Towards the Links of Cryptanalytic Methods on MPC/FHE/ZK-Friendly Symmetric-Key Primitives

Shiyao Chen, Chun Guo, Jian Guo, Li Liu, Meiqin Wang, Puwen Wei, Zeyu Xu

Nanyang Technological University
Shandong University

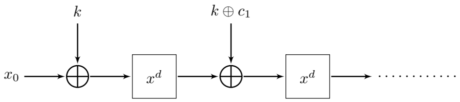
Mar, 2024 @ Leuven, Belgium

Contents

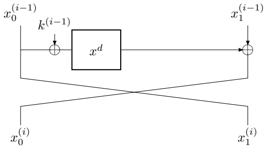
Contents

New Types of Finite Field Friendly Designs

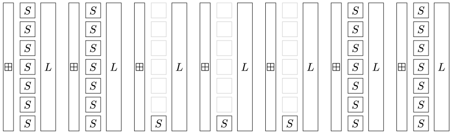
Many MPC/FHE/ZK-friendly ciphers are designed with novel operations and constructions, e.g., LowMC, MiMC, GMiMC, HADES, Ciminion, Rescue...



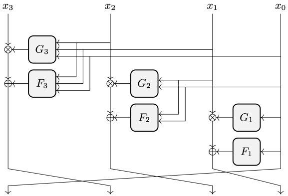
SPN



Feistel



P-SPN



Horst

Challenges of Cryptanalysis for Newly Symmetric-Key Primitives

Novel design ideas and constructions naturally lead to some potential threats.

- Algebraic attacks:
  - Gröbner-basis attack on Jarvis and Friday [ACG$^+$19].
  - High-order attack on full-round MiMC [EGL$^+$20].
  - Coefficient Grouping breaks Chaghri [LAW$^+$23].
  - etc.
- Statistical attacks:
  - Truncated differential attack on full-round GMiMC [BCD$^+$20].
  - etc.

Cryptanalysis and design of newly symmetric-key ciphers are becoming interesting but challenging tasks.

- Cryptanalysis needs to be investigated further.
- Design could be aided by more in-depth cryptanalysis.

Algebraic Cryptanalysis over Finite Field

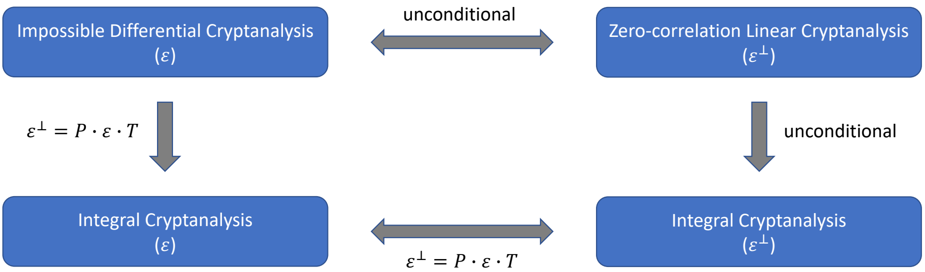
These novel symmetric-key designs are usually more vulnerable to algebraic attacks.

How to accurately evaluate algebraic properties of these new ciphers is still difficult.

There are usually two methods: degree-based and structural-based.

Links among Different Cryptanalytic Methods over $\mathbb{F}_2^n$

Links among different symmetric cryptanalytic methods over $\mathbb{F}_2^n$ have been well studied.



For example, links among impossible differential, zero-correlation linear and integral cryptanalysis over $\mathbb{F}_2^n$ [SLR$^+$15].

Why We Focus on Links over $\mathbb{F}_p$ ($p > 2$)?

- Integral (INT) cryptanalysis over $\mathbb{F}_p$ is still difficult to evaluate accurately.
- Impossible differential (IDC) and/or Zero-correlation linear hull (ZC) over $\mathbb{F}_p$ may be easier to construct.
- It will be convienient to derive structural-based integral distinguisher if with the links among IDC, ZC and INT over $\mathbb{F}_p$.

Contents

Main Obstacle of Generalizing Links to $\mathbb{F}_p$

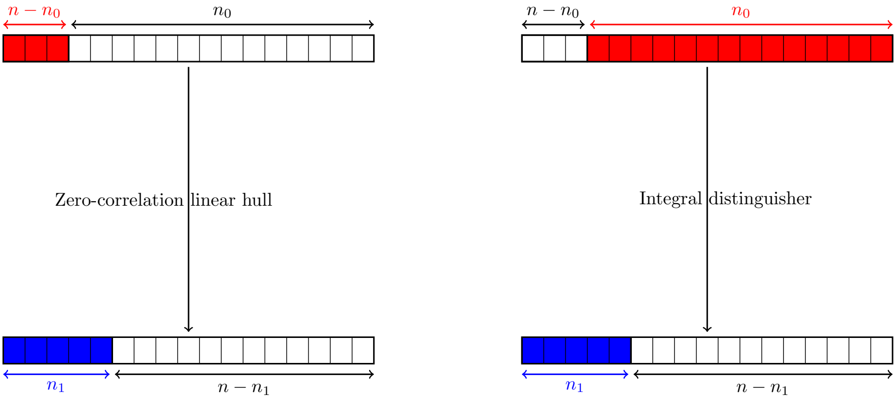
Definition (Correlation over $\mathbb{F}_p$ [BSV07])

Given a function $F : \mathbb{F}_p^t \to \mathbb{F}_p^s$, for a linear mask pair (u, v), where $u \in \mathbb{F}_p^t$ and $v \in \mathbb{F}_p^s$, then the correlation of linear approximation (u, v) of F is defined as

$$cor_F(u,v) = cor(u^T \cdot x - v^T \cdot F(x)) = \frac{1}{p^t} \sum_{x \in \mathbb{F}_p^t} \chi_u(x)\overline{\chi_v(F(x))} = \frac{1}{p^t} \sum_{x \in \mathbb{F}_p^t} e^{\frac{2\pi i}{p}(u^T \cdot x - v^T \cdot F(x))}.$$

- Considering the linear correlation over $\mathbb{F}_2^n$, parity-check is extensively used for its fast calculation.
- However, the correlation over $\mathbb{F}_p$, defined over a complex plane by Baignères *et al.* [BSV07], thus more complicated.
- Until the recent design Ciminion [DGGK21], trying to evaluate the security against this kind of linear attacks over $\mathbb{F}_p$.

Links of ZC and INT over $\mathbb{F}_p$



For the balance property and zero correlation, ZC and INT are the connections between the links over $\mathbb{F}_p$.

From ZC to INT over $\mathbb{F}_p$

Theorem (ZC to INT over $\mathbb{F}_p$)

If there exists a subspace A of $\mathbb{F}_p^t$ and a mask $b \in \mathbb{F}_p^t \backslash \{0\}$, such that for any $a \in A$, $cor(a^T \cdot x - b^T \cdot F(x)) = 0$ where $x \in \mathbb{F}_p^t$. For any $\lambda \in \mathbb{F}_p^t$, function $G_\lambda : A^\perp \mapsto \mathbb{F}_p^t$ is defined as $G_\lambda(x) = E(x + \lambda)$. Then for any $\lambda \in \mathbb{F}_p^t$, $b^T \cdot G_\lambda(x)$ is balanced on the subspace $A^\perp$, that is $cor(-b^T \cdot G_\lambda(x)) = 0$.

- For the condition over $\mathbb{F}_2^n$
    - "*input and output linear masks in zero-correlation approximations are independent*", as claimed in [BLNW12].
    - Later, this condition was relaxed in [SLR+15].
- However, it requires a subspace for the input mask when transforming ZC to INT over $\mathbb{F}_p$.[1]

[1] Beyne [Bey21] has already provided new insights into linear cryptanalysis over abelian groups and generalized the link between zero-correlation and integral attacks, which are obtained by introducing a geometric approach.

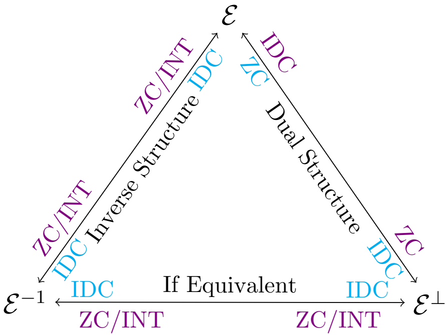
From INT to ZC over $\mathbb{F}_p$

Theorem (INT to ZC over $\mathbb{F}_p$)

Let $E(x) : \mathbb{F}_p^t \to \mathbb{F}_p^t$ be a function over $\mathbb{F}_p^t$, A be a nontrivial subspace of $\mathbb{F}_p^t$ and its orthogonal space $A^{\perp} = \{x \in \mathbb{F}_p^t | a^T \cdot x = 0, a \in A\}$. For any $\lambda \in \mathbb{F}_p^t$, function $G_\lambda : A^{\perp} \mapsto \mathbb{F}_p^t$ is defined as $G_\lambda(x) = E(x + \lambda)$. Then an integral distinguisher of E can lead to a zero-correlation linear hull with input masks A and nonzero output mask b, if and only if it is a balanced integral distinguisher with $b^T \cdot G_\lambda(x)$ balanced on the subspace $A^{\perp}$.

- Similar to that over $\mathbb{F}_2^n$, only INT with balanced property can be converted into ZC over $\mathbb{F}_p$.

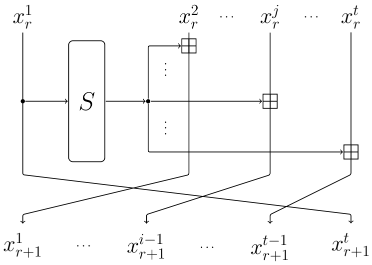
More Refined Links among IDC, ZC and INT over $\mathbb{F}_p$



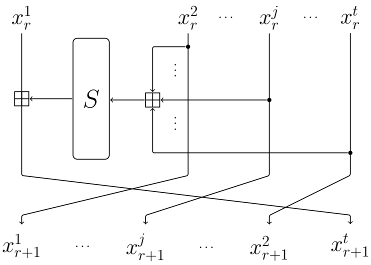
By covering more constructions ($\mathcal{F}_{SP}$, $\mathcal{GF}_{SP}$, $\mathcal{E}_{FP}$, $\mathcal{E}_{erf}, \mathcal{E}_{crf}$) and underlying structures ($\mathcal{E}$, $\mathcal{E}^{\perp}$, $\mathcal{E}^{-1}$), more refined links between IDC, ZC and INT over $\mathbb{F}_p$ are established.

Contents

Applications to GMiMC with Unbalanced Feistel Networks



The round function of $\text{GMiMC}_{\texttt{erf}}$.

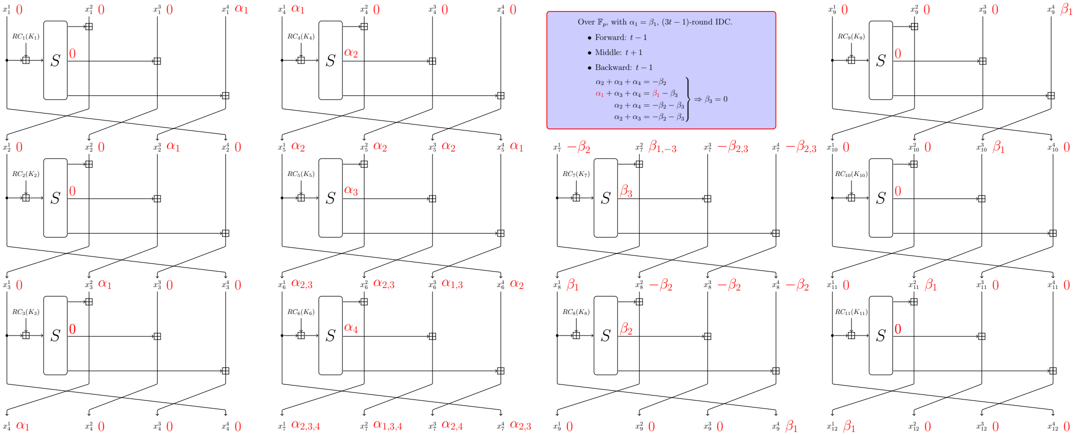


The round function of $\text{GMiMC}_{\texttt{crf}}$.

- Algebraic equation-based method for finding IDC/ZC.
- INT can be directly converted from IDC/ZC.
- Improvements up to 3-round for most cases, *arbitrary number of rounds* for special and limited cases.

Ciphers	Type	Rounds	Remarks	Source
$\text{GMiMC}_{\texttt{erf}}$	IDC	$2t-2$	$\alpha_1, \beta_1 \neq 0^\dagger$	[AGP+19]
		$3t-4$	$\alpha_1, \beta_1 \neq 0$ and $\alpha_1 \neq \beta_1$	[BCD+20]
		$\mathbf{3t-3}$	$\alpha_1, \beta_1 \neq 0$	This work
		$\mathbf{3t-1}$	$\alpha_1 = \beta_1$ and $t \not\equiv 1 \bmod p$	This work
		Arbitrary	$\alpha_1 = -\beta_1$ and $t \equiv 1 \bmod p$	This work
	ZC	$3t-4$	Transformed from IDC in [AGP+19]	
		$\mathbf{3t-3}$	$a_1, b_1 \neq 0^{\dagger\dagger}$	This work
		$\mathbf{3t-1}$	$a_1 = b_1$	This work
		Arbitrary	$t \equiv 1 \bmod p$	This work
	INT	$t + \lceil \log_3(t) \rceil^*$	Higher-order	[AGP+19]
		$2t - 2 + \lfloor \log_3(p-2) \rfloor$	Algebraic control method (Block cipher)	[BCD+20]
		$\mathbf{3t-3}$		This work
		$3t - 4 + \lfloor \log_3(p-2) \rfloor$	Algebraic control method (Hash function)	[BCD+20]
		Arbitrary	$t \equiv 1 \bmod p$	This work
	LC	$t-1$		[BCD+20]
		Arbitrary	$t \equiv 1 \bmod p$	This work
$\text{GMiMC}_{\texttt{crf}}$	IDC	$3t-4$		[AGP+19]
		$\mathbf{3t-3}$	$\alpha_1, \beta_1 \neq 0$	This work
		$\mathbf{3t-1}$	$\alpha_1 = \beta_1$	This work
		Arbitrary	$t \equiv 1 \bmod p$	This work
	ZC	$\mathbf{3t-3}$	$a_1, b_1 \neq 0$	This work
		$\mathbf{3t-1}$	$a_1 = b_1$ and $t \not\equiv 1 \bmod p$	This work
		Arbitrary	$a_1 = -b_1$ and $t \equiv 1 \bmod p$	This work
	INT	$2t + \lceil \log_3(t) \rceil^*$	Higher-order	[AGP+19]
		$\mathbf{3t-3}$		This work
	DC	$t-1$		
		Arbitrary	$t \equiv 1 \bmod p$	This work

Improvements of $(3t-1)$-round IDC of GMiMC$_{\texttt{erf}}$



$(3t-1)$ rounds IDC example of GMiMC$_{\texttt{erf}}$ with number of branch $t=4$.

Special Arbitrary Number of Rounds IDC of GMiMC$_{\texttt{erf}}$

For GMiMC$_{\texttt{erf}}$, special arbitrary number of rounds IDC can be constructed

- Input difference $(0, \cdots, 0, \alpha_1)$ and output difference $(\beta_1, 0, \cdots, 0)$
- $\alpha_1 = -\beta_1 \neq 0$
- $t \equiv 1 \bmod p$ (this condition may be possible for some ZK use cases also with full-data security)

However, this cannot be adapted to $\mathbb{F}_2^n$, due to the following equation

$$\alpha_1 + (t-1)\cdot\alpha_2 + \cdots (t-1)\cdot\alpha_{r_1+1} \equiv \beta_1 - (t-1)\cdot\beta_2 - \cdots (t-1)\cdot\beta_{r_2+1} \bmod p,$$

then combined with $\alpha_1 = -\beta_1$, we have $\alpha_1 = \beta_1 = 0$.

Contents

Conclusion

- Links over $\mathbb{F}_p$ could be useful tools for design and cryptanalysis of these newly MPC/FHE/ZK-friendly ciphers.
- More algebraic properties of symmetric ciphers over $\mathbb{F}_p$ are expected to be investigated.
- Novel non-linear operations, for example, the recent comprehensive analysis of Quadratic Functions [GOPS22, GGOP23, Gra23].

Thanks for your attention

[ACG+19] Martin R. Albrecht, Carlos Cid, Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, and Markus Schofnegger.
Algebraic cryptanalysis of STARK-friendly designs: Application to MARVELlous and MiMC.
In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019*, volume 11923 of *LNCS*, pages 371–397. Springer, 2019.

[AGP+19] M. R. Albrecht, L. Grassi, L. Perrin, S. Ramacher, C.n Rechberger, D. Rotaru, A. Roy, and M. Schofnegger.
Feistel structures for mpc, and more.
In *ESORICS 2019*, volume 11736 of *Lecture Notes in Computer Science*, pages 151–171. Springer, 2019.

[BCD+20] T. Beyne, A. Canteaut, I. Dinur, M. Eichlseder, G. Leander, G. Leurent, M. Naya-Plasencia, L. Perrin, Y. Sasaki, Y. Todo, and F. Wiemer.
Out of oddity - new cryptanalytic techniques against symmetric primitives optimized for integrity proof systems.
In *CRYPTO 2020*, volume 12172 of *Lecture Notes in Computer Science*, pages 299–328. Springer, 2020.

[Bey21] Tim Beyne.
A geometric approach to linear cryptanalysis.
In *Advances in Cryptology - ASIACRYPT 2021, Part I*, pages 36–66, 2021.

[BLNW12] Andrey Bogdanov, Gregor Leander, Kaisa Nyberg, and Meiqin Wang.
Integral and multidimensional linear distinguishers with correlation zero.
In *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, pages 244–261, 2012.

[BSV07] Thomas Baignères, Jacques Stern, and Serge Vaudenay.
Linear cryptanalysis of non binary ciphers.
In Carlisle M. Adams, Ali Miri, and Michael J. Wiener, editors, *SAC 2007*, volume 4876 of *LNCS*, pages 184–211. Springer, 2007.

[DGGK21] Christoph Dobraunig, Lorenzo Grassi, Anna Guinet, and Daniël Kuijsters.
Ciminion: Symmetric encryption based on toffoli-gates over large finite fields.
In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology - EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 3–34. Springer, 2021.

[EGL+20] Maria Eichlseder, Lorenzo Grassi, Reinhard Lüftenegger, Morten Øygarden, Christian Rechberger, Markus Schofnegger, and Qingju Wang.
An algebraic attack on ciphers with low-degree round functions: Application to full mimc.
In *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I*, pages 477–506, 2020.

[GGOP23] Ginevra Giordani, Lorenzo Grassi, Silvia Onofri, and Marco Pedicini.
Invertible quadratic non-linear functions over $\mathbb{F}_p^n$ via multiple local maps.
In *Progress in Cryptology - AFRICACRYPT 2023 - 14th International Conference on Cryptology in Africa, Sousse, Tunisia, July 19-21, 2023, Proceedings*, pages 151–176, 2023.

[GOPS22] Lorenzo Grassi, Silvia Onofri, Marco Pedicini, and Luca Sozzi.
Invertible quadratic non-linear layers for mpc-/fhe-/zk-friendly schemes over fnp application to poseidon.
IACR Trans. Symmetric Cryptol., 2022(3):20–72, 2022.

[Gra23] Lorenzo Grassi.
Bounded surjective quadratic functions over fnp for mpc-/zk-/fhe-friendly symmetric primitives.
IACR Trans. Symmetric Cryptol., 2023(2):94–131, 2023.

[LAW+23] Fukang Liu, Ravi Anand, Libo Wang, Willi Meier, and Takanori Isobe.
Coefficient grouping: Breaking chaghri and more.
In *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part IV*, pages 287–317, 2023.

[SLR+15] Bing Sun, Zhiqiang Liu, Vincent Rijmen, Ruilin Li, Lei Cheng, Qingju Wang, Hoda AlKhzaimi, and Chao Li.
Links among impossible differential, integral and zero correlation linear cryptanalysis.
In *Advances in Cryptology - CRYPTO 2015, Part I*, pages 95–115, 2015.