Generalized Triangular Dynamical System: An Algebraic System for Constructing Cryptographic Permutations over Finite Fields

Arnab Roy[1]
Matthias Johann Steiner[2]

[1]Universität Innsbruck, Austria
[2]Alpen-Adria-Universität Klagenfurt, Austria

M. Steiner has been supported by the European Research Council (ERC) (grant agreement No. 725042) and the enCRYPTON project (grant agreement No. 101079319).

Outline

universität innsbruck UNIVERSITÄT KLAGENFURT

How Do We Construct Block Ciphers?

- Fix a vector space over a finite field $\mathbb{F}_q^n$.
  - Classical designs: $\mathbb{F}_{2^m}^n$.
  - Modern designs for MPC or ZK: $\mathbb{F}_p^n$, where p prime.

How Do We Construct Block Ciphers?

- Fix a vector space over a finite field $\mathbb{F}_q^n$.
  - Classical designs: $\mathbb{F}_{2^m}^n$.
  - Modern designs for MPC or ZK: $\mathbb{F}_p^n$, where p prime.
- Choose a round function

$$\mathcal{R}_i(\boldsymbol{x}, \boldsymbol{k}_i) = \underbrace{\boldsymbol{M}}_{\text{matrix}} \underbrace{\mathcal{P}(\boldsymbol{x})}_{\text{non-linear perm.}} + \underbrace{\boldsymbol{k}_i}_{\text{round key}} + \underbrace{\boldsymbol{c}_i}_{\text{constant}} .$$

universität innsbruck
UNIVERSITÄT KLAGENFURT

How Do We Construct Block Ciphers?

- Fix a vector space over a finite field $\mathbb{F}_q^n$.
  - Classical designs: $\mathbb{F}_{2^m}^n$.
  - Modern designs for MPC or ZK: $\mathbb{F}_p^n$, where p prime.
- Choose a round function

$$\mathcal{R}_i(\boldsymbol{x}, \boldsymbol{k}_i) = \underbrace{\boldsymbol{M}}_{\text{matrix}} \quad \underbrace{\mathcal{P}(\boldsymbol{x})}_{\text{non-linear perm.}} \quad + \underbrace{\boldsymbol{k}_i}_{\text{round key}} + \underbrace{\boldsymbol{c}_i}_{\text{constant}} .$$

- Choose a key schedule.
  - E.g., linear $\boldsymbol{k}_i = \boldsymbol{M}_{\text{ks}}^i \boldsymbol{k}$.

universität innsbruck
UNIVERSITÄT KLAGENFURT

How Do We Construct Block Ciphers?

- Fix a vector space over a finite field $\mathbb{F}_q^n$.
  - Classical designs: $\mathbb{F}_{2^m}^n$.
  - Modern designs for MPC or ZK: $\mathbb{F}_p^n$, where p prime.
- Choose a round function

$$\mathcal{R}_i(\boldsymbol{x}, \boldsymbol{k}_i) = \underbrace{\boldsymbol{M}}_{\text{matrix}} \quad \underbrace{\mathcal{P}(\boldsymbol{x})}_{\text{non-linear perm.}} + \underbrace{\boldsymbol{k}_i}_{\text{round key}} + \underbrace{\boldsymbol{c}_i}_{\text{constant}} .$$

- Choose a key schedule.
  - E.g., linear $\boldsymbol{k}_i = \boldsymbol{M}_{\text{ks}}^i \boldsymbol{k}$.
- Obtain a cipher by iteration of round functions

$$\mathcal{C}(\boldsymbol{x}, \boldsymbol{k}) = \mathcal{R}_r \circ \cdots \circ \mathcal{R}_1(\boldsymbol{x}, \boldsymbol{k}).$$

Classical Non-Linear Layers

- Substitution-Permutation Network (SPN): Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a permutation, then

$$\mathcal{S} : \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} f(x_1) \\ \vdots \\ f(x_n) \end{pmatrix}.$$

- Feistel Networks: Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a function, then a 2-branch Feistel Network is given by

$$\mathcal{FN} : \begin{pmatrix} x_L \\ x_R \end{pmatrix} \mapsto \begin{pmatrix} x_R + f(x_L) \\ x_L \end{pmatrix}.$$

- And variations thereof.

Triangular Dynamical System (TDS) [OS10a]

- $\mathbb{F}_q$ finite field, $n \in \mathbb{Z}_{\geq 1}$, $g_i, h_i \in \mathbb{F}_q[x_{i+1}, \dots, x_n]$ polynomials.
- Then the TDS $\mathcal{F} = \{f_1, \dots, f_n\} \subset \mathbb{F}_q[x_1, \dots, x_n]$ is defined as

- Introduced by Ostafe and Sparlinski [OS10a].
- Can exhibit polynomial degree growth under iteration [OS10a, §2.2].

Triangular Dynamical System

Triangular Dynamical System (TDS) [OS10a]

- $\mathbb{F}_q$ finite field, $n \in \mathbb{Z}_{\geq 1}$, $g_i, h_i \in \mathbb{F}_q[x_{i+1}, \ldots, x_n]$ polynomials.
- Then the TDS $\mathcal{F} = \{f_1, \ldots, f_n\} \subset \mathbb{F}_q[x_1, \ldots, x_n]$ is defined as

$$f_n(x_1, \ldots, x_n) = x_n.$$

- Introduced by Ostafe and Sparlinski [OS10a].
- Can exhibit polynomial degree growth under iteration [OS10a, §2.2].

Triangular Dynamical System (TDS) [OS10a]

- $\mathbb{F}_q$ finite field, $n \in \mathbb{Z}_{\geq 1}$, $g_i, h_i \in \mathbb{F}_q[x_{i+1}, \dots, x_n]$ polynomials.
- Then the TDS $\mathcal{F} = \{f_1, \dots, f_n\} \subset \mathbb{F}_q[x_1, \dots, x_n]$ is defined as

$$
\begin{aligned}
f_{n-1}(x_1, \dots, x_n) &= x_{n-1} \cdot g_{n-1}(x_n) + h_{n-1}(x_n), \\
f_n(x_1, \dots, x_n) &= x_n.
\end{aligned}
$$

- Introduced by Ostafe and Sparlinski [OS10a].
- Can exhibit polynomial degree growth under iteration [OS10a, §2.2].

Triangular Dynamical System (TDS) [OS10a]

- $\mathbb{F}_q$ finite field, $n \in \mathbb{Z}_{\geq 1}$, $g_i, h_i \in \mathbb{F}_q[x_{i+1}, \dots, x_n]$ polynomials.
- Then the TDS $\mathcal{F} = \{f_1, \dots, f_n\} \subset \mathbb{F}_q[x_1, \dots, x_n]$ is defined as

$$
\begin{aligned}
f_1(x_1, \dots, x_n) &= x_1 \cdot g_1(x_2, \dots, x_n) + h_1(x_2, \dots, x_n), \\
f_2(x_1, \dots, x_n) &= x_2 \cdot g_2(x_3, \dots, x_n) + h_2(x_3, \dots, x_n), \\
&\vdots \\
f_{n-1}(x_1, \dots, x_n) &= x_{n-1} \cdot g_{n-1}(x_n) + h_{n-1}(x_n), \\
f_n(x_1, \dots, x_n) &= x_n.
\end{aligned}
$$

- Introduced by Ostafe and Sparlinski [OS10a].
- Can exhibit polynomial degree growth under iteration [OS10a, §2.2].

Triangular Dynamical System

- Introduced by Ostafe and Sparlinski [OS10a].
- Can exhibit polynomial degree growth under iteration [OS10a, §2.2].

Triangular Dynamical System

- Introduced by Ostafe and Sparlinski [OS10a].
- Can exhibit polynomial degree growth under iteration [OS10a, §2.2].
- Polynomial pseudo-random number generator $\boldsymbol{x}_i = \mathcal{F}(\boldsymbol{x}_{i-1})$ was investigated [OS10a, §3].
  - Polynomial degree growth implies low discrepancy.

universität innsbruck UNIVERSITÄT KLAGENFURT

Triangular Dynamical System

- Introduced by Ostafe and Sparlinski [OS10a].
- Can exhibit polynomial degree growth under iteration [OS10a, §2.2].
- Polynomial pseudo-random number generator $\boldsymbol{x}_i = \mathcal{F}(\boldsymbol{x}_{i-1})$ was investigated [OS10a, §3].
  - Polynomial degree growth implies low discrepancy.
- A hash function based on polynomial iterations was proposed [OS10b].

Generalized Triangular Dynamical System (GTDS)

- $\mathbb{F}_q$ finite field, $n \in \mathbb{Z}_{\geq 1}$.

Generalized Triangular Dynamical System (GTDS)

- $\mathbb{F}_q$ finite field, $n \in \mathbb{Z}_{\geq 1}$.
- $p_i \in \mathbb{F}_q[x_i]$ permutation polynomials.

Generalized Triangular Dynamical System (GTDS)

- $\mathbb{F}_q$ finite field, $n \in \mathbb{Z}_{\geq 1}$.
- $p_i \in \mathbb{F}_q[x_i]$ permutation polynomials.
- $g_i, h_i \in \mathbb{F}_q[x_{i+1}, \dots, x_n]$ polynomials such that the g_i's do not have zeros.

Generalized Triangular Dynamical System (GTDS)

- $\mathbb{F}_q$ finite field, $n \in \mathbb{Z}_{\geq 1}$.
- $p_i \in \mathbb{F}_q[x_i]$ permutation polynomials.
- $g_i, h_i \in \mathbb{F}_q[x_{i+1}, \dots, x_n]$ polynomials such that the g_i's do not have zeros.
- Then the GTDS $\mathcal{F} = \{f_1, \dots, f_n\} \subset \mathbb{F}_q[x_1, \dots, x_n]$ is defined as

Generalized Triangular Dynamical System (GTDS)

- $\mathbb{F}_q$ finite field, $n \in \mathbb{Z}_{\geq 1}$.
- $p_i \in \mathbb{F}_q[x_i]$ permutation polynomials.
- $g_i, h_i \in \mathbb{F}_q[x_{i+1}, \dots, x_n]$ polynomials such that the g_i's do not have zeros.
- Then the GTDS $\mathcal{F} = \{f_1, \dots, f_n\} \subset \mathbb{F}_q[x_1, \dots, x_n]$ is defined as

$$f_n(x_1, \dots, x_n) = p_n(x_n).$$

Generalized Triangular Dynamical System (GTDS)

- $\mathbb{F}_q$ finite field, $n \in \mathbb{Z}_{\geq 1}$.
- $p_i \in \mathbb{F}_q[x_i]$ permutation polynomials.
- $g_i, h_i \in \mathbb{F}_q[x_{i+1}, \dots, x_n]$ polynomials such that the g_i's do not have zeros.
- Then the GTDS $\mathcal{F} = \{f_1, \dots, f_n\} \subset \mathbb{F}_q[x_1, \dots, x_n]$ is defined as

$$
\begin{aligned}
f_{n-1}(x_1, \dots, x_n) &= p_{n-1}(x_{n-1}) \cdot g_{n-1}(x_n) + h_{n-1}(x_n), \\
f_n(x_1, \dots, x_n) &= p_n(x_n).
\end{aligned}
$$

Generalized Triangular Dynamical System (GTDS)

- $\mathbb{F}_q$ finite field, $n \in \mathbb{Z}_{\geq 1}$.
- $p_i \in \mathbb{F}_q[x_i]$ permutation polynomials.
- $g_i, h_i \in \mathbb{F}_q[x_{i+1}, \dots, x_n]$ polynomials such that the g_i's do not have zeros.
- Then the GTDS $\mathcal{F} = \{f_1, \dots, f_n\} \subset \mathbb{F}_q[x_1, \dots, x_n]$ is defined as

$$
\begin{aligned}
f_1(x_1, \dots, x_n) &= p_1(x_1) \cdot g_1(x_2, \dots, x_n) + h_1(x_2, \dots, x_n), \\
f_2(x_1, \dots, x_n) &= p_2(x_2) \cdot g_2(x_3, \dots, x_n) + h_2(x_3, \dots, x_n), \\
&\vdots \\
f_{n-1}(x_1, \dots, x_n) &= p_{n-1}(x_{n-1}) \cdot g_{n-1}(x_n) + h_{n-1}(x_n), \\
f_n(x_1, \dots, x_n) &= p_n(x_n).
\end{aligned}
$$

Invertibility of the GTDS

- Suppose we are given $\mathcal{F}(\boldsymbol{x}) = \boldsymbol{\alpha} \in \mathbb{F}_q^n$.
- For the n-th component:

$$p_n(x_n) = \alpha_n \qquad \Longrightarrow \qquad x_n = p_n^{-1}(\alpha_n).$$

Invertibility of the GTDS

- Suppose we are given $\mathcal{F}(\boldsymbol{x}) = \boldsymbol{\alpha} \in \mathbb{F}_q^n$.
- For the n-th component:

$$p_n(x_n) = \alpha_n \qquad \Longrightarrow \qquad x_n = p_n^{-1}(\alpha_n).$$

- For the $(n-1)$-th component:

$$p_{n-1}(x_{n-1}) \cdot g_{n-1}(x_n) + h_{n-1}(x_n) = \beta_{n-1}$$

Invertibility of the GTDS

- Suppose we are given $\mathcal{F}(\boldsymbol{x}) = \boldsymbol{\alpha} \in \mathbb{F}_q^n$.
- For the n-th component:

$$p_n(x_n) = \alpha_n \qquad \Longrightarrow \qquad x_n = p_n^{-1}(\alpha_n).$$

- For the $(n-1)$-th component:

$$p_{n-1}(x_{n-1}) \cdot g_{n-1}(x_n) + h_{n-1}(x_n) = \beta_{n-1}$$
$$\overset{g_{n-1}(x_n) \neq 0}{\Longrightarrow} p_{n-1}(x_{n-1}) = \frac{\beta_{n-1} - h_{n-1}(x_n)}{g_{n-1}(x_n)}$$

universität innsbruck | UNIVERSITÄT KLAGENFURT

Invertibility of the GTDS

- Suppose we are given $\mathcal{F}(\boldsymbol{x}) = \boldsymbol{\alpha} \in \mathbb{F}_q^n$.
- For the n-th component:

$$p_n(x_n) = \alpha_n \qquad \Longrightarrow \qquad x_n = p_n^{-1}(\alpha_n).$$

- For the $(n-1)$-th component:

$$\begin{aligned} p_{n-1}(x_{n-1}) \cdot g_{n-1}(x_n) + h_{n-1}(x_n) &= \beta_{n-1} \\ \overset{g_{n-1}(x_n) \neq 0}{\Longrightarrow} p_{n-1}(x_{n-1}) &= \frac{\beta_{n-1} - h_{n-1}(x_n)}{g_{n-1}(x_n)} \\ \Longrightarrow x_{n-1} &= p_{n-1}^{-1}\left(\frac{\beta_{n-1} - h_{n-1}(x_n)}{g_{n-1}(x_n)}\right). \end{aligned}$$

Invertibility of the GTDS

- Suppose we are given $\mathcal{F}(\boldsymbol{x}) = \boldsymbol{\alpha} \in \mathbb{F}_q^n$.
- For the n-th component:

$$p_n(x_n) = \alpha_n \qquad \Longrightarrow \qquad x_n = p_n^{-1}(\alpha_n).$$

- For the $(n-1)$-th component:

$$\begin{aligned} p_{n-1}(x_{n-1}) \cdot g_{n-1}(x_n) + h_{n-1}(x_n) &= \beta_{n-1} \\ \overset{g_{n-1}(x_n)\neq 0}{\Longrightarrow} p_{n-1}(x_{n-1}) &= \frac{\beta_{n-1} - h_{n-1}(x_n)}{g_{n-1}(x_n)} \\ \Longrightarrow x_{n-1} &= p_{n-1}^{-1}\left(\frac{\beta_{n-1} - h_{n-1}(x_n)}{g_{n-1}(x_n)}\right). \end{aligned}$$

- Iterate through $i = n-2, \ldots, 1$.

universität innsbruck UNIVERSITÄT KLAGENFURT

Enforcing No Zeros

- In general, finding $g_i \in \mathbb{F}_q[x_{i+1}, \ldots, x_n]$ such that $g_i(x_{i+1}, \ldots, x_n) \neq 0$ for all $x_{i+1}, \ldots, x_n \in \mathbb{F}_q$ is non-trivial.
- For MPC and ZK applications q usually is prime.

Enforcing No Zeros

- In general, finding $g_i \in \mathbb{F}_q[x_{i+1}, \ldots, x_n]$ such that $g_i(x_{i+1}, \ldots, x_n) \neq 0$ for all $x_{i+1}, \ldots, x_n \in \mathbb{F}_q$ is non-trivial.
- For MPC and ZK applications q usually is prime.
- Over prime fields we can use special case

$$g(x) = x^2 + a \cdot x + b.$$

Enforcing No Zeros

- In general, finding $g_i \in \mathbb{F}_q[x_{i+1}, \ldots, x_n]$ such that $g_i(x_{i+1}, \ldots, x_n) \neq 0$ for all $x_{i+1}, \ldots, x_n \in \mathbb{F}_q$ is non-trivial.
- For MPC and ZK applications q usually is prime.
- Over prime fields we can use special case

$$g(x) = x^2 + a \cdot x + b.$$

- With well-known formula for $g(x) = 0$

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4 \cdot a}}{2},$$

  we have that $g(x) \neq 0$ for all $x \in \mathbb{F}_q$ if and only if $b^2 - 4 \cdot a$ is non-square modulo q.
- Build more general g_i starting from g.

GTDS Instances I

SPN	GTDS
$\begin{pmatrix} p_1(x_1) \\ \vdots \\ p_n(x_n) \end{pmatrix}$	$\begin{pmatrix} p_1(x_1)\cancel{\cdot g_1(x_2,\dots,x_n)+h_1(x_2,\dots,x_n)} \\ \vdots \\ p_{n-1}(x_{n-1})\cancel{\cdot g_{n-1}(x_n)+h_{n-1}(x_n)} \\ p_n(x_n) \end{pmatrix}$
Generalized Feistel	**GTDS**
$\begin{pmatrix} x_1+h_1(x_2,\dots,x_n) \\ \vdots \\ x_{n-1}+h_n(x_n) \\ x_n \end{pmatrix}$	$\begin{pmatrix} x_1\cancel{\cdot g_1(x_2,\dots,x_n)}+h_1(x_2,\dots,x_n) \\ \vdots \\ x_{n-1}\cancel{\cdot g_{n-1}(x_n)}+h_n(x_n) \\ x_{n-1} \end{pmatrix}$

GTDS Instances II

- Horst Scheme [GHR+22, GHR+23]: $g, h \in \mathbb{F}_q[x]$ such that g does not have any zeros, then

$$\texttt{Horst}\begin{pmatrix} x_L \\ x_R \end{pmatrix} = \begin{pmatrix} x_R \\ x_L \cdot g(x_R) + h(x_R) \end{pmatrix}.$$

  - Independent development from us at the same time.

GTDS Instances II

- `Horst` Scheme [GHR+22, GHR+23]: $g, h \in \mathbb{F}_q[x]$ such that g does not have any zeros, then

$$\texttt{Horst}\begin{pmatrix} x_L \\ x_R \end{pmatrix} = \begin{pmatrix} x_R \\ x_L \cdot g(x_R) + h(x_R) \end{pmatrix}.$$

  - Independent development from us at the same time.
- `Horst` variations with $h = 0$ are used in Griffin [GHR+23] and `Reinforced Concrete`'s [GKL+22] `Bricks`.
  - Let $p, d, a_i, b_i \in \mathbb{Z}$ be such that p is prime, $\gcd(d, p-1) = 1$ and $b_i^2 - 4 \cdot a_i$ are non-squares modulo p:

$$\texttt{Bricks}: \mathbb{F}_p^3 \to \mathbb{F}_p^3, \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} x_1^d \\ x_2 \cdot \left(x_1^2 + a_1 \cdot x_1 + b_1\right) \\ x_3 \cdot \left(x_2^2 + a_2 \cdot x_2 + b_2\right) \end{pmatrix}.$$

GTDS Instances III

- Arion & ArionHash [RST23]: Offspring of this work.
  - First design that utilizes a full GTDS at round level.

[1] Recommended choices are $d_1 \in \{3, 5, 7\}$ and $d_2 \in \{129, 257\}$.

GTDS Instances III

- Arion & ArionHash [RST23]: Offspring of this work.
  - First design that utilizes a full GTDS at round level.
  - Let $p, d_1, d_2, n \in \mathbb{Z}_{\geq 1}$[1] be such that $\gcd(d_1 \cdot d_2, p - 1) = 1$.

[1] Recommended choices are $d_1 \in \{3, 5, 7\}$ and $d_2 \in \{129, 257\}$.

GTDS Instances III

- Arion & ArionHash [RST23]: Offspring of this work.
  - First design that utilizes a full GTDS at round level.
  - Let $p, d_1, d_2, n \in \mathbb{Z}_{\geq 1}$[1] be such that $\gcd(d_1 \cdot d_2, p - 1) = 1$.
  - Let $g_i, h_i \in \mathbb{F}_p[x_{i+1}, \dots, x_n]$ be quadratic polynomials such that the g_i's do not have zeros in $\mathbb{F}_p$.

[1] Recommended choices are $d_1 \in \{3, 5, 7\}$ and $d_2 \in \{129, 257\}$.

GTDS Instances III

- Arion & ArionHash [RST23]: Offspring of this work.
  - First design that utilizes a full GTDS at round level.
  - Let $p, d_1, d_2, n \in \mathbb{Z}_{\geq 1}$[1] be such that $\gcd\left(d_1 \cdot d_2, p - 1\right) = 1$.
  - Let $g_i, h_i \in \mathbb{F}_p[x_{i+1}, \dots, x_n]$ be quadratic polynomials such that the g_i's do not have zeros in $\mathbb{F}_p$.
- The Arion GTDS is defined as

$$
\begin{aligned}
f_i(x_1, \dots, x_n) &= x_i^{d_1} \cdot g_i(\sigma_{i+1,n}) + h_i(\sigma_{i+1,n}), \qquad 1 \leq i \leq n - 1, \\
f_n(x_1, \dots, x_n) &= x_n^{\frac{1}{d_2}},
\end{aligned}
$$

where

$$
\sigma_{i+1,n} = \sum_{j=i+1}^{n} x_j + f_j(x_1, \dots, x_n).
$$

[1] Recommended choices are $d_1 \in \{3, 5, 7\}$ and $d_2 \in \{129, 257\}$.

Differential Distribution Table [Nyb94]

- $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ function.
- The DDT entry of F at $\boldsymbol{a} \in \mathbb{F}_q^n$ and $\boldsymbol{b} \in \mathbb{F}_q^m$ is given by

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

- The Differential Uniformity of F is

$$\delta(F) = \max_{\boldsymbol{a} \in \mathbb{F}_q^n \setminus \{0\},\ \boldsymbol{b} \in \mathbb{F}_q^m} \delta_F(\boldsymbol{a}, \boldsymbol{b}).$$

Differential Distribution Table [Nyb94]

- $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ function.
- The DDT entry of F at $\boldsymbol{a} \in \mathbb{F}_q^n$ and $\boldsymbol{b} \in \mathbb{F}_q^m$ is given by

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

- The Differential Uniformity of F is

$$\delta(F) = \max_{\boldsymbol{a} \in \mathbb{F}_q^n \setminus \{0\},\ \boldsymbol{b} \in \mathbb{F}_q^m} \delta_F(\boldsymbol{a}, \boldsymbol{b}).$$

- For a GTDS $\mathcal{F}$ assume that $\delta(p_i) < q$ for all $1 \leq i \leq n$. (Then $\delta(p_i) < \deg(p_i)$.)

- Let us look at DDT equation

$$\begin{aligned} &\mathcal{F}(\boldsymbol{x}+\boldsymbol{a})-\mathcal{F}(\boldsymbol{x})=\boldsymbol{b} \\ \Rightarrow\ &p_n(x_n+a_n)-p_n(x_n)=b_n. \end{aligned}$$

  - At most $\deg(p_n)$ many solutions for $x_n \in \mathbb{F}_q$ if $a_n \neq 0$.

GDTS Cryptanalysis: Differential Cryptanalysis

- Let us look at DDT equation

$$\mathcal{F}(\boldsymbol{x} + \boldsymbol{a}) - \mathcal{F}(\boldsymbol{x}) = \boldsymbol{b}$$
$$\Rightarrow p_n(x_n + a_n) - p_n(x_n) = b_n.$$

  - At most $\deg(p_n)$ many solutions for $x_n \in \mathbb{F}_q$ if $a_n \neq 0$.
- For the $(n-1)$-th component, fix a solution $\tilde{x}_n \in \mathbb{F}_q$, then

$$p_{n-1}(x_{n-1} + a_{n-1}) \cdot g(\tilde{x}_n + a_n) + h(\tilde{x}_n + a_n)$$
$$- p_{n-1}(x_{n-1}) \cdot g(\tilde{x}_n) - h(\tilde{x}_n) = b_{n-1}.$$

universität innsbruck UNIVERSITÄT KLAGENFURT

- Let us look at DDT equation

$$\mathcal{F}(\boldsymbol{x}+\boldsymbol{a})-\mathcal{F}(\boldsymbol{x})=\boldsymbol{b}$$
$$\Rightarrow p_n(x_n+a_n)-p_n(x_n)=b_n.$$

  - At most $\deg(p_n)$ many solutions for $x_n \in \mathbb{F}_q$ if $a_n \neq 0$.
- For the $(n-1)$-th component, fix a solution $\tilde{x}_n \in \mathbb{F}_q$, then

$$p_{n-1}(x_{n-1}+a_{n-1})\cdot g(\tilde{x}_n+a_n)+h(\tilde{x}_n+a_n)$$
$$-p_{n-1}(x_{n-1})\cdot g(\tilde{x}_n)-h(\tilde{x}_n)=b_{n-1}.$$

  - If $a_{n-1}\neq 0$, then $\leq \deg(p_{n-1})$ many solutions for $x_{n-1}\in\mathbb{F}_q$.
  - Otherwise q many solutions $x_{n-1}\in\mathbb{F}_q$.

GDTS Cryptanalysis: Differential Cryptanalysis

- For a GTDS $\mathcal{F}$ with $1 < \delta(p_i) < q$, $1 \leq i \leq n$, upwards induction then yields that

$$\delta_{\mathcal{F}}(\boldsymbol{a}, \boldsymbol{b}) \leq \prod_{i=1}^{n} \begin{cases} \deg\left(p_i\right), & a_i \neq 0, \\ q, & a_i = 0. \end{cases}$$

- Almost the same DDT bound as SPN $\mathcal{S} = \big(p_1(x_1), \dots, p_n(x_n)\big)^\intercal$.
- The g_i, h_i's can only decrease the number of solutions, never increase them from the SPN bound.

universität innsbruck UNIVERSITÄT KLAGENFURT

Correlation [Bey21]

- $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ function, $\chi, \psi : \mathbb{F}_q^n \to \mathbb{C}$ additive characters.
- The correlation of F for the characters (χ, ψ) is given by

$$\mathrm{CORR}_F(\chi, \psi) = \frac{1}{q^n} \cdot \sum_{\boldsymbol{x} \in \mathbb{F}_q^n} \overline{\chi\big(F(\boldsymbol{x})\big)} \cdot \psi(\boldsymbol{x}).$$

Correlation [Bey21]

- $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ function, $\chi, \psi : \mathbb{F}_q^n \to \mathbb{C}$ additive characters.
- The correlation of F for the characters (χ, ψ) is given by

$$\mathrm{CORR}_F(\chi, \psi) = \frac{1}{q^n} \cdot \sum_{\mathbf{x} \in \mathbb{F}_q^n} \overline{\chi\big(F(\mathbf{x})\big)} \cdot \psi(\mathbf{x}).$$

- For a GTDS with $\gcd\left(\deg\left(p_i\right), q\right) = 1$, $1 \leq i \leq n$, we prove that

$$\left|\mathrm{CORR}_{\mathcal{F}}(\chi, \psi)\right| \leq \max_{1 \leq i \leq n} \frac{\deg\left(p_i\right) - 1}{\sqrt{q}}.$$

Correlation [Bey21]

- $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ function, $\chi, \psi : \mathbb{F}_q^n \to \mathbb{C}$ additive characters.
- The correlation of F for the characters (χ, ψ) is given by

$$\mathrm{CORR}_F(\chi, \psi) = \frac{1}{q^n} \cdot \sum_{\mathbf{x} \in \mathbb{F}_q^n} \overline{\chi(F(\mathbf{x}))} \cdot \psi(\mathbf{x}).$$

- For a GTDS with $\gcd(\deg(p_i), q) = 1$, $1 \leq i \leq n$, we prove that

$$|\mathrm{CORR}_{\mathcal{F}}(\chi, \psi)| \leq \max_{1 \leq i \leq n} \frac{\deg(p_i) - 1}{\sqrt{q}}.$$

- Gap between SPN bound

$$|\mathrm{CORR}_{\mathcal{S}}(\chi, \psi)| \leq \prod_{i=1}^{n} \begin{cases} \frac{\deg(p_i)-1}{\sqrt{q}}, & \chi \text{ non-const. on } x_i, \\ 1, & \text{else.} \end{cases}$$

Open Problems & Follow-Up Works

- **Open Problems**:
  - Extend generic analysis to more attacks and GTDS families.
  - For DDT, understand the impact of the g_i, h_i's.
  - For correlation, close the gap between SPN bound and our one.
  - Understand degree growth under iteration.
  - Etc.

universität innsbruck UNIVERSITÄT KLAGENFURT

Open Problems & Follow-Up Works

- **Open Problems**:
  - Extend generic analysis to more attacks and GTDS families.
  - For DDT, understand the impact of the g_i, h_i's.
  - For correlation, close the gap between SPN bound and our one.
  - Understand degree growth under iteration.
  - Etc.
- **Follow-Up Works**:
  - Arion & ArionHash [RST23], a cipher and hash function for Zero-Knowledge applications.
  - Estimation of the Boomerang Connectivity Table (BCT) for GTDS with $p_i(x_i) = x_i^d$ and $h_i = 0$ for all $1 \leq i \leq n$ [Ste23].

References I

Tim Beyne.
A geometric approach to linear cryptanalysis.
In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2021, Part I*, volume 13090 of *Lecture Notes in Computer Science*, pages 36–66, Singapore, December 6–10, 2021. Springer, Heidelberg, Germany.
doi:10.1007/978-3-030-92062-3_2.

Lorenzo Grassi, Yonglin Hao, Christian Rechberger, Markus Schofnegger, Roman Walch, and Qingju Wang.
A new Feistel approach meets fluid-SPN: Griffin for zero-knowledge applications.
Cryptology ePrint Archive, Report 2022/403, 2022.
https://eprint.iacr.org/2022/403.

universität innsbruck UNIVERSITÄT KLAGENFURT

References II

Lorenzo Grassi, Yonglin Hao, Christian Rechberger, Markus Schofnegger, Roman Walch, and Qingju Wang.
Horst meets fluid-SPN: Griffin for zero-knowledge applications.
In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology – CRYPTO 2023, Part III*, volume 14083 of *Lecture Notes in Computer Science*, pages 573–606, Santa Barbara, CA, USA, August 20–24, 2023. Springer, Heidelberg, Germany.
doi:10.1007/978-3-031-38548-3_19.

Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, Markus Schofnegger, and Roman Walch.
Reinforced concrete: A fast hash function for verifiable computation.
In Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi, editors, *ACM CCS 2022: 29th Conference on Computer and Communications Security*, pages 1323–1335, Los Angeles, CA, USA, November 7–11, 2022. ACM Press.
doi:10.1145/3548606.3560686.

Kaisa Nyberg.
Differentially uniform mappings for cryptography.
In Tor Helleseth, editor, *Advances in Cryptology – EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 55–64, Lofthus, Norway, May 23–27, 1994. Springer, Heidelberg, Germany.
doi:10.1007/3-540-48285-7_6.

Alina Ostafe and Igor E. Shparlinski.
On the degree growth in some polynomial dynamical systems and nonlinear pseudorandom number generators.
Math. Comput., 79(269):501–511, 2010.
doi:10.1090/S0025-5718-09-02271-6.

References V

Alina Ostafe and Igor E. Shparlinski.
Pseudorandom numbers and hash functions from iterations of multivariate polynomials.
Cryptography and Communications, 2(1):49–67, Apr 2010.
doi:10.1007/s12095-009-0016-0.

Arnab Roy, Matthias Johann Steiner, and Stefano Trevisani.
Arion: Arithmetization-oriented permutation and hashing from generalized triangular dynamical systems.
arXiv: 2303.04639, 2023.
Version: 3.
arXiv:2303.04639, doi:10.48550/ARXIV.2303.04639.

References VI

Matthias Johann Steiner.
A degree bound for the c-boomerang uniformity of permutation monomials, 2023.
arXiv:2307.12621.