Radboud University

An (almost) golden Kaisa S-box layer over $\mathbb{F}_q$ for odd q

D. Verbakel[1] D. Kuijsters[1] S. Mella[1] S. Picek[1] L. Mariot[2] J. Daemen[1]

BFA, September 7, 2023

Voss, Norway

Radboud University, NL

University of Twente, NL

ESCADA

Looking for a super-symmetric S-box

Let's call an S-box over $\mathbb{F}_{p^n}$ a golden Kaisa S-box if:

1. mask and difference propagation is governed by the same rules
2. forward and backward propagation is the same
3. every differential has DP $\leq p^{-n}/2$ and every linear approximation LP $\leq p^{-n}/2$

Looking for a super-symmetric S-box

Let's call an S-box over $\mathbb{F}_{p^n}$ a golden Kaisa S-box if:

1. mask and difference propagation is governed by the same rules
2. forward and backward propagation is the same
3. every differential has DP $\leq p^{-n}/2$ and every linear approximation LP $\leq p^{-n}/2$

- Can we find such a layer with S-boxes over $\mathbb{F}_{p^n}$ with $p^n \neq 8$?

Looking for a super-symmetric S-box

Let's call an S-box over $\mathbb{F}_{p^n}$ a golden Kaisa S-box if:

1. mask and difference propagation is governed by the same rules
2. forward and backward propagation is the same
3. every differential has DP $\leq p^{-n}/2$ and every linear approximation LP $\leq p^{-n}/2$

- Can we find such a layer with S-boxes over $\mathbb{F}_{p^n}$ with $p^n \neq 8$?
- For $p = 2$ it is not likely

Looking for a super-symmetric S-box

Let's call an S-box over $\mathbb{F}_{p^n}$ a golden Kaisa S-box if:

1. mask and difference propagation is governed by the same rules
2. forward and backward propagation is the same
3. every differential has DP $\leq p^{-n}/2$ and every linear approximation LP $\leq p^{-n}/2$

- Can we find such a layer with S-boxes over $\mathbb{F}_{p^n}$ with $p^n \neq 8$?
- For $p = 2$ it is not likely
- But what about p odd?

Difference and mask propagation properties of a transformation of $\mathbb{F}_{p^n}$

Differential probability (DP) of a differential (a, b)

$$\mathrm{DP}(a, b) = \frac{\#\{x \in \mathbb{F}_{p^n} \mid f(x + a) - f(x) = b\}}{p^n}$$

Correlation and *linear potential* (LP) of a linear approximation (a, b)

$$\mathrm{C}(a, b) = \frac{\sum_x \omega^{\mathrm{Tr}(ax - bf(x))}}{p^n} \text{ with } \omega = e^{\frac{2\pi i}{p}}$$

$$\mathrm{LP}(a, b) = \mathrm{C}(a, b)\overline{\mathrm{C}}(a, b)$$

Power function in $\mathbb{F}_{p^n}$

Power function in $\mathbb{F}_{p^n}$

- Power functions seem like a good place to start

Power function in $\mathbb{F}_{p^n}$

- Power functions seem like a good place to start
- Smallest exponent higher than 1: $e = 2$

Power function in $\mathbb{F}_{p^n}$

- Power functions seem like a good place to start
- Smallest exponent higher than 1: $e = 2$
- For $p = 2$ this gives a linear function

Power function in $\mathbb{F}_{p^n}$

- Power functions seem like a good place to start
- Smallest exponent higher than 1: $e = 2$
- For $p = 2$ this gives a linear function
- For odd p this is non-linear

Power function in $\mathbb{F}_{p^n}$

- Power functions seem like a good place to start
- Smallest exponent higher than 1: $e = 2$
- For $p = 2$ this gives a linear function
- For odd p this is non-linear
- Let us investigate DP and LP

Differential probabilities of squaring in $\mathbb{F}_{p^n}$ with odd p

Differential probabilities of squaring in $\mathbb{F}_{p^n}$ with odd p

$$\begin{aligned}
\mathrm{DP}(a, b) &= p^{-n} \# \{x \mid (x + a)^2 - x^2 = b\} \\
&= p^{-n} \# \{x \mid 2ax + a^2 = b\} \\
&= p^{-n} \# \{x \mid x = \frac{b}{2a} - \frac{a}{2}\} \\
&= p^{-n}
\end{aligned}$$

Differential probabilities of squaring in $\mathbb{F}_{p^n}$ with odd p

$$
\begin{aligned}
\mathrm{DP}(a,b) &= p^{-n}\#\{x \mid (x+a)^2 - x^2 = b\} \\
&= p^{-n}\#\{x \mid 2ax + a^2 = b\} \\
&= p^{-n}\#\{x \mid x = \frac{b}{2a} - \frac{a}{2}\} \\
&= p^{-n}
\end{aligned}
$$

- Summarizing:
  - $\forall a \neq 0, b : \mathrm{DP}(a,b) = p^{-n}$
  - $\forall b \neq 0 : \mathrm{DP}(0,b) = 0$ and $\mathrm{DP}(0,0) = 1$

Differential probabilities of squaring in $\mathbb{F}_{p^n}$ with odd p

$$\begin{aligned}\mathrm{DP}(a,b) &= p^{-n}\#\{x \mid (x+a)^2 - x^2 = b\} \\ &= p^{-n}\#\{x \mid 2ax + a^2 = b\} \\ &= p^{-n}\#\{x \mid x = \frac{b}{2a} - \frac{a}{2}\} \\ &= p^{-n}\end{aligned}$$

- Summarizing:
  - $\forall a \neq 0, b : \mathrm{DP}(a,b) = p^{-n}$
  - $\forall b \neq 0 : \mathrm{DP}(0,b) = 0$ and $\mathrm{DP}(0,0) = 1$
- Non-invertible: any non-zero difference can propagate to 0

Differential probabilities of squaring in $\mathbb{F}_{p^n}$ with odd p

$$
\begin{aligned}
\mathrm{DP}(a, b) &= p^{-n} \#\{x \mid (x+a)^2 - x^2 = b\} \\
&= p^{-n} \#\{x \mid 2ax + a^2 = b\} \\
&= p^{-n} \#\{x \mid x = \frac{b}{2a} - \frac{a}{2}\} \\
&= p^{-n}
\end{aligned}
$$

- Summarizing:
  - $\forall a \neq 0, b : \mathrm{DP}(a, b) = p^{-n}$
  - $\forall b \neq 0 : \mathrm{DP}(0, b) = 0$ and $\mathrm{DP}(0, 0) = 1$
- Non-invertible: any non-zero difference can propagate to 0
- $\mathrm{DP}(a, b) = \mathrm{DP}(b, a)$ if $a \neq 0$ and $b \neq 0$

Let us try correlation

Let us try correlation

$\mathrm{C}(a, b) = p^{-n} \sum_x \omega^{\mathrm{Tr}(ax - bx^2)}$

Let us try correlation

$\mathrm{C}(a, b) = p^{-n} \sum_x \omega^{\mathrm{Tr}(ax - bx^2)}$ Hmmm . . .

Let us try correlation

$\mathrm{C}(a, b) = p^{-n} \sum_x \omega^{\mathrm{Tr}(ax - bx^2)}$ Hmmm ... where to start??

Let us try correlation

$\mathrm{C}(a,b) = p^{-n}\sum_x \omega^{\mathrm{Tr}(ax-bx^2)}$ Hmmm ... where to start??

We find in [Lidl & Niederreiter 1997] Theorem 5.33 and can derive from that

$$\mathrm{C}(a,b) = \frac{1}{p^n}\sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}(bx^2-ax)} = \begin{cases} \frac{(-1)^{d-1}}{\sqrt{p^n}}\omega^{\mathrm{Tr}(-a^2(4b)^{-1})}\eta(b) & \text{if } p\equiv 1 \pmod 4 \\ \frac{(-1)^{d-1}}{\sqrt{p^n}} i^d \omega^{\mathrm{Tr}(-a^2(4b)^{-1})}\eta(b) & \text{if } p\equiv 3 \pmod 4 \end{cases}$$

with $\eta(b) = 1$ if b is a square in $\mathbb{F}_{p^n}$ and -1 otherwise.

Let us try correlation

$\mathrm{C}(a,b) = p^{-n} \sum_x \omega^{\mathrm{Tr}(ax-bx^2)}$ Hmmm . . . where to start??

We find in [Lidl & Niederreiter 1997] Theorem 5.33 and can derive from that

$$\mathrm{C}(a,b) = \frac{1}{p^n} \sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}(bx^2-ax)} = \begin{cases} \frac{(-1)^{d-1}}{\sqrt{p^n}} \omega^{\mathrm{Tr}(-a^2(4b)^{-1})} \eta(b) & \text{if } p \equiv 1 \pmod 4 \\ \frac{(-1)^{d-1}}{\sqrt{p^n}} i^d \omega^{\mathrm{Tr}(-a^2(4b)^{-1})} \eta(b) & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

with $\eta(b) = 1$ if b is a square in $\mathbb{F}_{p^n}$ and -1 otherwise.

- From this it follows that:

Let us try correlation

$\mathrm{C}(a,b) = p^{-n}\sum_x \omega^{\mathrm{Tr}(ax-bx^2)}$ Hmmm ... where to start??

We find in [Lidl & Niederreiter 1997] Theorem 5.33 and can derive from that

$$\mathrm{C}(a,b) = \frac{1}{p^n}\sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}(bx^2-ax)} = \begin{cases} \frac{(-1)^{d-1}}{\sqrt{p^n}}\omega^{\mathrm{Tr}(-a^2(4b)^{-1})}\eta(b) & \text{if } p\equiv 1 \pmod 4 \\ \frac{(-1)^{d-1}}{\sqrt{p^n}}i^d\omega^{\mathrm{Tr}(-a^2(4b)^{-1})}\eta(b) & \text{if } p\equiv 3 \pmod 4 \end{cases}$$

with $\eta(b)=1$ if b is a square in $\mathbb{F}_{p^n}$ and -1 otherwise.

- From this it follows that:
  - $\forall b\neq 0, a : \mathrm{LP}(a,b) = p^{-n}$
  - $\forall a\neq 0 : \mathrm{LP}(a,0) = 0$ and $\mathrm{LP}(0,0) = 1$

Let us try correlation

$\mathrm{C}(a,b) = p^{-n}\sum_x \omega^{\mathrm{Tr}(ax-bx^2)}$ Hmmm ... where to start??

We find in [Lidl & Niederreiter 1997] Theorem 5.33 and can derive from that

$$\mathrm{C}(a,b) = \frac{1}{p^n}\sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}(bx^2-ax)} = \begin{cases} \frac{(-1)^{d-1}}{\sqrt{p^n}}\omega^{\mathrm{Tr}(-a^2(4b)^{-1})}\eta(b) & \text{if } p\equiv 1 \pmod 4 \\ \frac{(-1)^{d-1}}{\sqrt{p^n}} i^d \omega^{\mathrm{Tr}(-a^2(4b)^{-1})}\eta(b) & \text{if } p\equiv 3 \pmod 4 \end{cases}$$

with $\eta(b) = 1$ if b is a square in $\mathbb{F}_{p^n}$ and -1 otherwise.

- From this it follows that:
  - $\forall b \neq 0, a : \mathrm{LP}(a,b) = p^{-n}$
  - $\forall a \neq 0 : \mathrm{LP}(a,0) = 0$ and $\mathrm{LP}(0,0) = 1$
- Imbalanced: all output masks are correlated to zero input mask

Let us try correlation

$\mathrm{C}(a,b) = p^{-n}\sum_x \omega^{\mathrm{Tr}(ax-bx^2)}$ Hmmm ... where to start??

We find in [Lidl & Niederreiter 1997] Theorem 5.33 and can derive from that

$$\mathrm{C}(a,b) = \frac{1}{p^n}\sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}(bx^2-ax)} = \begin{cases} \frac{(-1)^{d-1}}{\sqrt{p^n}}\omega^{\mathrm{Tr}(-a^2(4b)^{-1})}\eta(b) & \text{if } p\equiv 1 \pmod 4 \\ \frac{(-1)^{d-1}}{\sqrt{p^n}} i^d \omega^{\mathrm{Tr}(-a^2(4b)^{-1})}\eta(b) & \text{if } p\equiv 3 \pmod 4 \end{cases}$$

with $\eta(b) = 1$ if b is a square in $\mathbb{F}_{p^n}$ and -1 otherwise.

- From this it follows that:
  - $\forall b \neq 0, a : \mathsf{LP}(a,b) = p^{-n}$
  - $\forall a \neq 0 : \mathsf{LP}(a,0) = 0$ and $\mathsf{LP}(0,0) = 1$
- Imbalanced: all output masks are correlated to zero input mask
- $\mathsf{LP}(a,b) = \mathsf{LP}(b,a)$ if $a \neq 0$ and $b \neq 0$

Does it satisfy the criteria?

The three criteria are (almost) satisfied for any p and n:

Does it satisfy the criteria?

The three criteria are (almost) satisfied for any p and n:

1. forward propagation of differences and backward propagation of masks and vice versa follow the same rules:

Does it satisfy the criteria?

The three criteria are (almost) satisfied for any p and n:

1. forward propagation of differences and backward propagation of masks and vice versa follow the same rules: yes!

Does it satisfy the criteria?

The three criteria are (almost) satisfied for any p and n:

1. forward propagation of differences and backward propagation of masks and vice versa follow the same rules: yes!
2. forward and backward propagation is the same, *except for zero output differences and input masks*:

Does it satisfy the criteria?

The three criteria are (almost) satisfied for any p and n:

1. forward propagation of differences and backward propagation of masks and vice versa follow the same rules: yes!
2. forward and backward propagation is the same, *except for zero output differences and input masks*: almost

Does it satisfy the criteria?

The three criteria are (almost) satisfied for any p and n:

1. forward propagation of differences and backward propagation of masks and vice versa follow the same rules: yes!
2. forward and backward propagation is the same, *except for zero output differences and input masks*: almost
3. every differential has $\text{DP} = p^{-n}$ and every linear approximation $\text{LP} = p^{-n}$:

Does it satisfy the criteria?

The three criteria are (almost) satisfied for any p and n:

1. forward propagation of differences and backward propagation of masks and vice versa follow the same rules: yes!
2. forward and backward propagation is the same, *except for zero output differences and input masks*: almost
3. every differential has $\text{DP} = p^{-n}$ and every linear approximation $\text{LP} = p^{-n}$: even better!

Does it satisfy the criteria?

The three criteria are (almost) satisfied for any p and n:

1. forward propagation of differences and backward propagation of masks and vice versa follow the same rules: yes!
2. forward and backward propagation is the same, *except for zero output differences and input masks*: almost
3. every differential has $\mathrm{DP} = p^{-n}$ and every linear approximation $\mathrm{LP} = p^{-n}$: even better!

Now let us try to build an S-box layer from that!

An S-box layer of squaring in $\mathbb{F}_{p^n}$

An S-box layer of squaring in $\mathbb{F}_{p^n}$

- Input differences a active in a single S-box have $\mathrm{DP}(a, 0) = p^{-n}$

An S-box layer of squaring in $\mathbb{F}_{p^n}$

- Input differences a active in a single S-box have $\mathrm{DP}(a, 0) = p^{-n}$
  - in most constructions the adversary can apply such differences

An S-box layer of squaring in $\mathbb{F}_{p^n}$

- Input differences a active in a single S-box have $\mathrm{DP}(a, 0) = p^{-n}$
  - in most constructions the adversary can apply such differences
  - presence of a collision is easy to detect and can be used as a distinguisher

An S-box layer of squaring in $\mathbb{F}_{p^n}$

- Input differences a active in a single S-box have $\mathrm{DP}(a, 0) = p^{-n}$
  - in most constructions the adversary can apply such differences
  - presence of a collision is easy to detect and can be used as a distinguisher
  - unacceptable weakness

An S-box layer of squaring in $\mathbb{F}_{p^n}$

- Input differences a active in a single S-box have $\mathrm{DP}(a, 0) = p^{-n}$
  - in most constructions the adversary can apply such differences
  - presence of a collision is easy to detect and can be used as a distinguisher
  - unacceptable weakness
- Output masks b restricted to a single S-box have $\mathrm{LP}(0, b) = p^{-n}$

An S-box layer of squaring in $\mathbb{F}_{p^n}$

- Input differences a active in a single S-box have $\mathrm{DP}(a, 0) = p^{-n}$
  - in most constructions the adversary can apply such differences
  - presence of a collision is easy to detect and can be used as a distinguisher
  - unacceptable weakness
- Output masks b restricted to a single S-box have $\mathrm{LP}(0, b) = p^{-n}$
  - measurable bias in the output

An S-box layer of squaring in $\mathbb{F}_{p^n}$

- Input differences a active in a single S-box have $\mathrm{DP}(a, 0) = p^{-n}$
  - in most constructions the adversary can apply such differences
  - presence of a collision is easy to detect and can be used as a distinguisher
  - unacceptable weakness
- Output masks b restricted to a single S-box have $\mathrm{LP}(0, b) = p^{-n}$
  - measurable bias in the output
  - phases of bias allow determining *whitening key*, etc.

An S-box layer of squaring in $\mathbb{F}_{p^n}$

- Input differences a active in a single S-box have $\mathrm{DP}(a, 0) = p^{-n}$
  - in most constructions the adversary can apply such differences
  - presence of a collision is easy to detect and can be used as a distinguisher
  - unacceptable weakness
- Output masks b restricted to a single S-box have $\mathrm{LP}(0, b) = p^{-n}$
  - measurable bias in the output
  - phases of bias allow determining *whitening key*, etc.
  - unacceptable weakness

An S-box layer of squaring in $\mathbb{F}_{p^n}$

- Input differences a active in a single S-box have $\mathrm{DP}(a, 0) = p^{-n}$
  - in most constructions the adversary can apply such differences
  - presence of a collision is easy to detect and can be used as a distinguisher
  - unacceptable weakness
- Output masks b restricted to a single S-box have $\mathrm{LP}(0, b) = p^{-n}$
  - measurable bias in the output
  - phases of bias allow determining *whitening key*, etc.
  - unacceptable weakness
- problem is *local collision/bias*

Building a non-linear layer from squaring without local collision/bias

Building a non-linear layer from squaring without local collision/bias

Specification:

$$\gamma : \forall 0 \leq i < m : y_i \leftarrow x_i + x_{i+1 \bmod m}^2$$

Building a non-linear layer from squaring without local collision/bias

Specification:

$$\gamma : \forall 0 \leq i < m : y_i \leftarrow x_i + x_{i+1 \bmod m}^2$$

Still not invertible but no local collisions or bias

Building a non-linear layer from squaring without local collision/bias

Specification:

$$\gamma : \forall 0 \leq i < m : y_i \leftarrow x_i + x_{i+1 \bmod m}^2$$

Still not invertible but no local collisions or bias

- $\mathrm{DP}(a, 0) > 0$ implies that all coordinates of a are non-zero

Building a non-linear layer from squaring without local collision/bias

Specification:

$$\gamma : \forall 0 \leq i < m : y_i \leftarrow x_i + x_{i+1 \bmod m}^2$$

Still not invertible but no local collisions or bias

- $\mathrm{DP}(a, 0) > 0$ implies that all coordinates of a are non-zero
  - $\mathrm{DP}(a, 0) = p^{-nm}$

Building a non-linear layer from squaring without local collision/bias

Specification:

$$\gamma : \forall 0 \leq i < m : y_i \leftarrow x_i + x_{i+1 \bmod m}^2$$

Still not invertible but no local collisions or bias

- $\mathrm{DP}(a, 0) > 0$ implies that all coordinates of a are non-zero
  - $\mathrm{DP}(a, 0) = p^{-nm}$
  - In case of duplex it is infeasible to apply such a difference

Building a non-linear layer from squaring without local collision/bias

Specification:

$$\gamma : \forall 0 \leq i < m : y_i \leftarrow x_i + x_{i+1 \bmod m}^2$$

Still not invertible but no local collisions or bias

- $\mathrm{DP}(a, 0) > 0$ implies that all coordinates of a are non-zero
  - $\mathrm{DP}(a, 0) = p^{-nm}$
  - In case of duplex it is infeasible to apply such a difference
- $\mathrm{LP}(0, b) > 0$ implies that all coordinates of b are non-zero

Building a non-linear layer from squaring without local collision/bias

Specification:

$$\gamma : \forall 0 \leq i < m : y_i \leftarrow x_i + x_{i+1 \bmod m}^2$$

Still not invertible but no local collisions or bias

- $\mathrm{DP}(a, 0) > 0$ implies that all coordinates of a are non-zero
  - $\mathrm{DP}(a, 0) = p^{-nm}$
  - In case of duplex it is infeasible to apply such a difference
- $\mathrm{LP}(0, b) > 0$ implies that all coordinates of b are non-zero
  - $\mathrm{LP}(a, 0) = p^{-nm}$

Building a non-linear layer from squaring without local collision/bias

Specification:

$$\gamma : \forall 0 \leq i < m : y_i \leftarrow x_i + x_{i+1 \bmod m}^2$$

Still not invertible but no local collisions or bias

- $\mathrm{DP}(a, 0) > 0$ implies that all coordinates of a are non-zero
  - $\mathrm{DP}(a, 0) = p^{-nm}$
  - In case of duplex it is infeasible to apply such a difference
- $\mathrm{LP}(0, b) > 0$ implies that all coordinates of b are non-zero
  - $\mathrm{LP}(a, 0) = p^{-nm}$
  - In case of duplex these biases cannot be observed

Building a non-linear layer from squaring without local collision/bias

Specification:

$$\gamma : \forall 0 \leq i < m : y_i \leftarrow x_i + x_{i+1 \bmod m}^2$$

Still not invertible but no local collisions or bias

- $\mathrm{DP}(a, 0) > 0$ implies that all coordinates of a are non-zero
  - $\mathrm{DP}(a, 0) = p^{-nm}$
  - In case of duplex it is infeasible to apply such a difference
- $\mathrm{LP}(0, b) > 0$ implies that all coordinates of b are non-zero
  - $\mathrm{LP}(a, 0) = p^{-nm}$
  - In case of duplex these biases cannot be observed

But isn't the invertibility a global problem?

Collision probability

Collision probability

Collision probability of a function f over G

Probability when we randomly take two inputs, that the corresponding outputs collide, minus the probability that we choose two equal inputs:

$$\mathrm{CP}(f) = \frac{\#\{(x,y) \in G \times G \mid f(x) = f(y)\}}{|G|^2} - \frac{1}{|G|}$$

Collision probability

Collision probability of a function f over G

Probability when we randomly take two inputs, that the corresponding outputs collide, minus the probability that we choose two equal inputs:

$$\mathrm{CP}(f) = \frac{\#\{(x,y) \in G \times G \mid f(x) = f(y)\}}{|G|^2} - \frac{1}{|G|}$$

- Any permutation has collision probability 0

Collision probability

Collision probability of a function f over G

Probability when we randomly take two inputs, that the corresponding outputs collide, minus the probability that we choose two equal inputs:

$$\mathrm{CP}(f) = \frac{\#\{(x,y) \in G \times G \mid f(x) = f(y)\}}{|G|^2} - \frac{1}{|G|}$$

- Any permutation has collision probability 0
- A random transformation with domain G has expected collision probability $1/|G|$

Collision probability

Collision probability of a function f over G

Probability when we randomly take two inputs, that the corresponding outputs collide, minus the probability that we choose two equal inputs:

$$\mathrm{CP}(f) = \frac{\#\{(x,y) \in G \times G \mid f(x) = f(y)\}}{|G|^2} - \frac{1}{|G|}$$

- Any permutation has collision probability 0
- A random transformation with domain G has expected collision probability $1/|G|$
- We have also

$$\mathrm{CP}(f) = \frac{\sum_{a \in G^*} \mathrm{DP}(a,0)}{|G|}$$

Collision probability of γ

Collision probability of γ

There are $(p^n - 1)^m$ input differences a with $\mathrm{DP}(a, 0) = p^{-nm}$, so

$$\mathrm{CP}(\gamma) = \frac{(p^n - 1)^m}{p^{2nm}}$$

Collision probability of γ

There are $(p^n - 1)^m$ input differences a with $\mathrm{DP}(a, 0) = p^{-nm}$, so

$$\mathrm{CP}(\gamma) = \frac{(p^n - 1)^m}{p^{2nm}}$$

- For large p^n this is approximated by p^{-nm}, same as a random transformation

Collision probability of γ

There are $(p^n - 1)^m$ input differences a with $\text{DP}(a, 0) = p^{-nm}$, so

$$\text{CP}(\gamma) = \frac{(p^n - 1)^m}{p^{2nm}}$$

- For large p^n this is approximated by p^{-nm}, same as a random transformation
- For $p^n = 3$ this becomes $\frac{2^m}{3^{2m}}$, a factor $(2/3)^m$ less than a random transformation

Collision probability of γ

There are $(p^n - 1)^m$ input differences a with $\mathrm{DP}(a, 0) = p^{-nm}$, so

$$\mathrm{CP}(\gamma) = \frac{(p^n - 1)^m}{p^{2nm}}$$

- For large p^n this is approximated by p^{-nm}, same as a random transformation
- For $p^n = 3$ this becomes $\frac{2^m}{3^{2m}}$, a factor $(2/3)^m$ less than a random transformation
- Doing r rounds roughly multiplies this collision probability with a factor r

Collision probability of γ

There are $(p^n - 1)^m$ input differences a with $\mathrm{DP}(a, 0) = p^{-nm}$, so

$$\mathrm{CP}(\gamma) = \frac{(p^n - 1)^m}{p^{2nm}}$$

- For large p^n this is approximated by p^{-nm}, same as a random transformation
- For $p^n = 3$ this becomes $\frac{2^m}{3^{2m}}$, a factor $(2/3)^m$ less than a random transformation
- Doing r rounds roughly multiplies this collision probability with a factor r
- A priori not problematic if the domain is large enough

Differential propagation behavior of γ

Differential propagation behavior of γ

- Output differences b compatible with given input difference a form an affine space

Differential propagation behavior of γ

- Output differences b compatible with given input difference a form an affine space
  - dimension is # active elements in input difference a: $\mathrm{DP}(a, b) = p^{-n\,\mathrm{HW}(a)}$

Differential propagation behavior of γ

- Output differences b compatible with given input difference a form an affine space
  - dimension is # active elements in input difference a: $\mathrm{DP}(a, b) = p^{-n\,\mathrm{HW}(a)}$
  - easy to specify basis and offsets

Differential propagation behavior of γ

- Output differences b compatible with given input difference a form an affine space
  - dimension is # active elements in input difference a: $\mathrm{DP}(a, b) = p^{-n\,\mathrm{HW}(a)}$
  - easy to specify basis and offsets
- Given an output difference b, compatible input differences a form no affine space

Differential propagation behavior of γ

- Output differences b compatible with given input difference a form an affine space
  - dimension is # active elements in input difference a: $\mathrm{DP}(a, b) = p^{-n\,\mathrm{HW}(a)}$
  - easy to specify basis and offsets
- Given an output difference b, compatible input differences a form no affine space
- Still it is possible to characterize in a simple way the set

Differential propagation behavior of γ

- Output differences b compatible with given input difference a form an affine space
  - dimension is # active elements in input difference a: $\mathrm{DP}(a, b) = p^{-n\,\mathrm{HW}(a)}$
  - easy to specify basis and offsets
- Given an output difference b, compatible input differences a form no affine space
- Still it is possible to characterize in a simple way the set
- We have efficient algorithms for, given b

Differential propagation behavior of γ

- Output differences b compatible with given input difference a form an affine space
  - dimension is # active elements in input difference a: $\mathrm{DP}(a, b) = p^{-n\,\mathrm{HW}(a)}$
  - easy to specify basis and offsets
- Given an output difference b, compatible input differences a form no affine space
- Still it is possible to characterize in a simple way the set
- We have efficient algorithms for, given b
  - Generate all input differences a for which $\mathrm{DP}(a, b)$ is above a given threshold

Differential propagation behavior of γ

- Output differences b compatible with given input difference a form an affine space
  - dimension is # active elements in input difference a: $\mathrm{DP}(a, b) = p^{-n\,\mathrm{HW}(a)}$
  - easy to specify basis and offsets
- Given an output difference b, compatible input differences a form no affine space
- Still it is possible to characterize in a simple way the set
- We have efficient algorithms for, given b
  - Generate all input differences a for which $\mathrm{DP}(a, b)$ is above a given threshold
  - And find $\max_a \mathrm{DP}(a, b)$

Correlation

Correlation

- Input masks a compatible with a given output mask b form an affine space

Correlation

- Input masks a compatible with a given output mask b form an affine space
  - dimension is $\#$ active elements in output mask b: $\mathrm{LP}(a, b) = p^{-n\,\mathrm{HW}(b)}$

Correlation

- Input masks a compatible with a given output mask b form an affine space
  - dimension is $\#$ active elements in output mask b: $\mathrm{LP}(a, b) = p^{-n\,\mathrm{HW}(b)}$
  - easy to specify basis and offsets

Correlation

- Input masks a compatible with a given output mask b form an affine space
  - dimension is # active elements in output mask b: $\mathrm{LP}(a, b) = p^{-n\,\mathrm{HW}(b)}$
  - easy to specify basis and offsets
- Exactly the same algorithms as for differentials but:

Correlation

- Input masks a compatible with a given output mask b form an affine space
  - dimension is $\#$ active elements in output mask b: $\mathrm{LP}(a, b) = p^{-n\,\mathrm{HW}(b)}$
  - easy to specify basis and offsets
- Exactly the same algorithms as for differentials but:
  - with input and output swapped

Correlation

- Input masks a compatible with a given output mask b form an affine space
  - dimension is # active elements in output mask b: $\mathrm{LP}(a, b) = p^{-n\,\mathrm{HW}(b)}$
  - easy to specify basis and offsets
- Exactly the same algorithms as for differentials but:
  - with input and output swapped
  - with left (i) and right $(-i)$ swapped

Thanks for your attention!