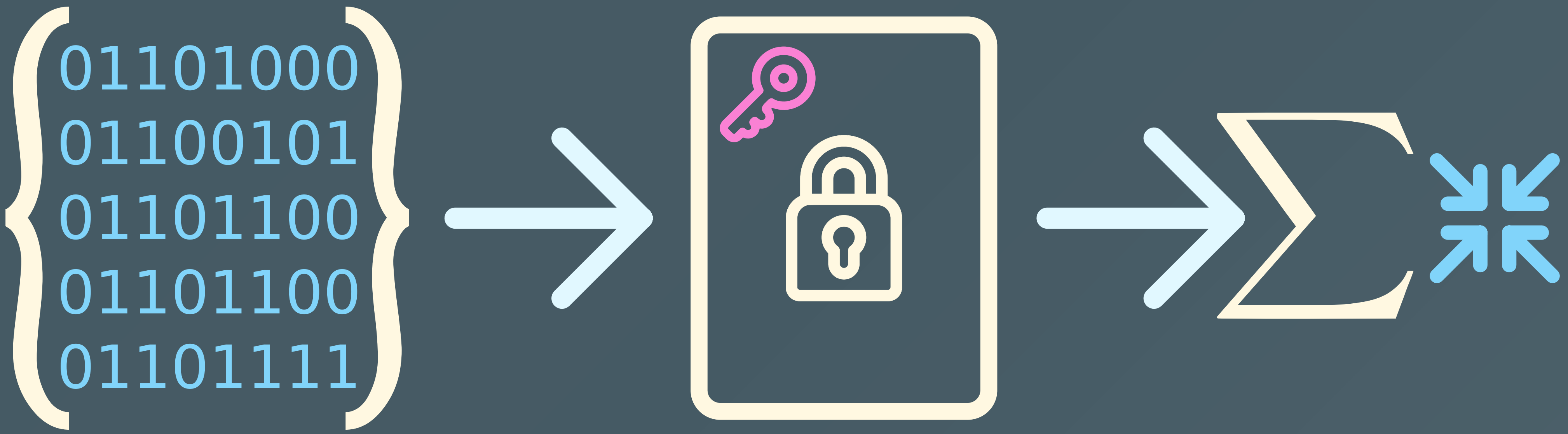
Integral Cryptanalysis Using Algebraic Transition Matrices

Tim Beyne and Michiel Verbauwhede

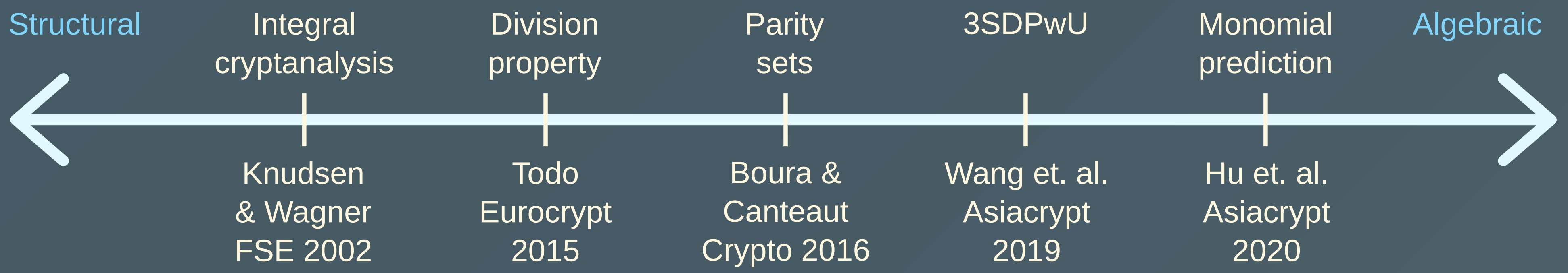
COSIC

KU LEUVEN

What's in a title: Integral Cryptanalysis



A Brief History of Integral Cryptanalysis

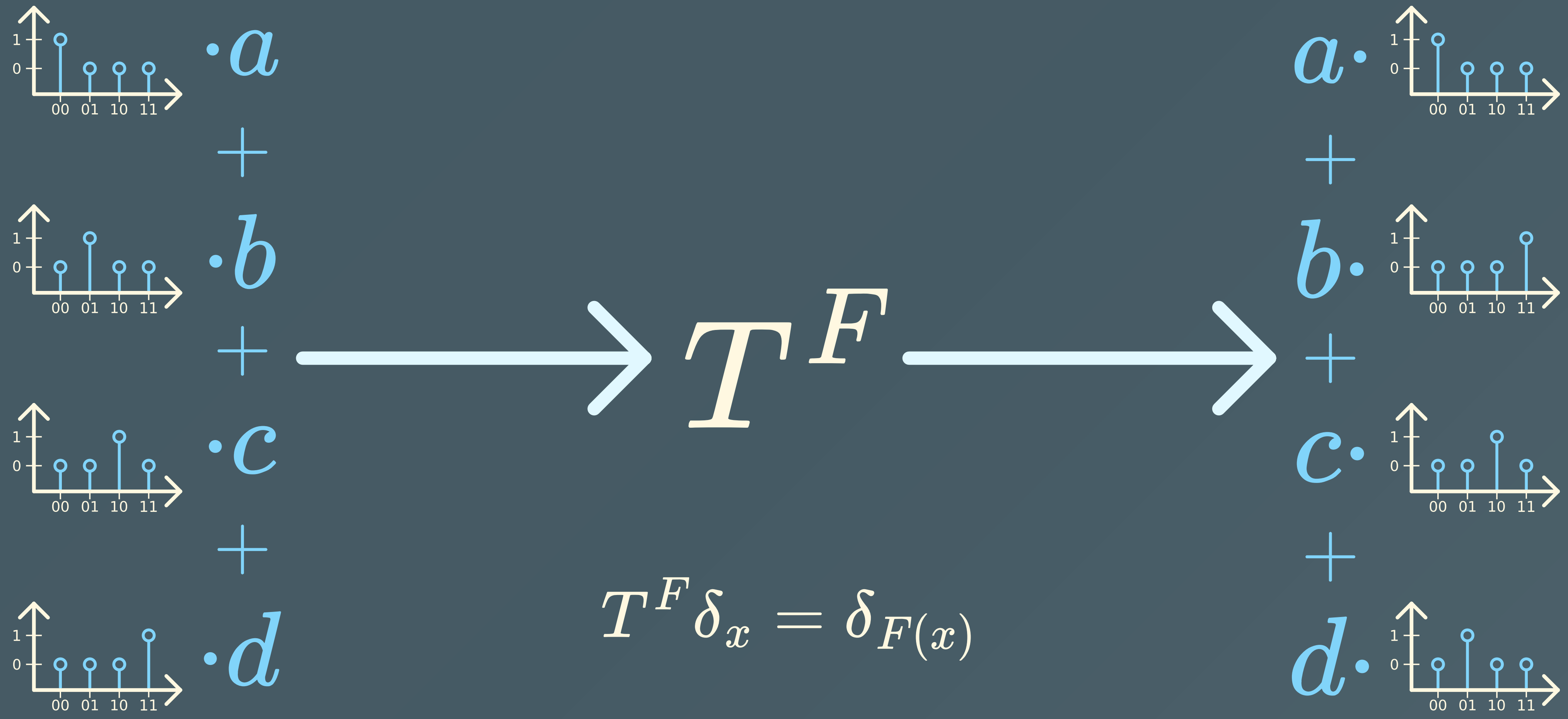


A Brief History of Integral Cryptanalysis

$$\{x \mid x \preccurlyeq u\} \qquad \sum_{x \preccurlyeq u} x^v = \delta_{u,v} \qquad \sum_{v \in \mathbf{F}_2^n} \lambda_v x^v$$

Structural	Integral cryptanalysis	Division property	Parity sets	3SDPwU	Monomial prediction	Algebraic
	Knudsen & Wagner FSE 2002	Todo Eurocrypt 2015	Boura & Canteaut Crypto 2016	Wang et. al. Asiacrypt 2019	Hu et. al. Asiacrypt 2020	

What's in a title: Transition Matrices



$$T^F \delta_x = \delta_{F(x)}$$

What's in a title: Transition Matrices

Linear	Differential	Integral
$\mathbb{F}_2^n \to \mathbb{R}$	$\mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{R}$	$\mathbb{F}_2^n \to \mathbb{F}_2$
$(-1)^{u^\intercal x}$	$(-1)^{u^\intercal x}\delta_a(y-x)$	?
C^F	D^F	A^F

What's in a title: Transition Matrices

Linear	Differential	Integral
$\mathbb{F}_2^n \to \mathbb{R}$	$\mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{R}$	$\mathbb{F}_2^n \to \mathbb{F}_2$
$(-1)^{u^\top x}$	$(-1)^{u^\top x}\delta_a(y-x)$	?
C^F	D^F	A^F

$$C^{F_r \circ \cdots \circ F_1}_{u_r, u_0} = \left(\prod_{i=1}^{r} C^{F_i}\right)_{u_r, u_0} = \underbrace{\sum_{u_1, \ldots, u_{r-1}}}_{\text{trails}} \underbrace{\prod_{i=1}^{r} C^{F_i}_{u_i, u_{i-1}}}_{\text{correlation}}$$

Algebraic Transition Matrices

$$\sum_{x \preccurlyeq u} x^v = \underbrace{\mathbf{1}_{\{x \preccurlyeq u\}}}_{\text{precursor}} \cdot \underbrace{x^v}_{\text{monomial}} = \delta_{u,v}$$

$$A^F = \mathscr{P}_m T^F \mathscr{P}_n^{-1}$$

$$\mathscr{P}_n = \mathscr{P}_n^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{\otimes n}$$

Algebraic Transition Matrices: An example

$$F(x) = (F_1(x), F_2(x)) = (x_2 + 1, x_1 + x_1 x_2)$$

$$\begin{array}{c} \\ 1 \\ F_1 \\ F_2 \\ F_1 F_2 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & x_1 & x_2 & x_1 x_2 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \end{array} = A^F$$

Algebraic Transition Matrices: An example

$$F^{\underline{0}}(x) = 1$$

$$\begin{array}{c c} & \begin{array}{cccc} 1 & x_1 & x_2 & x_1x_2 \end{array} \\ \begin{array}{c} 1 \\ F_1 \\ F_2 \\ F_1F_2 \end{array} & \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \end{array} = A^F$$

Algebraic Transition Matrices: An example

$$F_1(x) = x_2 + 1$$

$$\begin{array}{cc} & \begin{array}{cccc} 1 & x_1 & x_2 & x_1x_2 \end{array} \\ \begin{array}{c} 1 \\ F_1 \\ F_2 \\ F_1F_2 \end{array} & \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \end{array} = A^F$$

Algebraic Transition Matrices: An example

$$F_2(x) = x_1 + x_1 x_2$$

$$\begin{array}{c c} & \begin{array}{cccc} 1 & x_1 & x_2 & x_1x_2 \end{array} \\ \begin{array}{c} 1 \\ F_1 \\ F_2 \\ F_1F_2 \end{array} & \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \end{array} = A^F$$

Algebraic Transition Matrices: An example

$$F^1(x) = x_1 + x_1 x_2$$

$$\begin{array}{c c} & \begin{array}{cccc} 1 & x_1 & x_2 & x_1x_2 \end{array} \\ \begin{array}{c} 1 \\ F_1 \\ F_2 \\ F_1F_2 \end{array} & \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \end{array} = A^F$$

Algebraic Trails

$$A^{F_r \circ \cdots \circ F_1}_{u_r, u_0} = \left(\prod_{i=1}^{r} A^{F_i} \right)_{u_r, \underbrace{u_0}_{\text{exponent}}} = \underbrace{\sum_{u_1, \ldots, u_{r-1}}}_{\text{algebraic trail}} \underbrace{\prod_{i=1}^{r} A^{F_i}_{u_i, u_{i-1}}}_{\text{correlation}}$$

Algebraic Trails

$u_1 \in \operatorname{supp}\left(A^F \delta_{u_0}\right)$

$A^F_{u_4,u_3} = 1$

$$u_0 \ \boxed{R_1} \ u_1 \ \boxed{R_2} \ u_2 \ \boxed{R_3} \ u_3 \ \boxed{R_4} \ u_4$$

parity set propagation $\longrightarrow$

$\longleftarrow$ monomial trail

Key Addition

$$A^{\tau_k} = \bigotimes_i \begin{bmatrix} 1 & 0 \\ k_i & 1 \end{bmatrix}$$

$$A^{\tau_k}_{v,u} = \begin{cases} k^{u+v} & \text{if } u \preccurlyeq v\,, \\ 0 & \text{otherwise}\,. \end{cases}$$

$$A^{\tau_{k_2} \circ F \circ \tau_{k_1}}_{v,u} \neq 0 \implies A^{\tau_{k_2} \circ F \circ \tau_{k_1}}_{v' \succcurlyeq v, u' \preccurlyeq u} = f(k_1, k_2)$$

Finding Integral Properties

Simple properties

$$\sum_{x \preccurlyeq u} F^v(x) = A^F_{v,u}$$

1. Prove all trails from u to v have zero correlation.
2. Prove all trails from u to v are key-independent, then sum trails.
3. Sum trails from u to v per key-monomial.

Finding Integral Properties

Compound properties

$$\sum_{x \in X} r\left(F(x)\right) = \left(\mathscr{P}_m^{-\mathsf{T}} r\right) \cdot A^F \left(\mathscr{P}_n \mathbf{1}_X\right) = 0$$

Finding Integral Properties

Compound properties

$$\sum_{x \in X} r\left(F(x)\right) = r^\circ \cdot A^F \tilde{\mathbf{1}}_X = 0$$

$$= \operatorname{vec}\left(A^F\right) \cdot \underbrace{\left(\tilde{\mathbf{1}}_x \otimes r^\circ\right)}_{g}$$

$$\sum_{x \in \mathbb{F}_2^n} g(F(x), x) = 0$$

Finding Integral Properties

Compound properties

$$\sum_{x \in X} r\left(F(x)\right) = r^\circ \cdot A^F \tilde{\mathbf{1}}_X = 0$$

$$= \underbrace{\mathrm{vec}\left(A^F\right)} \cdot \underbrace{\left(\tilde{\mathbf{1}}_x \otimes r^\circ\right)}_{g}$$

$$\begin{array}{c} k_1 \\ \\ \\ k_n \end{array} \begin{bmatrix} \mathrm{vec}\left(A^{F_{k_1}}\right) \\ \vdots \\ \mathrm{vec}\left(A^{F_{k_n}}\right) \end{bmatrix} g = 0$$

$$\sum_{x \in \mathbb{F}_2^n} g(F(x), x) = 0$$

Finding Integral Properties

Compound properties

$$\sum_{x \in X} F^v(x) = A^F_{v,:} \cdot \tilde{\mathbf{1}}_X = A^{F_2}_{v,:} \cdot \qquad A^{F_1} \tilde{\mathbf{1}}_X \qquad = 0$$

Finding Integral Properties

Compound properties

$$\sum_{x \in X} F^v(x) = A^F_{v,:} \cdot \tilde{\mathbf{1}}_X = \underbrace{A^{F_2}_{v,:}}_{\text{oracle}} \cdot \underbrace{A^{F_1} \tilde{\mathbf{1}}_X}_{\text{exact computation}} = 0$$

$\operatorname{span}\left(\{\delta_x : x \in \operatorname{supp}(A^{F_2}_{v,:})\}\right) \subseteq P$

choose $V \subseteq \mathbb{F}_2^{\mathbb{F}_2^n}$

$$\ker \pi_P \circ A^{F_1} \circ i_V$$

Finding Integral Properties on 9-round PRESENT

- 9 rounds: 470 dimensional space of properties

$$\sum_{x_1=x_2=x_3=x_4=0} F_5(x) + F_{13}(x) = c_1$$

$$\sum_{x_5=0} F_5(x) + \sum_{x_9=0} F_{13}(x) = c_2$$

$$\sum_{x_5+x_9=0} F_1(x)F_{17}(x)F_{33}(x)F_{49}(x) = c_3$$

Duality

$$\sum_{x \preccurlyeq u} x^v = \underbrace{\mathbf{1}_{\{x \preccurlyeq u\}}}_{\text{precursor}} \cdot \underbrace{x^v}_{\text{monomial}} = \delta_{u,v}$$

$$E^F = \mathscr{M}_m T^F \mathscr{M}_n^{-1}$$

Duality

$$\sum_{x \preccurlyeq u} x^v = \underbrace{\mathbf{1}_{\{x \preccurlyeq u\}}}_{\text{precursor}} \cdot \underbrace{x^v}_{\text{monomial}} = \delta_{u,v}$$

$$E^F = \mathscr{M}_m T^F \mathscr{M}_n^{-1}$$

$$\begin{tikzcd}
A^F \arrow[r, "\mathsf{T}"] \arrow[d, "\mathscr{M}\mathscr{P}^{-1}"'] & E^{F^*} \arrow[d, "\mathscr{P}\mathscr{M}^{-1}"] \\
E^F \arrow[r, "\mathsf{T}"] & A^{F^*}
\end{tikzcd}$$

Conclusion

- Integral cryptanalysis fits in the geometric approach
  - New insight in and better understanding of integral cryptanalysis
  - Improved search methods

Future work

- Don't ignore the key
  - Weak key
  - Key schedule
- Build on/Improve search for generalized integral properties
  - Allow key in computation
  - Key-recovery by selection of useful properties from solution space

Coming Soon

- Ultrametric integral cryptanalysis
  - Justification of basis by simplification of multiplication
  - $\sum_{x \in X} r(F(x)) = 0 \mod 2^l$