Statistical properties of Butterfly-like constructions

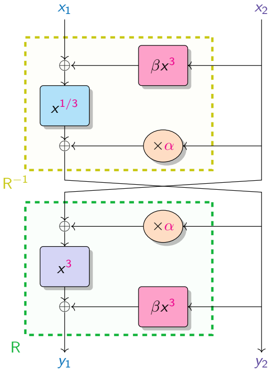
Clémence Bouvier

Université de Lorraine, CNRS, Inria, LORIA

Fq16, São Carlos, Brazil
July 11th, 2025

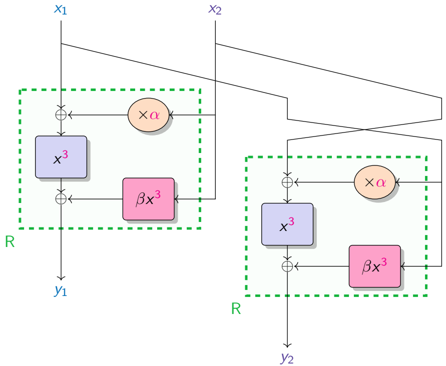
Original Butterfly

Introduced by [Perrin, Udovenko and Biryukov, CRYPTO 2016] over binary fields, $\mathbb{F}_{2^n}^2$, n odd.



Open variant.

$$\begin{cases} y_1 &= R(x_2, R^{-1}(x_1, x_2)) &= (x_2 + \alpha y_2)^3 + \beta {y_2}^3 \\ y_2 &= R^{-1}(x_1, x_2) &= (x_1 - \beta {x_2}^3)^{1/3} - \alpha x_2 \,. \end{cases}$$

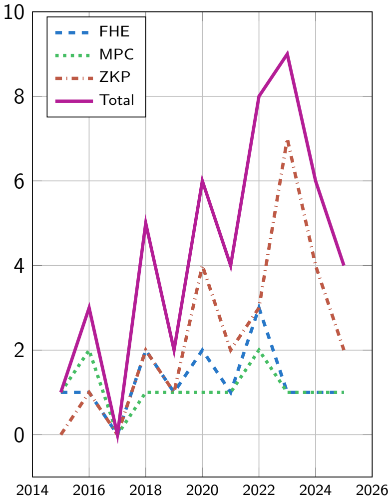


Closed variant.

$$\begin{cases} y_1 &= R(x_1, x_2) &= (x_1 + \alpha x_2)^3 + \beta {x_2}^3 \\ y_2 &= R(x_2, x_1) &= (x_2 + \alpha x_1)^3 + \beta {x_1}^3 \,. \end{cases}$$

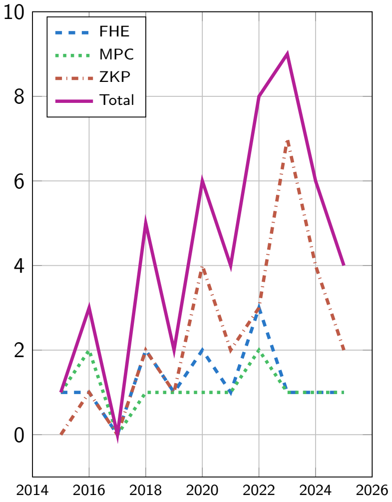
A new context

New symmetric primitives



A new context

New symmetric primitives



Traditional case

- ⋆ Operations: logical gates or CPU instructions
- ⋆ Field size:

$$\mathbb{F}_2^n, \text{ with } n \simeq 4, 8$$

- ⋆ Cryptanalysis: decades

Arithmetization-Oriented

- ⋆ Operations: large finite-field arithmetic
- ⋆ Field size:

$$\mathbb{F}_q, \text{ with } q \in \{2^n, p\}, p \simeq 2^n, n \geq 32$$

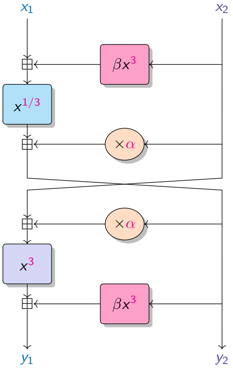
- ⋆ Cryptanalysis: ≤ 8 years

Butterflies in the context of ZKP?

- ⋆ Flystel a degenerated case of Butterfly
- ⋆ Differential properties: solving an open problem
- ⋆ Linear properties: link with cohomology

From Butterfly to Flystel

Introduced by [Bouvier, Briaud, Chaidos, Perrin, Salen, Velichkov and Willems, CRYPTO 2023]

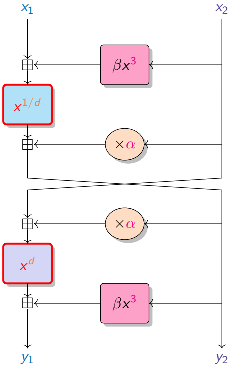


Open variant.

$$\begin{cases} y_1 &= (x_2 + \alpha y_2)^3 + \beta {y_2}^3 \\ y_2 &= (x_1 + \beta {x_2}^3)^{1/3} + \alpha x_2 \,. \end{cases}$$

From Butterfly to Flystel

Introduced by [Bouvier, Briaud, Chaidos, Perrin, Salen, Velichkov and Willems, CRYPTO 2023]

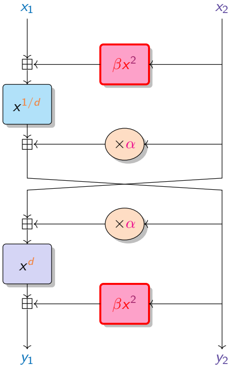


Open variant.

$$\begin{cases} y_1 &= (x_2 + \alpha y_2)^d + \beta {y_2}^3 \\ y_2 &= (x_1 + \beta {x_2}^3)^{1/d} + \alpha x_2\,. \end{cases}$$

From Butterfly to Flystel

Introduced by [Bouvier, Briaud, Chaidos, Perrin, Salen, Velichkov and Willems, CRYPTO 2023]

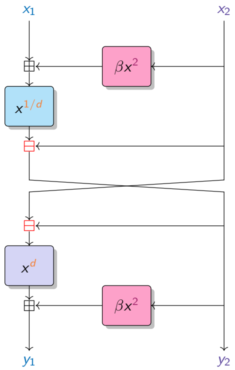


Open variant.

$$\begin{cases} y_1 &= (x_2 + \alpha y_2)^d + \beta {y_2}^2 \\ y_2 &= (x_1 + \beta {x_2}^2)^{1/d} + \alpha x_2 \,. \end{cases}$$

From Butterfly to Flystel

Introduced by [Bouvier, Briaud, Chaidos, Perrin, Salen, Velichkov and Willems, CRYPTO 2023]

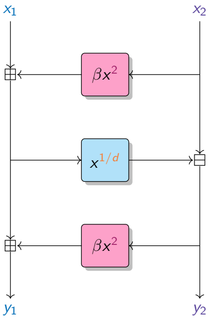


Open variant.

$$\begin{cases} y_1 &= (x_2 - y_2)^d + \beta {y_2}^2 \\ y_2 &= (x_1 + \beta {x_2}^2)^{1/d} - x_2 \,. \end{cases}$$

From Butterfly to Flystel

Introduced by [Bouvier, Briaud, Chaidos, Perrin, Salen, Velichkov and Willems, CRYPTO 2023]

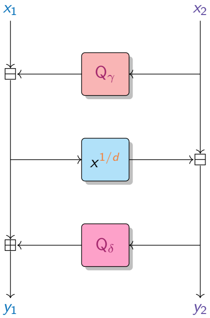


Open variant.

$$\begin{cases} y_1 &= (x_2 - y_2)^d + \beta {y_2}^2 \\ y_2 &= (x_1 + \beta {x_2}^2)^{1/d} - x_2 \,. \end{cases}$$

From Butterfly to Flystel

Introduced by [Bouvier, Briaud, Chaidos, Perrin, Salen, Velichkov and Willems, CRYPTO 2023]

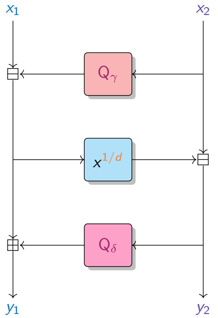


Open variant.

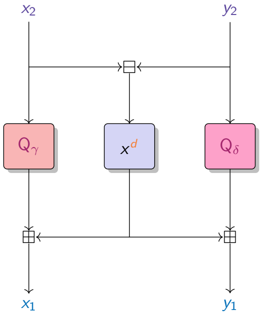
$$\begin{cases} y_1 &= (x_2 - y_2)^d + Q_\delta(y_2) \\ y_2 &= (x_1 - Q_\gamma(x_2))^{1/d} - x_2 \,. \end{cases}$$

From Butterfly to Flystel

Introduced by [Bouvier, Briaud, Chaidos, Perrin, Salen, Velichkov and Willems, CRYPTO 2023]



Open variant.



Closed variant.

$$\begin{cases} y_1 &= (x_2 - y_2)^d + Q_\delta(y_2) \\ y_2 &= (x_1 - Q_\gamma(x_2))^{1/d} - x_2 \,. \end{cases}$$

$$\begin{cases} x_1 &= (x_2 - y_2)^d + Q_\gamma(x_2) \\ y_1 &= (x_2 - y_2)^d + Q_\delta(y_2) \,. \end{cases}$$

Statistical properties

- ⋆ Differential properties

- ⋆ Linear properties

Statistical properties

⋆ Differential properties

Definition

Let $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be a function. The **Differential uniformity** δ_F is given by

$$\delta_F = \max_{a \neq 0, b} |\{x \in \mathbb{F}_q^n, F(x+a) - F(x) = b\}|$$

⋆ Linear properties

Statistical properties

⋆ Differential properties

Definition

Let $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be a function. The **Differential uniformity** δ_F is given by

$$\delta_F = \max_{a \neq 0, b} \left| \{ x \in \mathbb{F}_q^n, F(x+a) - F(x) = b \} \right|$$

⋆ Linear properties

Definition

Let $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be a function and ω a primitive element.
The **Linearity** $\mathcal{L}_F$ is the highest Walsh coefficient.

$$\mathcal{L}_F = \max_{u, v \neq 0} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{(\langle v, F(x) \rangle \oplus \langle u, x \rangle)} \right|$$

Statistical properties

⋆ Differential properties

Definition

Let $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be a function. The **Differential uniformity** δ_F is given by

$$\delta_F = \max_{a \neq 0, b} \left| \{ x \in \mathbb{F}_q^n, F(x+a) - F(x) = b \} \right|$$

⋆ Linear properties

Definition

Let $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be a function and ω a primitive element.
The **Linearity** $\mathcal{L}_F$ is the highest Walsh coefficient.

$$\mathcal{L}_F = \max_{u, v \neq 0} \left| \sum_{x \in \mathbb{F}_p^n} e^{\left(\frac{2i\pi}{p}\right)(\langle v, F(x) \rangle - \langle u, x \rangle)} \right|$$

Differential Properties

Proposition [Bouvier et al., 2023]

The **Flystel**

$$\mathsf{F} : \mathbb{F}_p^2 \to \mathbb{F}_p^2,\ (x_1, x_2) \mapsto \left((x_1 - x_2)^d + \mathsf{Q}_\gamma(x_1)\ ,\ (x_1 - x_2)^d + \mathsf{Q}_\delta(x_2)\right)$$

has differential uniformity

$$\delta_{\mathsf{F}} = \max_{a \neq 0, b} \left|\{x \in \mathbb{F}_p^2, \mathsf{F}(x + a) - \mathsf{F}(x) = b\}\right| \leq d - 1\ .$$

Differential Properties

Proposition [Bouvier et al., 2023]

The **Flystel**

$$\mathsf{F} : \mathbb{F}_p^2 \to \mathbb{F}_p^2,\ (x_1, x_2) \mapsto ((x_1 - x_2)^d + \mathsf{Q}_\gamma(x_1)\ ,\ (x_1 - x_2)^d + \mathsf{Q}_\delta(x_2))$$

has differential uniformity

$$\delta_\mathsf{F} \ = \ \max_{a \neq 0, b} |\{x \in \mathbb{F}_p^2, \mathsf{F}(x+a) - \mathsf{F}(x) = b\}| \ \leq \ d - 1\ .$$

Solving an open problem since 2014 on APN permutations over $\mathbb{F}_p^2$

Existence of APN permutations

F is Almost Perfect Nonlinear iff

$$\delta_\mathsf{F} \ = \ \max_{a \neq 0, b} |\{x \in \mathbb{F}_p^m, \mathsf{F}(x+a) - \mathsf{F}(x) = b\}| \ = \ 2\ .$$

Flystel in $\mathbb{F}_p$ with x^3: APN permutation

Weil bound

Proposition [Weil, 1948]

Let $f \in \mathbb{F}_p[x]$ be a univariate polynomial with $\deg(f) = d$. Then

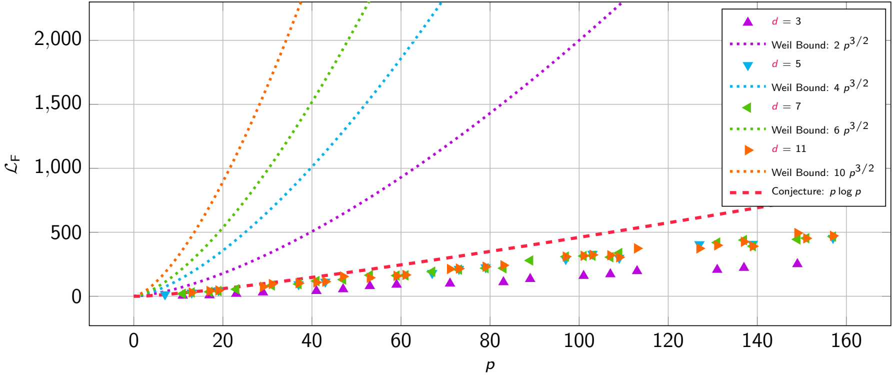
$$\mathcal{L}_f \leq (d-1)\sqrt{p}$$

Weil bound

Proposition [Weil, 1948]

Let f $\in \mathbb{F}_p[x]$ be a univariate polynomial with $\deg(f) = d$. Then

$$\mathcal{L}_f \leq (d-1)\sqrt{p}$$



Exponential sums

- ⋆ Direct applications of results for exponential sums [Beyne and Bouvier, 2024]

Exponential sums

⋆ Direct applications of results for exponential sums [Beyne and Bouvier, 2024]

⋆ 3 different results (generalization of Weil bound)... for 3 important constructions

- ⋆ Deligne, 1974 — Generalization of the Butterfly construction
- ⋆ Denef and Loeser, 1991 — 3-round Feistel network
- ⋆ Rojas-León, 2006 — Generalization of the Flystel construction

Functions with 2 variables

$$\boxed{F \in \mathbb{F}_q[x_1, x_2],\ \exists C \in \mathbb{F}_q,\ \mathcal{L}_F \leq C \times q}$$

Exponential sums

- ⋆ Direct applications of results for exponential sums [Beyne and Bouvier, 2024]

- ⋆ 3 different results (generalization of Weil bound)... for 3 important constructions
  - ⋆ Deligne, 1974 — Generalization of the Butterfly construction
  - ⋆ Denef and Loeser, 1991 — 3-round Feistel network
  - ⋆ Rojas-León, 2006 — Generalization of the Flystel construction

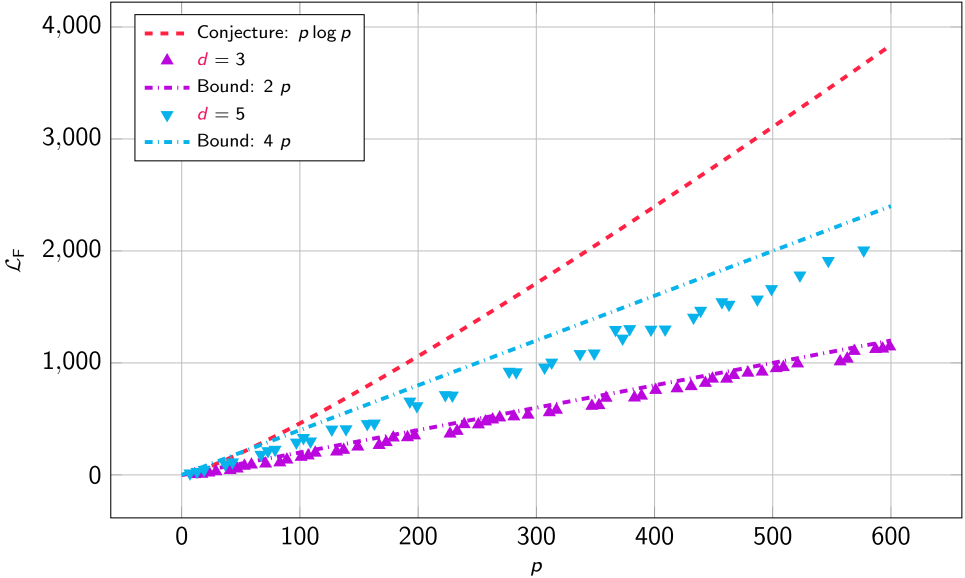
  Functions with 2 variables

$$\boxed{\mathsf{F} \in \mathbb{F}_q[x_1, x_2],\ \exists C \in \mathbb{F}_q,\ \mathcal{L}_\mathsf{F} \leq C \times q}$$

- ⋆ Solving conjecture on the linearity of the Flystel construction (for $d \leq \log p$)

$$\mathcal{L}_\mathsf{F} \leq (d-1)p\ .$$

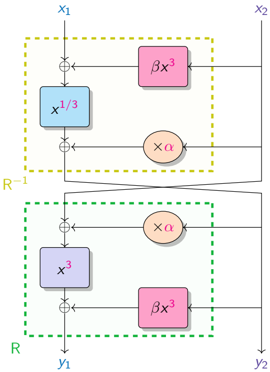
Solving conjecture



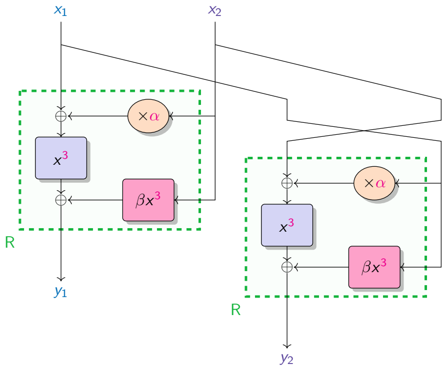
Can we go further?

- Is the Flystel an optimal construction?
  - Statistical properties (differential and linear)
  - ZK-performance
- How to classify Butterfly-like constructions?

Back to TU decomposition



Open variant.

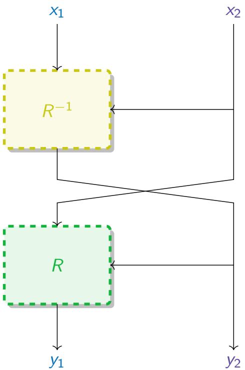


Closed variant.

$$\begin{cases} y_1 &= (x_2 + \alpha y_2)^3 + \beta {y_2}^3 \\ y_2 &= (x_1 - \beta {x_2}^3)^{1/3} - \alpha x_2 \,. \end{cases}$$

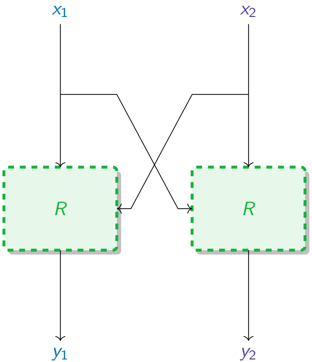
$$\begin{cases} y_1 &= (x_1 + \alpha x_2)^3 + \beta {x_2}^3 \\ y_2 &= (x_2 + \alpha x_1)^3 + \beta {x_1}^3 \,. \end{cases}$$

Back to TU decomposition



Open variant.

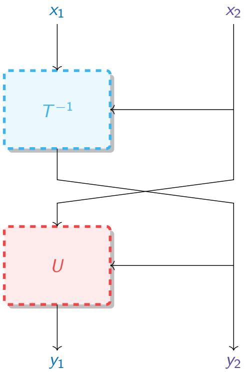
$$\begin{cases} y_1 &= R(x_2, R^{-1}(x_1, x_2)) \\ y_2 &= R^{-1}(x_1, x_2)\,. \end{cases}$$



Closed variant.

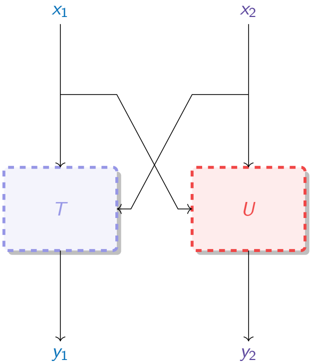
$$\begin{cases} y_1 &= R(x_1, x_2) \\ y_2 &= R(x_2, x_1)\,. \end{cases}$$

Back to TU decomposition



Open variant.

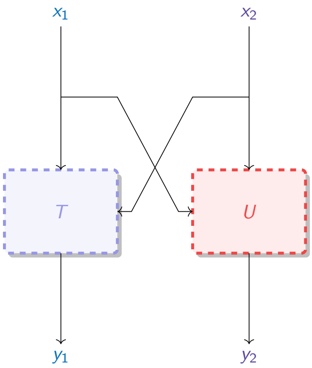
$$\begin{cases} y_1 &= U(x_2, T^{-1}(x_1, x_2)) \\ y_2 &= T^{-1}(x_1, x_2)\,. \end{cases}$$



Closed variant.

$$\begin{cases} y_1 &= T(x_1, x_2) \\ y_2 &= U(x_2, x_1)\,. \end{cases}$$

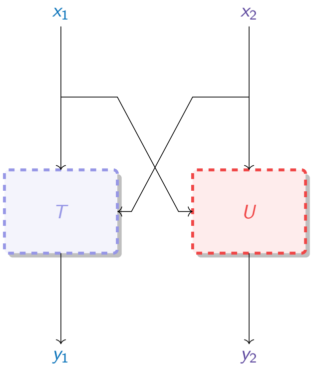
Specific cases



Closed variant.

$$\begin{cases} y_1 &= T(x_1, x_2) \\ y_2 &= U(x_2, x_1)\,. \end{cases}$$

Specific cases



Closed variant.

$$\begin{cases} y_1 &= T(x_1, x_2) \\ y_2 &= U(x_2, x_1) \,. \end{cases}$$

⋆ Asymmetric TU with

s.t.
$$F : \mathbb{F}_p^2 \to \mathbb{F}_p^2, (x_1, x_2) \mapsto (y_1, y_2)$$
$$\begin{cases} y_1 &= G_1(x_1, x_2) + H_1(x_1, x_2) \\ y_2 &= H_2(x_1, x_2) \ , \end{cases}$$

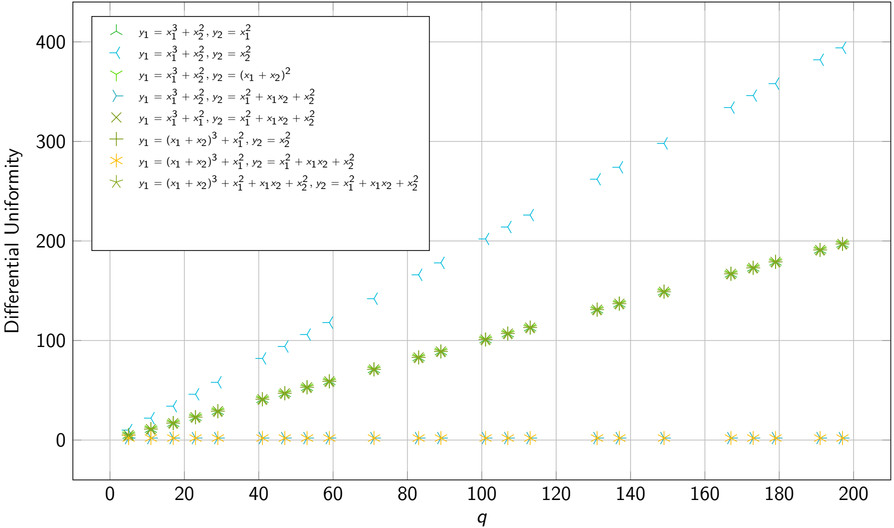
⋆ Symmetric TU with

s.t.
$$F : \mathbb{F}_p^2 \to \mathbb{F}_p^2, (x_1, x_2) \mapsto (y_1, y_2)$$
$$\begin{cases} y_1 &= G_1(x_1, x_2) + H_1(x_1, x_2) \\ y_2 &= G_2(x_1, x_2) + H_2(x_1, x_2) \ , \end{cases}$$

where

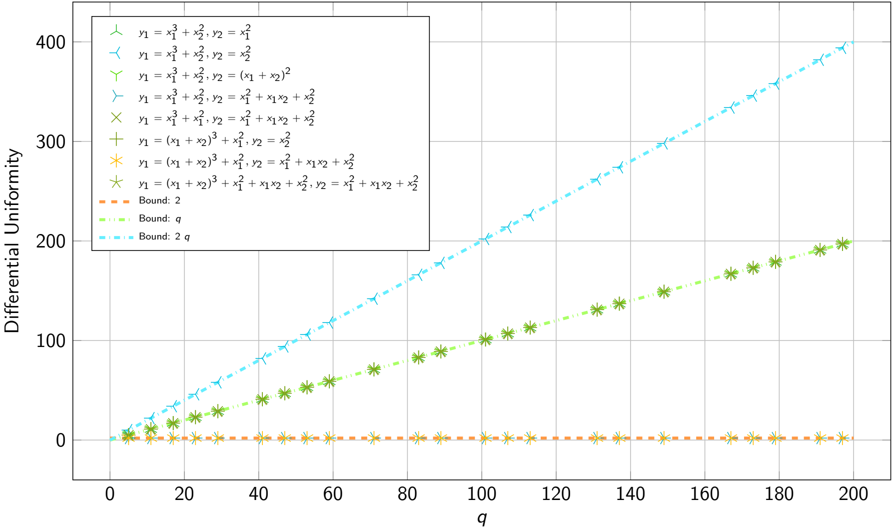
- ⋆ G_i: functions with only cubic terms
- ⋆ H_i: functions with only quadratic terms

Differential properties



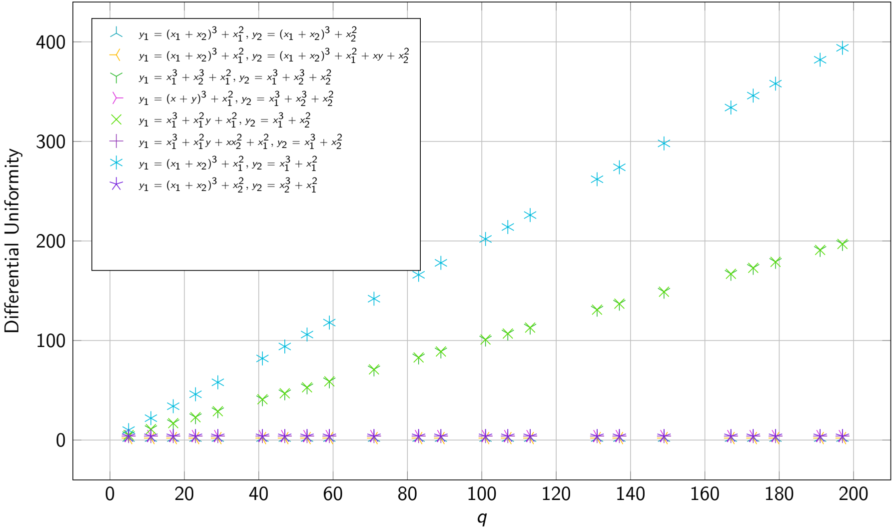
Asymmetric TU

Differential properties



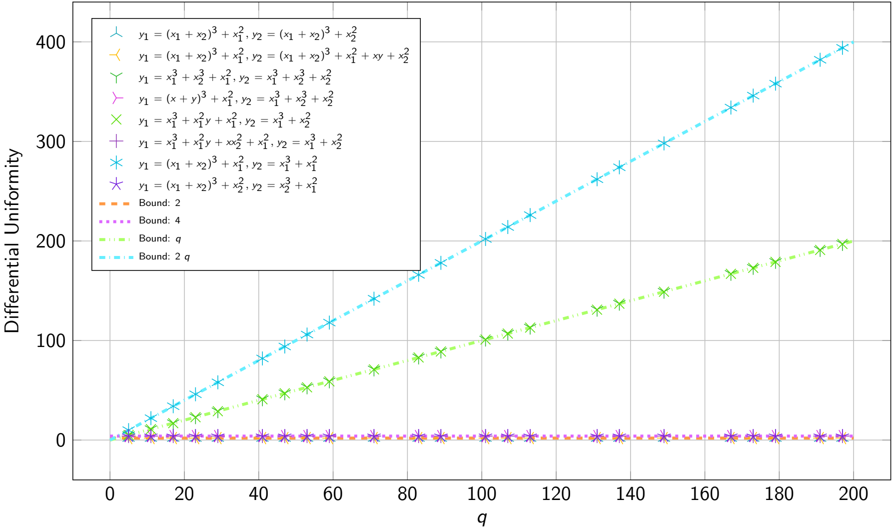
Asymmetric TU

Differential properties



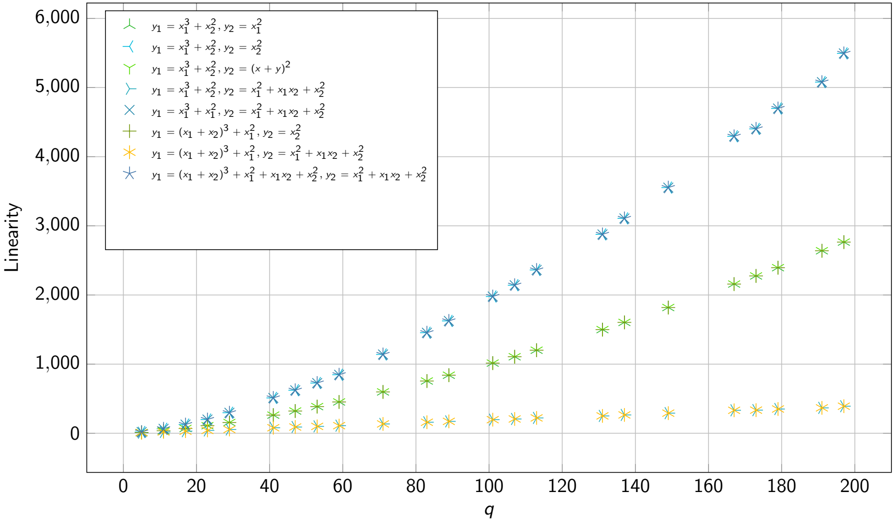
Symmetric TU

Differential properties



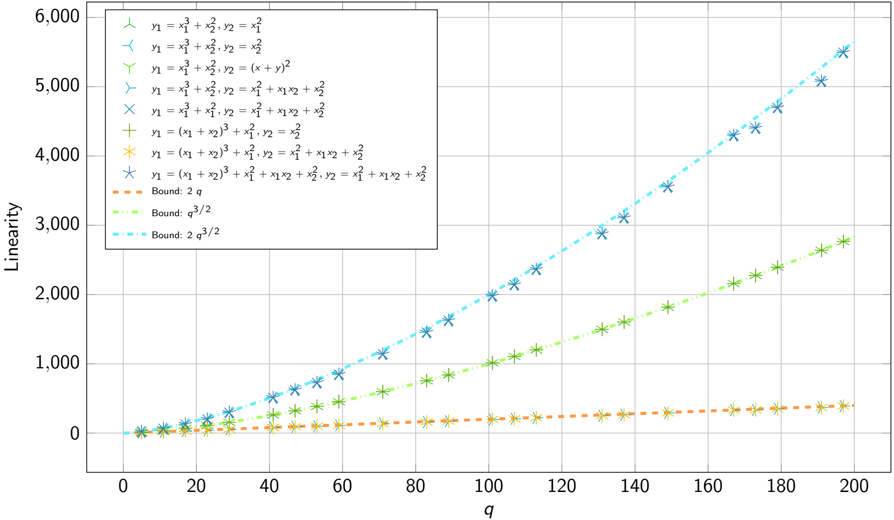
Symmetric TU

Linear properties



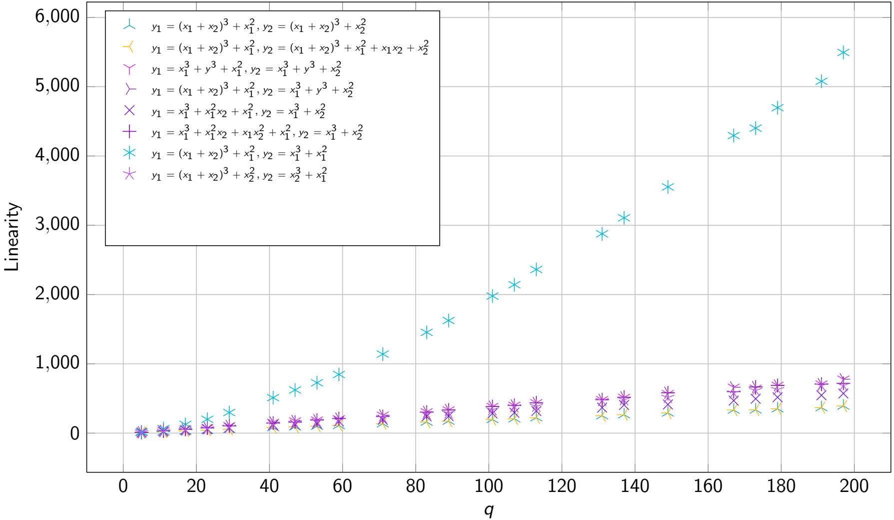
Asymmetric TU

Linear properties



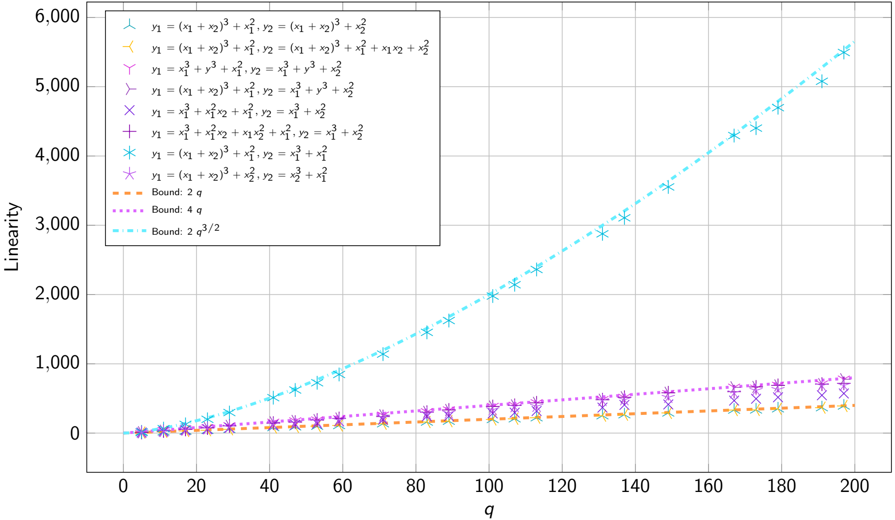
Asymmetric TU

Linear properties



Symmetric TU

Linear properties



Symmetric TU

Performance metric

What does "efficient" mean for Zero-Knowledge Proofs?

Performance metric

What does "efficient" mean for Zero-Knowledge Proofs?

"It depends"

Performance metric

What does "efficient" mean for Zero-Knowledge Proofs?

"It depends"

Example

R1CS (Rank-1 Constraint System): minimizing the number of multiplications

$$y = (ax + b)^3(cx + d) + ex$$

$t_0 = a \cdot x$	$t_3 = t_2 \times t_1$	$t_6 = t_3 \times t_5$
$t_1 = t_0 + b$	$t_4 = c \cdot x$	$t_7 = e \cdot x$
$t_2 = t_1 \times t_1$	$t_5 = t_4 + d$	$t_8 = t_6 + t_7$

Performance metric

What does "efficient" mean for Zero-Knowledge Proofs?

"It depends"

Example

R1CS (Rank-1 Constraint System): minimizing the number of multiplications

$$y = (ax + b)^3(cx + d) + ex$$

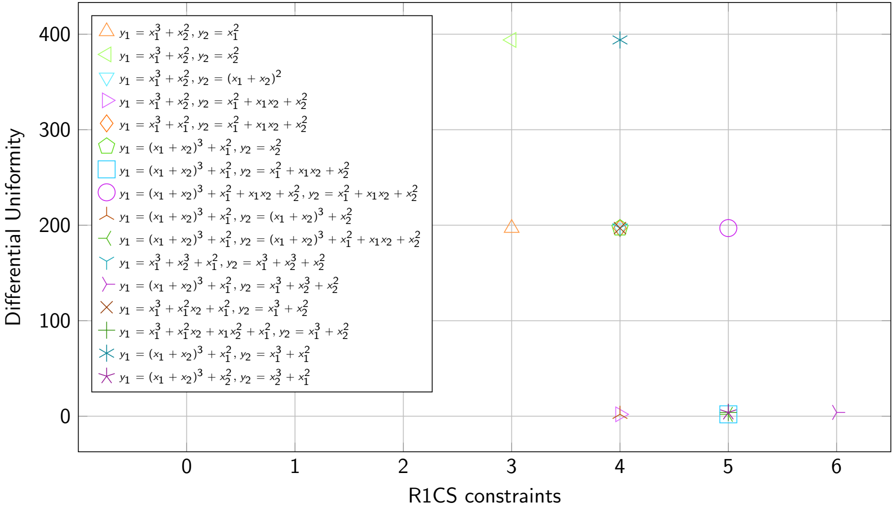
$t_0 = a \cdot x$ $\quad$ $t_3 = t_2 \times t_1$ $\quad$ $t_6 = t_3 \times t_5$

$t_1 = t_0 + b$ $\quad$ $t_4 = c \cdot x$ $\quad$ $t_7 = e \cdot x$

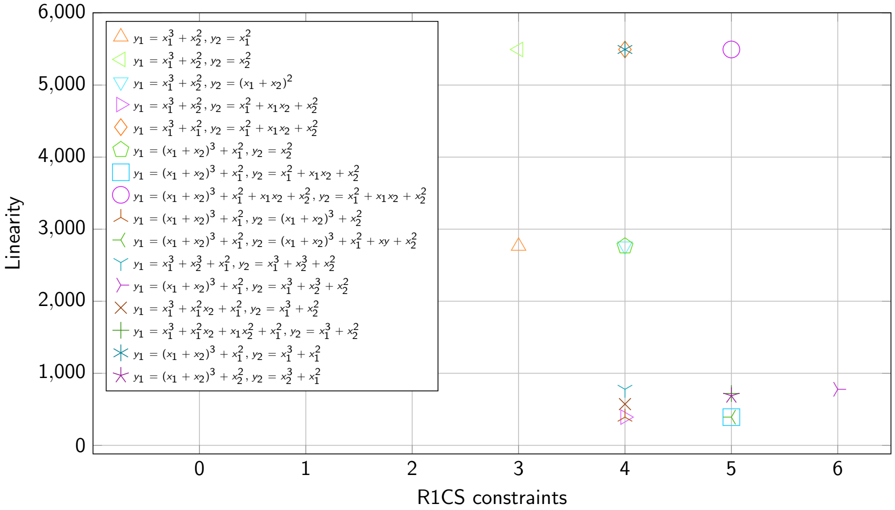
$t_2 = t_1 \times t_1$ $\quad$ $t_5 = t_4 + d$ $\quad$ $t_8 = t_6 + t_7$

3 constraints

ZK performance



ZK performance



Conclusions and Perspectives

- Butterfly-like constructions in $\mathbb{F}_p$:
  - Nice results for the differential uniformity and the linearity
  - Interesting structures for ZKP

Conclusions and Perspectives

- Butterfly-like constructions in $\mathbb{F}_p$:
  - Nice results for the differential uniformity and the linearity
  - Interesting structures for ZKP
- Future works:
  - Can we systematise such a classification?
  - And extend it to other properties?

Conclusions and Perspectives

- ⋆ Butterfly-like constructions in $\mathbb{F}_p$:
  - ⋆ Nice results for the differential uniformity and the linearity
  - ⋆ Interesting structures for ZKP
- ⋆ Future works:
  - ⋆ Can we systematise such a classification?
  - ⋆ And extend it to other properties?

Thank you