Ultrametric Integral Cryptanalysis

Tim Beyne, **Michiel Verbauwhede**

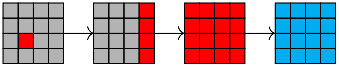
COSIC, KU Leuven

December 10, 2024

Integral Cryptanalysis

Structural approach

Integral cryptanalysis
[Knudsen and Wagner, 2002]



Algebraic approach

Higher order differentials [Knudsen, 1995]

$$\sum_{x \in V} f(x + a) = 0$$

where $\deg(f) < \dim(V)$

Partial consolidation

- Division property [Todo, 2015]
- Parity sets [Boura and Canteaut, 2016]
- Monomial trails [Hu et al., 2020]
- Algebraic trails [Beyne and Verbauwhede, 2023]

$$\{x | x \preccurlyeq u\} \rightarrow \sum_{x \preccurlyeq u} x^v = \delta^u(v) \leftarrow \sum_{v \in \mathbb{F}_2^n} \lambda_v x^v$$

Divisibility Properties

Zero-sum over $\mathbb{F}_2$

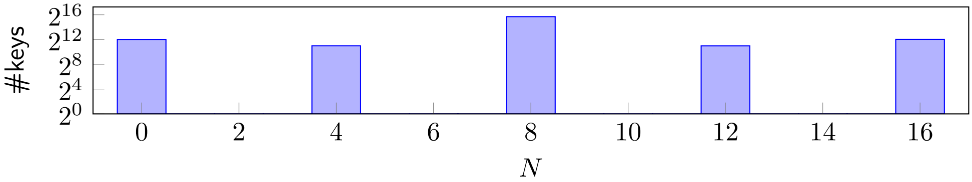
$\sum_{x \in X} f(x) = 0$

Saturation

$f(x) = 1$ has $|X|/2$ solutions in X

Divisibility by 2^t

Experiment on 4-round PRESENT:



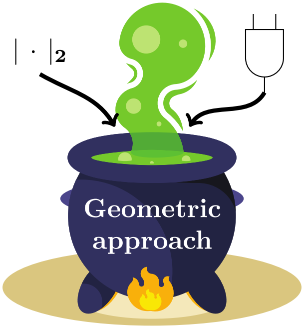
Overview

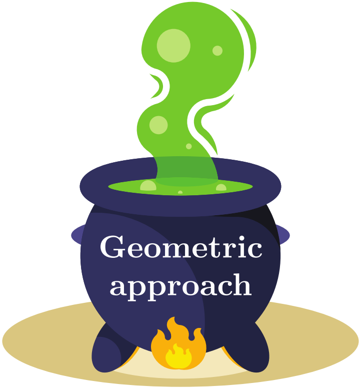
Goals

- Understand and analyze divisibility properties
- Improve understanding of integral cryptanalysis

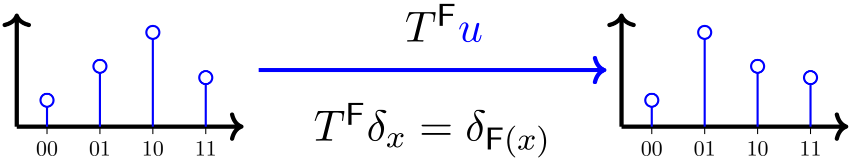
Ultrametric integral cryptanalysis in the geometric approach

- 2-adic absolute value on $\mathbb{Q}$
- Multiplicative analog of linear cryptanalysis




Geometric
approach

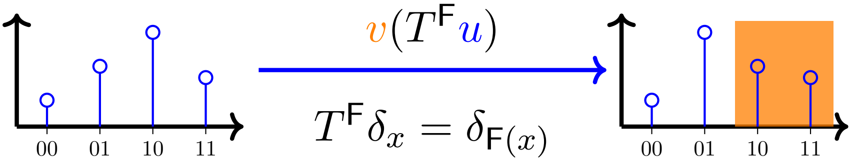
Geometric Approach



Properties

- $T^{\mathsf{F}_2 \circ \mathsf{F}_1} = T^{\mathsf{F}_2} T^{\mathsf{F}_1}$
- $T^{\mathsf{F}_1 \| \mathsf{F}_2} = T^{\mathsf{F}_1} \otimes T^{\mathsf{F}_2}$

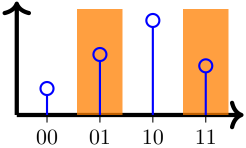
Geometric Approach



Properties

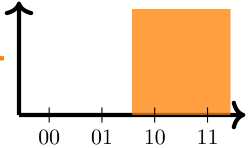
- $T^{\mathsf{F}_2 \circ \mathsf{F}_1} = T^{\mathsf{F}_2} T^{\mathsf{F}_1}$
- $T^{\mathsf{F}_1 \| \mathsf{F}_2} = T^{\mathsf{F}_1} \otimes T^{\mathsf{F}_2}$

Geometric Approach



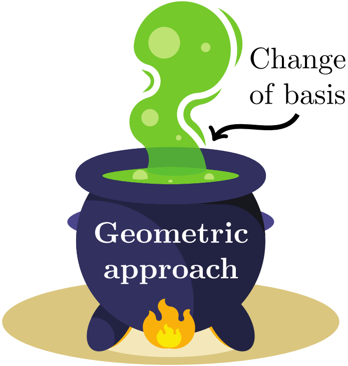
$$(T^{\mathsf{F}^\vee} v)(u)$$

$$T^{\mathsf{F}^\vee} v = v \circ \mathsf{F}$$



Properties

- $T^{\mathsf{F}_2 \circ \mathsf{F}_1{}^\vee} = T^{\mathsf{F}_1{}^\vee} T^{\mathsf{F}_2{}^\vee}$
- $T^{\mathsf{F}_1 \| \mathsf{F}_2{}^\vee} = T^{\mathsf{F}_1{}^\vee} \otimes T^{\mathsf{F}_2{}^\vee}$


Change
of basis
Geometric
approach

Linear Cryptanalysis

Simplifying key addition

- Basis, $\{\chi_u\}$, diagonalizes T^{+t}, i.e. $x \mapsto x + t$
- Dual basis of characters, $\{\chi^v\}$, where $\chi^v(\chi_u) = \delta^v(u)$
- Correlation matrix: $C^{\mathsf{F}} = \mathscr{F} T^{\mathsf{F}} \mathscr{F}^{-1}$

$$C^{+t} = \mathscr{F} T^{+t} \mathscr{F}^{-1}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & (-1)^t \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1-t & t \\ t & 1-t \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

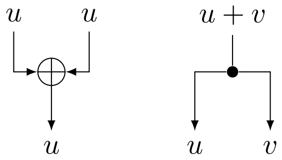
Orthogonal

Linear Cryptanalysis

Properties

- $C^{\mathsf{F}_2 \circ \mathsf{F}_1} = C^{\mathsf{F}_2} C^{\mathsf{F}_1}$
- $C^{\mathsf{F}_1 \| \mathsf{F}_2} = C^{\mathsf{F}_1} \otimes C^{\mathsf{F}_2}$
- If F is a linear map, then

$$C^{\mathsf{F}}_{v,u} = \begin{cases} 1, & \text{if } \chi^v \circ \mathsf{F} = \chi^u \\ 0, & \text{otherwise} \end{cases}$$



Linear Cryptanalysis

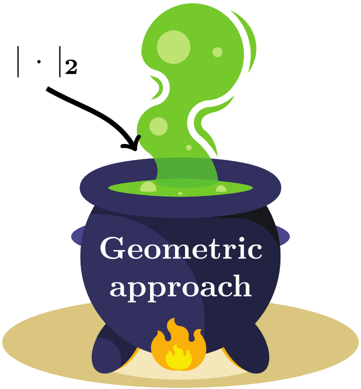
Dominant trail approximation

$$C^{\mathsf{F}_r \circ \cdots \circ \mathsf{F}_1} = C^{\mathsf{F}_r} \cdots C^{\mathsf{F}_1}$$

$$C^{\mathsf{F}_r \circ \cdots \circ \mathsf{F}_1}_{u_{r+1},u_1} = \underbrace{\sum_{u_2,\ldots,u_r}}_{\text{trail}} \underbrace{\prod_{i=1}^{r} C^{\mathsf{F}_i}_{u_{i+1},u_i}}_{\text{correlation}} = \sum_{u \in \Lambda} \prod_{i=1}^{r} C^{\mathsf{F}_i}_{u_{i+1},u_i} + \underbrace{\sum_{u \in \Omega \setminus \Lambda} \prod_{i=1}^{r} C^{\mathsf{F}_i}_{u_{i+1},u_i}}_{|\cdot| \approx 0}$$

Zero-correlation linear cryptanalysis

$$\prod_{i=1}^{r} C^{\mathsf{F}_i}_{u_{i+1},u_i} = 0 \text{ for all } u \in \Omega \implies C^{\mathsf{F}_r \circ \cdots \circ \mathsf{F}_1}_{u_{r+1},u_1} = 0$$


$\| \cdot \|_2$
Geometric approach

Metric Structure

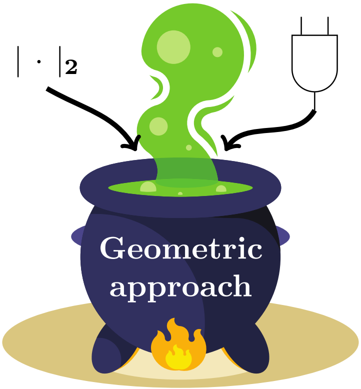
Divisibility property in the geometric approach

$$v(T^{\mathsf{F}} u) \equiv 0 \mod 2^{\nu}$$

- u is indicator of input set
- v maps output bit to $\{0,1\} \subset \mathbb{Q}$

2-adic absolute value

- 2-adic absolute value $|x|_2 = 2^{-\nu}$ where 2^{ν} is the largest power of 2 dividing $x \in \mathbb{Z}$
- $\left|v(T^{\mathsf{F}} u)\right|_2 \leq 2^{-\nu}$
- Ultrametric triangle inequality $|x+y|_2 \leq \max\{|x|_2, |y|_2\}$


$\| \cdot \|_2$
Geometric approach

Simplifying Bit-wise AND with Constants

- Character basis diagonalizes $T^{\wedge t}$, i.e. $x \mapsto x \wedge t$
- $\tau : \mathbb{F}_2 \to \mathbb{Q}$, where $\tau(0) = 0$, $\tau(1) = 1$
- $\mu^v(x) = \tau(x^v)$ and $\mu_u(x) = \sum_{x \preccurlyeq u} (-1)^{\mathsf{wt}(x+u)} \delta_x$
- Ultrametric integral transition matrix: $A^{\mathsf{F}} = \mathscr{U} T^{\mathsf{F}} \mathscr{U}^{-1}$

$$A^{\wedge t} = \mathscr{U} T^{\wedge t} \mathscr{U}^{-1}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & \tau(t) \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 - \tau(t) \\ 0 & \tau(t) \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$$

Non-orthogonal

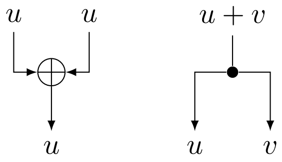
- $A^{\mathsf{F}} \mod 2$ is the algebraic transition matrix

Ultrametric Integral Transition Matrices

Properties

- $C^{\mathsf{F}_2 \circ \mathsf{F}_1} = C^{\mathsf{F}_2} C^{\mathsf{F}_1}$
- $C^{\mathsf{F}_1 \| \mathsf{F}_2} = C^{\mathsf{F}_1} \otimes C^{\mathsf{F}_2}$
- If F is a linear map, then

$$C^{\mathsf{F}}_{v,u} = \begin{cases} 1, & \text{if } \chi^v \circ \mathsf{F} = \chi^u \\ 0, & \text{otherwise} \end{cases}$$



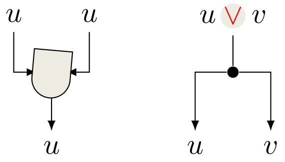
Ultrametric Integral Transition Matrices

Properties

- $A^{\mathsf{F}_2 \circ \mathsf{F}_1} = A^{\mathsf{F}_2} A^{\mathsf{F}_1}$
- $A^{\mathsf{F}_1 \| \mathsf{F}_2} = A^{\mathsf{F}_1} \otimes A^{\mathsf{F}_2}$
- If F is multiplicative, then

  $\mathsf{F}(x \wedge y) = \mathsf{F}(x) \wedge \mathsf{F}(y)$

$$A^{\mathsf{F}}_{v,u} = \begin{cases} 1, & \text{if } \mu^v \circ \mathsf{F} = \mu^u \\ 0, & \text{otherwise} \end{cases}$$



Dominant Trail Approximation

$$A^{\mathsf{F}_r \circ \cdots \circ \mathsf{F}_1} = A^{\mathsf{F}_r} \cdots A^{\mathsf{F}_1}$$

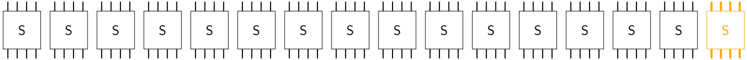
$$A^{\mathsf{F}_r \circ \cdots \circ \mathsf{F}_1}_{u_{r+1}, u_1} = \sum_{u \in \Lambda} \prod_{i=1}^{r} A^{\mathsf{F}_i}_{u_{i+1}, u_i} + \underbrace{\sum_{u \in \Omega \setminus \Lambda} \prod_{i=1}^{r} A^{\mathsf{F}_i}_{u_{i+1}, u_i}}_{|\cdot|_2 \approx 0} \equiv \sum_{u \in \Lambda} \prod_{i=1}^{r} A^{\mathsf{F}_i}_{u_{i+1}, u_i} \mod 2^{\nu}$$

Approximate zero-correlation

$$\left| \sum_{u \in \Omega \setminus \Lambda} \prod_{i=1}^{r} A^{\mathsf{F}_i}_{u_{i+1}, u_i} \right|_2 \leq \max_{u \in \Omega \setminus \Lambda} \left| \prod_{i=1}^{r} A^{\mathsf{F}_i}_{u_{i+1}, u_i} \right|_2 \leq 2^{-\nu}$$

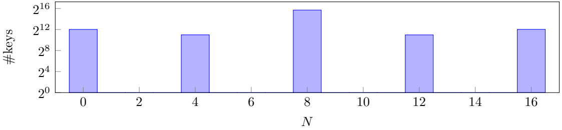
- Show that correlation is small for all non-dominant trails

Example



$$\left[\mathscr{U}\,\delta_X\right]_v = \begin{cases} 2^{\mathsf{wt}(u)-\mathsf{wt}(v)} & \text{if } v \preccurlyeq u\,, \\ 0 & \text{else}\,. \end{cases}$$

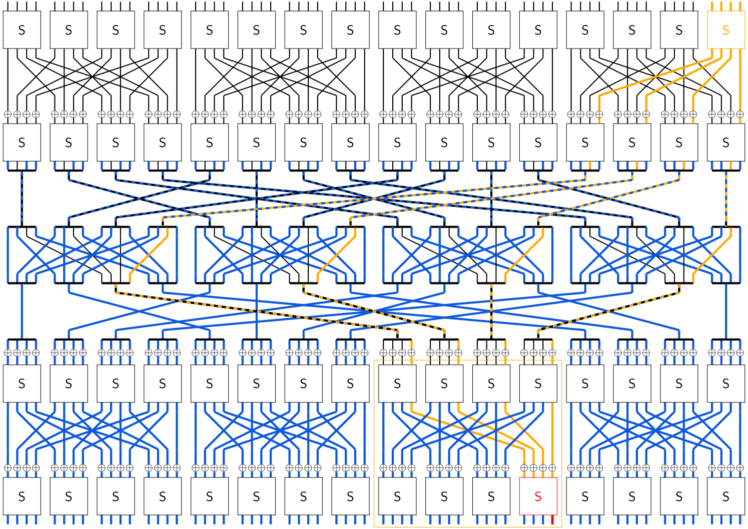
with $u = \mathtt{00\ldots01111}$



μ^w

with $w = \underbrace{\mathtt{0\ldots0}}_{\times 47}\,\mathtt{1}\,\underbrace{\mathtt{0\ldots0}}_{\times 16}$

Approximate Miss-in-the-Middle



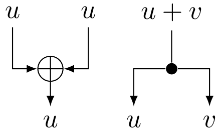
Automated Ultrametric Integral Cryptanalysis of PRESENT and SIMON

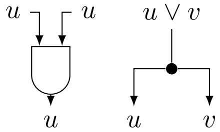
- SAT-based implementation
- Higher divisibility for properties from [Todo, 2015, Boura and Canteaut, 2016, Wang et al., 2019]

rounds	u	$\log_2(\text{data})$	ν_i for bit i 1	2	3	4
4	`000000000000000f`	4	3	2	2	2
5	`000000000000fff0`	12	5	5	5	5
6	`00000000ffffffff`	32	7	4	4	4
7	`fffffffffffff000`	52	9	5	5	5
8	`fffffffffffffffe`	63	8	5	5	5
9	`fffffffffffffffe`	63	2	1	1	1

- No improvements on minimal data properties [Todo and Morii, 2016, Xiang et al., 2016]
- Reduce data complexity in key-recovery attack

	Linear cryptanalysis	Ultrametric integral cryptanalysis
Field of definition	$\mathbb{Q}$ or $\mathbb{R}$ Archimedean ordinary absolute value $\lvert\cdot\rvert$	$\mathbb{Q}$ or $\mathbb{Q}_2$ non-Archimedean 2-adic absolute value $\lvert\cdot\rvert_2$
Geometric theory	'diagonalizes' additions $x \mapsto x + k$ additive characters χ^u Fourier transformation $\mathscr{F}$ $C^{\mathsf{F}} = \mathscr{F} T^{\mathsf{F}} \mathscr{F}^{-1}$	'diagonalizes' multiplications $x \mapsto x \wedge k$ multiplicative characters μ^u ultrametric integral change-of-basis $\mathscr{U}$ $A^{\mathsf{F}} = \mathscr{U} T^{\mathsf{F}} \mathscr{U}^{-1}$
Theory of trails	masks $u_1, u_2, \ldots$ correlation $\prod_{i=1}^{r} C^{\mathsf{F}_i}_{u_{i+1},u_i}$ linear functions linear diffusion, nonlinear confusion	exponents $u_1, u_2, \ldots$ correlation $\prod_{i=1}^{r} A^{\mathsf{F}_i}_{u_{i+1},u_i}$ multiplicative functions nonlinear diffusion, linear confusion





Beyne, T. and Verbauwhede, M. (2023).
Integral cryptanalysis using algebraic transition matrices.
IACR Trans. Symm. Cryptol., 2023(4):244–269.

Boura, C. and Canteaut, A. (2016).
Another view of the division property.
In Robshaw, M. and Katz, J., editors, *CRYPTO 2016, Part I*, volume 9814 of *LNCS*, pages 654–682. Springer, Berlin, Heidelberg.

Hu, K., Sun, S., Wang, M., and Wang, Q. (2020).
An algebraic formulation of the division property: Revisiting degree evaluations, cube attacks, and key-independent sums.
In Moriai, S. and Wang, H., editors, *ASIACRYPT 2020, Part I*, volume 12491 of *LNCS*, pages 446–476. Springer, Cham.

Knudsen, L. R. (1995).
Truncated and higher order differentials.
In Preneel, B., editor, *FSE'94*, volume 1008 of *LNCS*, pages 196–211. Springer, Berlin, Heidelberg.

Knudsen, L. R. and Wagner, D. (2002).
Integral cryptanalysis.
In Daemen, J. and Rijmen, V., editors, *FSE 2002*, volume 2365 of *LNCS*, pages 112–127. Springer, Berlin, Heidelberg.

Todo, Y. (2015).
Structural evaluation by generalized integral property.
In Oswald, E. and Fischlin, M., editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 287–314. Springer, Berlin, Heidelberg.

Todo, Y. and Morii, M. (2016).
Bit-based division property and application to simon family.
In Peyrin, T., editor, *FSE 2016*, volume 9783 of *LNCS*, pages 357–377. Springer, Berlin, Heidelberg.

Wang, S., Hu, B., Guan, J., Zhang, K., and Shi, T. (2019).
MILP-aided method of searching division property using three subsets and applications.
In Galbraith, S. D. and Moriai, S., editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 398–427. Springer, Cham.

Xiang, Z., Zhang, W., Bao, Z., and Lin, D. (2016).
Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers.
In Cheon, J. H. and Takagi, T., editors, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 648–678. Springer, Berlin, Heidelberg.