F^{(r)}{}_R \circ F^{(r-1)} \circ \dots)(\boldsymbol{x}_L, \boldsymbol{x}_R)$ *does* ***NOT*** *contain monomials* $\boldsymbol{x}_L^{\alpha_L}\boldsymbol{x}_R^{\alpha_R}$
*with* $(\mathrm{wt}\,\alpha_L, \mathrm{wt}\,\alpha_R) \succeq (k_L, k_R)$

# Word-based division property - Trails

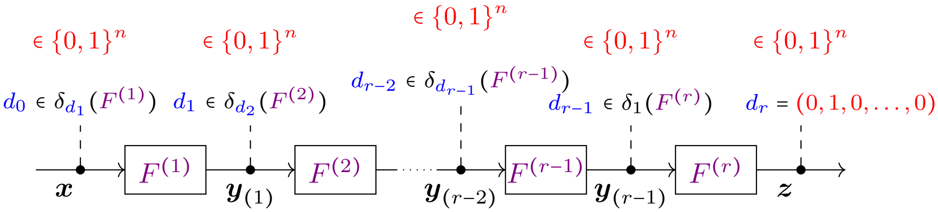



## Definition (Trail)

A sequence $(d_0, \ldots, d_r)$, $d_i \in \{0,\ldots,n\}^2$ is called a **trail** if $d_i \in \delta_{d_{i+1}}(F^{(i+1)})$ or all $i$, denoted

$$d_0 \xrightarrow{F^{(1)}} d_1 \xrightarrow{F^{(2)}} \ldots \xrightarrow{F^{(r-1)}} d_{r-1} \xrightarrow{F^{(r)}} d_r$$

# Bit-based division property (conventional)




## Definition

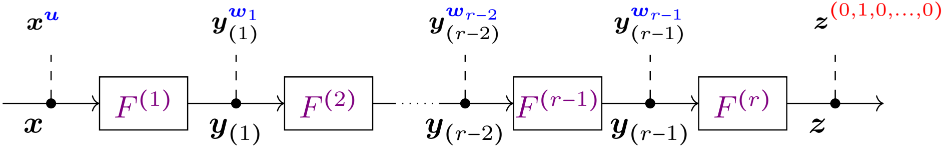
$$\delta_{\boldsymbol{k}}(F) = \mathrm{MaxSet}\{\ \boldsymbol{\alpha} \mid \boldsymbol{\beta} \preceq \boldsymbol{k},\ F(\boldsymbol{x})^{\boldsymbol{\beta}} \text{ contains } \boldsymbol{x}^{\boldsymbol{\alpha}}\ \}$$

## Proposition

*$d_0 = \boldsymbol{k}$ can **NOT** be reached (from $d_r = (0,1,0,\dots,0)$)*

*$\Rightarrow (F^{(r)}{}_2 \circ F^{(r-1)} \circ \dots)(\boldsymbol{x})$ does **NOT** contain monomial multiples of $\boldsymbol{x}^{\boldsymbol{k}}$*

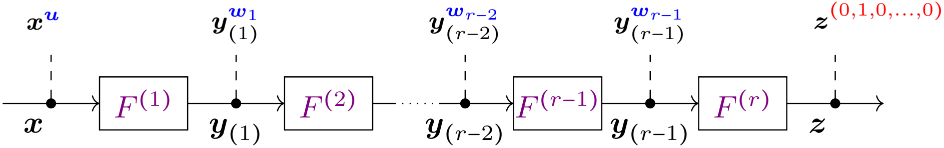
# Bit-based division property (simpler formulation, Hu, Sun, Wang, and Wang 2020)




**Definition**

$x^{u} \xrightarrow{F} y^{v}$ if $F(x)^{v}$ contains a multiple of $x^{u}$ in its ANF

# Bit-based division property (simpler formulation, Hu, Sun, Wang, and Wang 2020)




## Definition

$x^{u} \xrightarrow{F} y^{v}$ if $F(x)^{v}$ contains a multiple of $x^{u}$ in its ANF

## Proposition

*Fix* $u$, $v$. *Then,* $\nexists w_1, \ldots, w_{r-1} : (x^{u} \xrightarrow{F^{(1)}} y_{(1)}^{w_1} \to \ldots \to y_{(r-1)}^{w_{r-1}} \xrightarrow{F^{(r)}} z^{v})$
*implies* $x^{u} \xrightarrow{F^{r} \circ \ldots \circ F^{1}} z^{v}$ *does not hold (*$F(z)^{v}$ *does NOT contain a multiple of* $x^{u}$*)*

# Bound Summary (Review)

Degree bounds

Naive bound ($\deg F$)

Boura-Canteaut ($\deg F^{-1}$)

Carlet ($\deg \mathbb{1}_{\Gamma_F}$)

$\delta_k(F)$ Full $\delta(F)$ = state-based division property

$\delta_{k_L,k_R}(F)$ word-based division property

$\delta_{\boldsymbol{k}}(F)$ bit-based division property

Monomial bounds

perfect division property (bit-based)

precision

information used

computations

# Plan


Problem formulation

Degree bounds

Division property

- From state-based to bit-based
- On bit-based division property
- Computational aspects

Perfect division property and degree lower bounds

Conclusions

# Interesting properties

**Definition**

$\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow{F} \boldsymbol{y}^{\boldsymbol{v}}$ if $F(\boldsymbol{x})^{\boldsymbol{v}'}$ contains a multiple of $\boldsymbol{x}^{\boldsymbol{u}}$ in its ANF for some $\boldsymbol{v}' \preceq \boldsymbol{v}$

**Theorem (Udovenko 2021)**

*The following are equivalent:*

1. $\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow{F} \boldsymbol{y}^{\boldsymbol{v}}$
2. $\boldsymbol{y}^{\neg\boldsymbol{v}} \xrightarrow{F^{-1}} \boldsymbol{x}^{\neg\boldsymbol{u}}$
3. $\boldsymbol{x}^{\boldsymbol{u}}\boldsymbol{y}^{\neg\boldsymbol{v}}$ *divides a monomial in* $\mathbb{1}_{\Gamma_F}(\boldsymbol{x}, \boldsymbol{y})$

# Graph-indicator formulation

**Proposition (Carlet 2020)**

*Let* $F^{(i)} : \mathbb{F}_2^{m_{i-1}} \to \mathbb{F}_2^{m_i}$, $i \in \{1, \ldots, r\}$, *and* $F = F^{(r)} \circ \ldots \circ F^{(1)}$. *Then,*

$$\mathbb{1}_{\Gamma_F}(\boldsymbol{x}, \boldsymbol{z}) = \sum_{\substack{(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_{r-1}) \\ \in \mathbb{F}_2^{m_1} \times \ldots \times \mathbb{F}_2^{m_{r-1}}}} \mathbb{1}_{\Gamma_{F^{(1)}}}(\boldsymbol{x}, \boldsymbol{y}_1) \cdot \mathbb{1}_{\Gamma_{F^{(2)}}}(\boldsymbol{y}_1, \boldsymbol{y}_2) \cdot \ldots \cdot \mathbb{1}_{\Gamma_{F^{(r)}}}(\boldsymbol{y}_{r-1}, \boldsymbol{z}).$$

# Graph-indicator formulation

## Proposition (Carlet 2020)

*Let* $F^{(i)} : \mathbb{F}_2^{m_{i-1}} \to \mathbb{F}_2^{m_i}$, $i \in \{1, \ldots, r\}$, *and* $F = F^{(r)} \circ \ldots \circ F^{(1)}$. *Then,*

$$\mathbb{1}_{\Gamma_F}(\boldsymbol{x}, \boldsymbol{z}) = \sum_{\substack{(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_{r-1}) \\ \in \mathbb{F}_2^{m_1} \times \ldots \times \mathbb{F}_2^{m_{r-1}}}} \mathbb{1}_{\Gamma_{F^{(1)}}}(\boldsymbol{x}, \boldsymbol{y}_1) \cdot \mathbb{1}_{\Gamma_{F^{(2)}}}(\boldsymbol{y}_1, \boldsymbol{y}_2) \cdot \ldots \cdot \mathbb{1}_{\Gamma_{F^{(r)}}}(\boldsymbol{y}_{r-1}, \boldsymbol{z}).$$

## Theorem

$\mathbb{1}_{\Gamma_F}(\boldsymbol{x}, \boldsymbol{z})$ *contains a multiple of* $\boldsymbol{x}^{\boldsymbol{u}} \boldsymbol{z}^{\boldsymbol{v}}$ ***only if*** *there exists a monomial sequence*

$$\begin{aligned} \boldsymbol{x}^{\boldsymbol{u}'} \boldsymbol{y}_1^{\boldsymbol{w}_1} &\in \mathbb{1}_{\Gamma_{F^{(1)}}}(\boldsymbol{x}, \boldsymbol{y}_1) \\ \boldsymbol{y}_1^{\boldsymbol{w}'_1} \boldsymbol{y}_2^{\boldsymbol{w}_2} &\in \mathbb{1}_{\Gamma_{F^{(2)}}}(\boldsymbol{y}_1, \boldsymbol{y}_2) \\ &\ldots \\ \boldsymbol{y}_{r-1}^{\boldsymbol{w}'_{r-1}} \boldsymbol{z}^{\boldsymbol{v}'} &\in \mathbb{1}_{\Gamma_{F^{(2)}}}(\boldsymbol{y}_1, \boldsymbol{y}_2) \end{aligned}$$

*with* $\boldsymbol{w}_1 \vee \boldsymbol{w}'_1 = \ldots \boldsymbol{w}_{r-1} \vee \boldsymbol{w}'_{r-1} = (1, \ldots, 1)$,
$\boldsymbol{u}' \succeq \boldsymbol{u}$, $\boldsymbol{v}' \succeq \boldsymbol{v}$

# Graph-indicator formulation

**Theorem**

$\mathbb{1}_{\Gamma_F}(\boldsymbol{x}, \boldsymbol{z})$ *contains a multiple of* $\boldsymbol{x}^{\boldsymbol{u}}\boldsymbol{z}^{\boldsymbol{v}}$ ***only if*** *there exists a monomial sequence*

$$\begin{aligned} \boldsymbol{x}^{\boldsymbol{u}'}\boldsymbol{y}_1^{\boldsymbol{w}_1} &\in \mathbb{1}_{\Gamma_{F^{(1)}}}(\boldsymbol{x}, \boldsymbol{y}_1) \\ \boldsymbol{y}_1^{\boldsymbol{w}_1'}\boldsymbol{y}_2^{\boldsymbol{w}_2} &\in \mathbb{1}_{\Gamma_{F^{(2)}}}(\boldsymbol{y}_1, \boldsymbol{y}_2) \\ &\dots \\ \boldsymbol{y}_{r-1}^{\boldsymbol{w}_{r-1}'}\boldsymbol{z}^{\boldsymbol{v}'} &\in \mathbb{1}_{\Gamma_{F^{(2)}}}(\boldsymbol{y}_1, \boldsymbol{y}_2) \end{aligned}$$

*with* $\boldsymbol{w}_1 \vee \boldsymbol{w}_1' = \dots \boldsymbol{w}_{r-1} \vee \boldsymbol{w}_{r-1}' = (1, \dots, 1)$,
$\boldsymbol{u}' \succeq \boldsymbol{u}, \boldsymbol{v}' \succeq \boldsymbol{v}$

***if and only*** *there exists a division property trail*

$$\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow{F^{(1)}} \boldsymbol{y}_1^{t_1} \xrightarrow{F^{(2)}} \dots \xrightarrow{F^{(r-1)}} \boldsymbol{y}_{r-1}^{t_{r-1}} \xrightarrow{F^{(r)}} \boldsymbol{z}^{\neg\boldsymbol{v}}$$

# Plan

- Problem formulation
- Degree bounds
- Division property
  - From state-based to bit-based
  - On bit-based division property
  - Computational aspects
- Perfect division property and degree lower bounds
- Conclusions

# Computational aspects

- $\exists \boldsymbol{u}, \ldots, \boldsymbol{v} : (\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow{F^{(1)}} \ldots \xrightarrow{F^{(r)}} \boldsymbol{z}^{\boldsymbol{v}})$ ? - a search problem
- word-based : exhaustive search / dynamic programming
- bit-based : use SAT solver or MILP optimizer (integer programming)

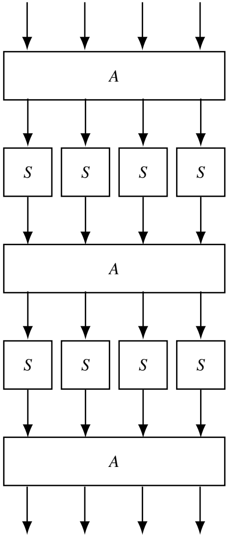
# Computational aspects

- $\exists \boldsymbol{u}, \ldots, \boldsymbol{v} : (\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow{F^{(1)}} \ldots \xrightarrow{F^{(r)}} \boldsymbol{z}^{\boldsymbol{v}})$ ? - a search problem
- word-based : exhaustive search / dynamic programming
- bit-based : use SAT solver or MILP optimizer (integer programming)

How to encode constraints of round propagation?

- parallel functions propagate separately
- precision loss: $\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow{F^{(1)}} \boldsymbol{z}^{\boldsymbol{w}} \xrightarrow{F^{(2)}} \boldsymbol{y}^{\boldsymbol{v}}$ may result in worse bounds than $\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow{F^{(2)} \circ F^{(1)}} \boldsymbol{y}^{\boldsymbol{v}}$

# Recall: SPN structure



# Model S-box

**Example**: $S : \mathbb{F}_2^8 \to \mathbb{F}_2^8$

## Generic approaches

- Compute set of valid transitions $D = \{(\boldsymbol{u}, \boldsymbol{v})\} \subseteq \mathbb{F}_2^{16}$, $\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow{S} \boldsymbol{y}^{\boldsymbol{v}}$

# Model S-box

**Example**: $S : \mathbb{F}_2^8 \to \mathbb{F}_2^8$

## Generic approaches

- Compute set of valid transitions $D = \{(\boldsymbol{u}, \boldsymbol{v})\} \subseteq \mathbb{F}_2^{16}$, $\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow{S} \boldsymbol{y}^{\boldsymbol{v}}$
- SAT: logic synthesis (Quine-McCluskey, Espresso, etc.)
- MILP: convex hull + greedy optimization

# Model S-box

**Example**: $S : \mathbb{F}_2^8 \to \mathbb{F}_2^8$

## Generic approaches

- Compute set of valid transitions $D = \{(\boldsymbol{u}, \boldsymbol{v})\} \subseteq \mathbb{F}_2^{16}$, $\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow{S} \boldsymbol{y}^{\boldsymbol{v}}$
- SAT: logic synthesis (Quine-McCluskey, Espresso, etc.)
- MILP: convex hull + greedy optimization

## Better approaches

- valid transitions are monotone $\Rightarrow$ 1 DNF clause per maximal monomial in $\mathbb{1}_{\Gamma_S}$
  $\boldsymbol{x}^{0101}\boldsymbol{y}^{0111} \quad \Rightarrow \quad (\neg u_1 \wedge \neg u_3 \wedge v_1)$

# Model S-box

**Example**: $S : \mathbb{F}_2^8 \to \mathbb{F}_2^8$

## Generic approaches

- Compute set of valid transitions $D = \{(\boldsymbol{u}, \boldsymbol{v})\} \subseteq \mathbb{F}_2^{16}$, $\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow{S} \boldsymbol{y}^{\boldsymbol{v}}$
- SAT: logic synthesis (Quine-McCluskey, Espresso, etc.)
- MILP: convex hull + greedy optimization

## Better approaches

- valid transitions are monotone $\Rightarrow$ 1 DNF clause per maximal monomial in $\mathbb{1}_{\Gamma_S}$
  $\boldsymbol{x}^{0101}\boldsymbol{y}^{0111} \quad \Rightarrow \quad (\neg u_1 \wedge \neg u_3 \wedge v_1)$
- remove redundant transitions (reduce search space): another monotone bound

# Model S-box

**Example**: $S : \mathbb{F}_2^8 \to \mathbb{F}_2^8$

## Generic approaches

- Compute set of valid transitions $D = \{(\boldsymbol{u}, \boldsymbol{v})\} \subseteq \mathbb{F}_2^{16}$, $\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow{S} \boldsymbol{y}^{\boldsymbol{v}}$
- SAT: logic synthesis (Quine-McCluskey, Espresso, etc.)
- MILP: convex hull + greedy optimization

## Better approaches

- valid transitions are monotone $\Rightarrow$ 1 DNF clause per maximal monomial in $\mathbb{1}_{\Gamma_S}$
  $\boldsymbol{x}^{0101}\boldsymbol{y}^{0111} \quad \Rightarrow \quad (\neg u_1 \wedge \neg u_3 \wedge v_1)$
- remove redundant transitions (reduce search space): another monotone bound
- 1 CNF clause is 1 inequality: (can be improved)
  $(u_0 \vee \neg u_1 \vee u_2) \iff u_0 + (1 - u_1) + u_2 \geq 1$ (binary variables)

# Model S-box

**Example**: $S : \mathbb{F}_2^8 \to \mathbb{F}_2^8$     AES S-box: $\approx 400$ CNF clauses, 27 inequalities

## Generic approaches

- Compute set of valid transitions $D = \{(\boldsymbol{u}, \boldsymbol{v})\} \subseteq \mathbb{F}_2^{16}$, $\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow{S} \boldsymbol{y}^{\boldsymbol{v}}$
- SAT: logic synthesis (Quine-McCluskey, Espresso, etc.)
- MILP: convex hull + greedy optimization

## Better approaches

- valid transitions are monotone $\Rightarrow$ 1 DNF clause per maximal monomial in $\mathbb{1}_{\Gamma_S}$
  $\boldsymbol{x}^{0101}\boldsymbol{y}^{0111} \quad \Rightarrow \quad (\neg u_1 \wedge \neg u_3 \wedge v_1)$
- remove redundant transitions (reduce search space): another monotone bound
- 1 CNF clause is 1 inequality: (can be improved)
  $(u_0 \vee \neg u_1 \vee u_2) \iff u_0 + (1 - u_1) + u_2 \geq 1$ (binary variables)

# Model linear layer

**Example**: $L : \mathbb{F}_2^{32} \to \mathbb{F}_2^{32}$

**Proposition (Zhang and Rijmen 2018)**

*$\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow{L} \boldsymbol{y}^{\boldsymbol{v}}$ and $\boldsymbol{v}$ is minimal $\iff$ the submatrix of $L$ indexed by the vectors $\boldsymbol{u}, \boldsymbol{v}$ is invertible*

# Model linear layer

**Example**: $L : \mathbb{F}_2^{32} \to \mathbb{F}_2^{32}$

**Proposition (Zhang and Rijmen 2018)**

$\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow{L} \boldsymbol{y}^{\boldsymbol{v}}$ *and* $\boldsymbol{v}$ *is minimal* $\iff$ *the submatrix of* $L$ *indexed by the vectors* $\boldsymbol{u}, \boldsymbol{v}$ *is invertible*

problem: very difficult to encode

# Model linear layer

**Example**: $L : \mathbb{F}_2^{32} \to \mathbb{F}_2^{32}$

**Proposition (Zhang and Rijmen 2018)**

$\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow{L} \boldsymbol{y}^{\boldsymbol{v}}$ *and* $\boldsymbol{v}$ *is minimal* $\iff$ *the submatrix of* $L$ *indexed by the vectors* $\boldsymbol{u}, \boldsymbol{v}$ *is invertible*

problem: very difficult to encode

solution 1: model the inverse matrix by variables, encode matrix multiplication

# Model linear layer

**Example**: $L : \mathbb{F}_2^{32} \to \mathbb{F}_2^{32}$

**Proposition (Zhang and Rijmen 2018)**

$\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow{L} \boldsymbol{y}^{\boldsymbol{v}}$ *and* $\boldsymbol{v}$ *is minimal* $\iff$ *the submatrix of* $L$ *indexed by the vectors* $\boldsymbol{u}, \boldsymbol{v}$ *is invertible*

problem: very difficult to encode

solution 1: model the inverse matrix by variables, encode matrix multiplication

solution 2: use a lossy method (decompose $L$ into XORs) and filter solutions (lazy, callback)

# Plan


Problem formulation

Degree bounds

Division property

Perfect division property and degree lower bounds

- Definition
- Computational aspects
- Proving degree lower bounds

Conclusions

# Plan


Problem formulation

Degree bounds

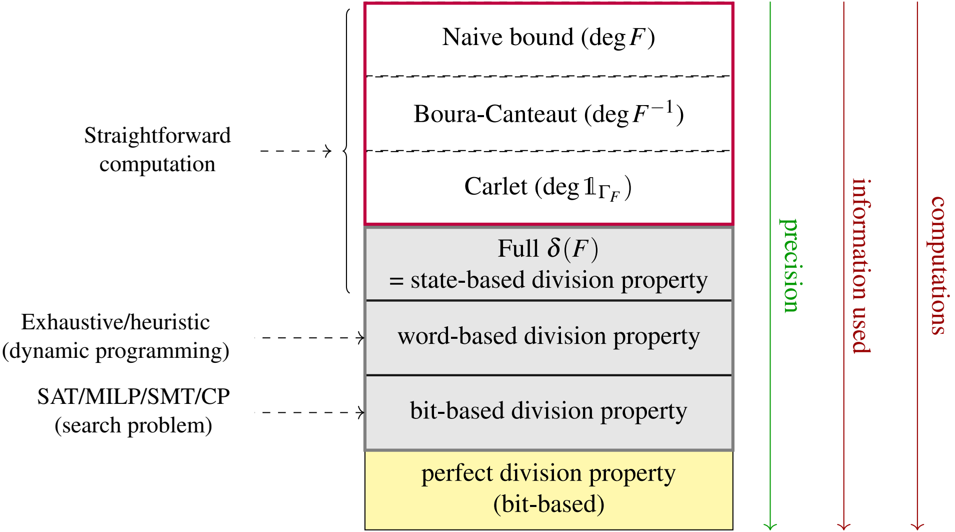
Division property

Perfect division property and degree lower bounds

- Definition
- Computational aspects
- Proving degree lower bounds

Conclusions

# Bound Summary (Review)



# Bound Summary (Review)

Straightforward computation
- Naive bound ($\deg F$)
- Boura-Canteaut ($\deg F^{-1}$)
- Carlet ($\deg \mathbb{1}_{\Gamma_F}$)
- Full $\delta(F)$ = state-based division property

Exhaustive/heuristic (dynamic programming)
- word-based division property

SAT/MILP/SMT/CP (search problem)
- bit-based division property

SAT/MILP/SMT/CP (counting problem)
- perfect division property (bit-based)

precision

information used

computations

# Perfect division property

**Definition**

$\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow{F} \boldsymbol{y}^{\boldsymbol{v}}$ if $F(\boldsymbol{x})^{\boldsymbol{v}'}$ contains a multiple of $\boldsymbol{x}^{\boldsymbol{u}}$ in its ANF for some $\boldsymbol{v}' \preceq \boldsymbol{v}$

# Perfect division property

**Definition**

$\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow[\text{exact}]{F} \boldsymbol{y}^{\boldsymbol{v}}$ if $F(\boldsymbol{x})^{\boldsymbol{v}}$ contains ~~a multiple of~~ $\boldsymbol{x}^{\boldsymbol{u}}$ in its ANF ~~for some~~ $\cancel{\boldsymbol{v}' \preceq \boldsymbol{v}}$

# Perfect division property

**Definition**

$\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow[\text{exact}]{F} \boldsymbol{y}^{\boldsymbol{v}}$ if $F(\boldsymbol{x})^{\boldsymbol{v}}$ contains $\boldsymbol{x}^{\boldsymbol{u}}$ in its ANF

# Perfect division property

## Definition

$\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow[\text{exact}]{F} \boldsymbol{y}^{\boldsymbol{v}}$ if $F(\boldsymbol{x})^{\boldsymbol{v}}$ contains $\boldsymbol{x}^{\boldsymbol{u}}$ in its ANF

## Theorem (Hu, Sun, Wang, and Wang 2020)

*A trail*

$$\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow[\text{exact}]{F^{(r)} \circ F^{(r-1)} \circ \ldots \circ F^{(1)}} \boldsymbol{z}^{\boldsymbol{v}}$$

*is valid **if and only if** the total number of trails*

$$\boldsymbol{x}^{\boldsymbol{u}} \xrightarrow[\text{exact}]{F^{(1)}} \boldsymbol{y}_{(1)}^{\boldsymbol{w}_1} \xrightarrow[\text{exact}]{F^{(2)}} \cdots \xrightarrow[\text{exact}]{F^{(r-1)}} \boldsymbol{y}_{(r-1)}^{\boldsymbol{w}_{r-1}} \xrightarrow[\text{exact}]{F^{(s)}} \boldsymbol{z}^{\boldsymbol{v}}$$

*is odd (trail = vector $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{r-1})$)*

# Plan


Problem formulation

Degree bounds

Division property

Perfect division property and degree lower bounds

- Definition
- Computational aspects
- Proving degree lower bounds

Conclusions

# Computational aspects

- SAT/MILP models: similar, but have to use generic models (not monotone anymore)
- Have to count trails: feasible only in a few cases (small block size/small number of rounds)
- Have to include keys as variables (all previous techniques were key-agnostic)

# Plan


Problem formulation

Degree bounds

Division property

Perfect division property and degree lower bounds

- Definition
- Computational aspects
- Proving degree lower bounds

Conclusions

# Proving degree lower bounds (1)

Let $E(\boldsymbol{x}, \boldsymbol{k}) : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{F}_2^n$ be a keyed permutation. We want to prove absence of *integral distinguishers*:

**Definition (Integral resistance)**

For any set of inputs $\emptyset \subsetneq X \subsetneq \mathbb{F}_2^n$ and any $\boldsymbol{\beta} \in \mathbb{F}_2^n \setminus \{0\}$, the function $\sum_{\boldsymbol{x} \in X} \langle \boldsymbol{\beta}, E(\boldsymbol{x}, \boldsymbol{k}) \rangle$ is strictly key dependent.

# Proving degree lower bounds (1)

Let $E(\boldsymbol{x}, \boldsymbol{k}) : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{F}_2^n$ be a keyed permutation. We want to prove absence of *integral distinguishers*:

**Definition (Integral resistance)**

For any set of inputs $\emptyset \subsetneq X \subsetneq \mathbb{F}_2^n$ and any $\beta \in \mathbb{F}_2^n \setminus \{0\}$, the function $\sum_{\boldsymbol{x} \in X} \langle \beta, E(\boldsymbol{x}, \boldsymbol{k}) \rangle$ is strictly key dependent.

**Theorem (Hebborn, Lambin, Leander, and Todo 2021)**

*It is sufficient to require that* $\forall \boldsymbol{u}, \beta \in \mathbb{F}_2^n$ *the coefficient of* $\boldsymbol{x}^{\boldsymbol{u}}$ *in* $\langle \beta, E(\boldsymbol{x}, \boldsymbol{k}) \rangle$ *is a non-constant function of the key, and all these functions are linearly independent* $(\boldsymbol{u} \neq (1, \ldots, 1), \beta \neq (0, \ldots, 0))$

# Proving degree lower bounds (2)

**Definition (Integral resistance matrix: Hebborn, Lambin, Leander, and Todo 2021)**

Let $\lambda_{i,j;\boldsymbol{v}}$ denote the coefficient of $\boldsymbol{x}^{\neg \boldsymbol{e}_j} \boldsymbol{k}^{\boldsymbol{v}}$ in $E_i(\boldsymbol{x}, \boldsymbol{k})$. For some vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s$ let

$$\mathcal{I} = \begin{pmatrix} \lambda_{1,1;\boldsymbol{v_1}} & \lambda_{1,1;\boldsymbol{v_2}} & \cdots & \lambda_{1,1;\boldsymbol{v}_s} \\ \lambda_{2,1;\boldsymbol{v_1}} & \lambda_{2,1;\boldsymbol{v_2}} & \cdots & \lambda_{2,1;\boldsymbol{v}_s} \\ & \vdots & & \\ \lambda_{n,1;\boldsymbol{v_1}} & \lambda_{n,1;\boldsymbol{v_2}} & \cdots & \lambda_{n,1;\boldsymbol{v}_s} \\ \lambda_{1,2;\boldsymbol{v_1}} & \lambda_{1,2;\boldsymbol{v_2}} & \cdots & \lambda_{1,2;\boldsymbol{v}_s} \\ \lambda_{2,2;\boldsymbol{v_1}} & \lambda_{1,2;\boldsymbol{v_2}} & \cdots & \lambda_{2,2;\boldsymbol{v}_s} \\ & \vdots & & \\ \lambda_{i,j;\boldsymbol{v_1}} & \lambda_{i,j;\boldsymbol{v_2}} & \cdots & \lambda_{i,j;\boldsymbol{v}_s} \\ & \vdots & & \\ \lambda_{n-1,n;\boldsymbol{v_1}} & \lambda_{n-1,n;\boldsymbol{v_2}} & \cdots & \lambda_{n-1,n;\boldsymbol{v}_s} \end{pmatrix} \in \mathbb{F}_2^{n^2 \times s}$$

# Proving degree lower bounds (3)

**Theorem (Hebborn, Lambin, Leander, and Todo 2021)**

*If there exists an integral resistance matrix $I$ of full rank $n^2$ for $E(\boldsymbol{x}, \boldsymbol{k})$, then $E'(\boldsymbol{x}, \boldsymbol{k} || \boldsymbol{k'}) = E(\boldsymbol{x} + \boldsymbol{k'}, \boldsymbol{k}) : \mathbb{F}_2^n \times \mathbb{F}_2^{m'} \times \mathbb{F}_2^m$ is integral resistant.*

# Proving degree lower bounds (3)

**Theorem (Hebborn, Lambin, Leander, and Todo 2021)**

*If there exists an integral resistance matrix $I$ of full rank $n^2$ for $E(\boldsymbol{x}, \boldsymbol{k})$, then $E'(\boldsymbol{x}, \boldsymbol{k}||\boldsymbol{k'}) = E(\boldsymbol{x} + \boldsymbol{k'}, \boldsymbol{k}) : \mathbb{F}_2^n \times \mathbb{F}_2^{m'} \times \mathbb{F}_2^m$ is integral resistant.*

Extra whitening key $\boldsymbol{k'}$: translate key-dependence from maximal monomials to lower-degree monomials

Example: $x_1 x_2 x_3$ becomes $(x_1 + \boldsymbol{k'}_1)(x_2 + \boldsymbol{k'}_2)(x_3 + \boldsymbol{k'}_3)$ with all $2^3$ functions (from fixing $x$) being linearly independent

# Proving degree lower bounds (3)

**Theorem (Hebborn, Lambin, Leander, and Todo 2021)**

*If there exists an integral resistance matrix $I$ of full rank $n^2$ for $E(\boldsymbol{x}, \boldsymbol{k})$, then $E'(\boldsymbol{x}, \boldsymbol{k} \| \boldsymbol{k'}) = E(\boldsymbol{x} + \boldsymbol{k'}, \boldsymbol{k}) : \mathbb{F}_2^n \times \mathbb{F}_2^{m'} \times \mathbb{F}_2^m$ is integral resistant.*

Extra whitening key $\boldsymbol{k'}$: translate key-dependence from maximal monomials to lower-degree monomials

Example: $x_1 x_2 x_3$ becomes $(x_1 + \boldsymbol{k'}_1)(x_2 + \boldsymbol{k'}_2)(x_3 + \boldsymbol{k'}_3)$ with all $2^3$ functions (from fixing $x$) being linearly independent

Cost: $\geq n^4$ calls to perfect division property (parity counting)

Optimization: carefully choose key monomials (the $\boldsymbol{v}_i$) to aid computations

# Plan


Problem formulation

Degree bounds

Division property

Perfect division property and degree lower bounds

Conclusions

# Open problem - extended representation

Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ for a small $n$, e.g. $n = 4, 8$

# Open problem - extended representation

Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ for a small $n$, e.g. $n = 4, 8$

$\mathbb{1}_{\Gamma_S}$ typically has few maximal monomials $\boldsymbol{x}^{\boldsymbol{u}}\boldsymbol{y}^{\boldsymbol{v}}$

# Open problem - extended representation

Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ for a small $n$, e.g. $n = 4, 8$

$\mathbb{1}_{\Gamma_S}$ typically has few maximal monomials $\boldsymbol{x}^{\boldsymbol{u}} \boldsymbol{y}^{\boldsymbol{v}}$

For linear maps $A$, $B$, maximal monomials of $\mathbb{1}_{\Gamma_{B \circ S \circ A}}$ can not be computed from $\mathrm{MaxSet}(\mathbb{1}_{\Gamma_S})$ (in general)

# Open problem - extended representation

Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ for a small $n$, e.g. $n = 4, 8$

$\mathbb{1}_{\Gamma_S}$ typically has few maximal monomials $\boldsymbol{x}^{\boldsymbol{u}} \boldsymbol{y}^{\boldsymbol{v}}$

For linear maps $A$, $B$, maximal monomials of $\mathbb{1}_{\Gamma_{B \circ S \circ A}}$ can not be computed from $\mathrm{MaxSet}(\mathbb{1}_{\Gamma_S})$ (in general)

Question: how to represent all such sets compactly?

## Conclusions

- division property is a powerful technique for degree/monomial bounds
- information/precision/computations trade-off
- links to theory (graph indicators)

## Conclusions

- division property is a powerful technique for degree/monomial bounds
- information/precision/computations trade-off
- links to theory (graph indicators)

## Open problems

- represent $\mathrm{MaxSet}(\mathbb{1}_{\Gamma_{B \circ S \circ A}})$ for all linear $A, B$ compactly
- computational hardness (conventional division property)
- better handling of large linear maps
- generalization to non-binary fields

# Conclusions

## Conclusions

- division property is a powerful technique for degree/monomial bounds
- information/precision/computations trade-off
- links to theory (graph indicators)

## Open problems

- represent $\mathrm{MaxSet}(\mathbb{1}_{\Gamma_{B \circ S \circ A}})$ for all linear $A, B$ compactly
- computational hardness (conventional division property)
- better handling of large linear maps
- generalization to non-binary fields

**C.f. survey "Mathematical aspects of division property" (CCDS 2023)**

# References i


- Boura, Christina and Anne Canteaut (2013). "On the Influence of the Algebraic Degree of $F^{-1}$ on the Algebraic Degree of G ∘ F". In: *IEEE Transactions on Information Theory* 59.1, pp. 691–702.
- Boura, Christina, Anne Canteaut, and Christophe De Cannière (Feb. 2011). "Higher-Order Differential Properties of Keccak and Luffa". In: *FSE 2011*. Ed. by Antoine Joux. Vol. 6733. LNCS. Springer, Heidelberg, pp. 252–269. doi: 10.1007/978-3-642-21702-9_15.
- Carlet, Claude (2020). "Graph indicators of vectorial functions and bounds on the algebraic degree of composite functions". In: *IEEE Transactions on Information Theory*, pp. 1–1. doi: 10.1109/TIT.2020.3017494.

- Hebborn, Phil, Baptiste Lambin, Gregor Leander, and Yosuke Todo (Dec. 2021). "Strong and Tight Security Guarantees Against Integral Distinguishers". In: *ASIACRYPT 2021, Part I*. Ed. by Mehdi Tibouchi and Huaxiong Wang. Vol. 13090. LNCS. Springer, Heidelberg, pp. 362–391. doi: 10.1007/978-3-030-92062-3_13.
- Hu, Kai, Siwei Sun, Meiqin Wang, and Qingju Wang (Dec. 2020). "An Algebraic Formulation of the Division Property: Revisiting Degree Evaluations, Cube Attacks, and Key-Independent Sums". In: *ASIACRYPT 2020, Part I*. Ed. by Shiho Moriai and Huaxiong Wang. Vol. 12491. LNCS. Springer, Heidelberg, pp. 446–476. doi: 10.1007/978-3-030-64837-4_15.

Udovenko, Aleksei (Dec. 2021). "Convexity of Division Property Transitions: Theory, Algorithms and Compact Models". In: *ASIACRYPT 2021, Part I*. Ed. by Mehdi Tibouchi and Huaxiong Wang. Vol. 13090. LNCS. Springer, Heidelberg, pp. 332–361. doi: 10.1007/978-3-030-92062-3_12.

Zhang, Wenying and Vincent Rijmen (Aug. 2018). "Division Cryptanalysis of Block Ciphers with a Binary Diffusion Layer". In: *IET Information Security* 13.2, pp. 87–95. issn: 1751-8717.