A Geometric Approach to Linear Cryptanalysis

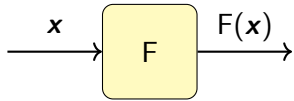
Tim Beyne

imec-COSIC, ESAT, KULeuven

December 6, 2021

COSIC

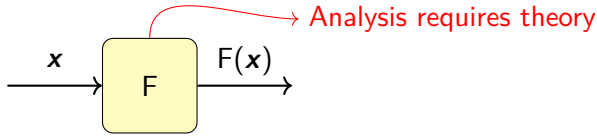
Linear cryptanalysis



$$C^{\mathsf{F}}_{v,u} = 2 \times \left(\Pr[u^\top \boldsymbol{x} = v^\top \mathsf{F}(\boldsymbol{x})] - \tfrac{1}{2}\right)$$

- Linear distinguisher: $1/(C^{\mathsf{F}}_{v,u})^2$ samples
- Variants/extensions:
  - Multiple- and multidimensional linear cryptanalysis
  - Zero-correlation linear cryptanalysis
  - Invariant subspaces and nonlinear invariants
  - I/O sums, partitioning, ... (nonlinear)

Linear cryptanalysis



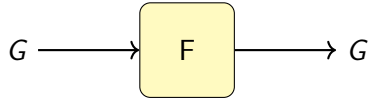
$$C^{\mathsf{F}}_{v,u} = 2 \times \left(\Pr[u^\top \boldsymbol{x} = v^\top \mathsf{F}(\boldsymbol{x})] - \tfrac{1}{2}\right)$$

- Linear distinguisher: $1/(C^{\mathsf{F}}_{v,u})^2$ samples
- Variants/extensions:
  - Multiple- and multidimensional linear cryptanalysis
  - Zero-correlation linear cryptanalysis
  - Invariant subspaces and nonlinear invariants
  - I/O sums, partitioning, ... (nonlinear)

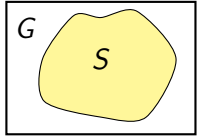
Goals

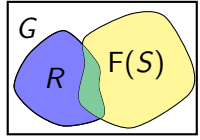
1. Uniform description of different variants of linear cyptanalysis
2. Generalization of approximations and the links between them
3. Alternative motivation for trails and the general piling-up principle

Input and output properties



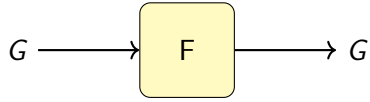
Subset $S \subseteq G$



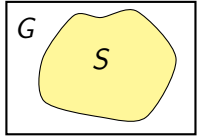


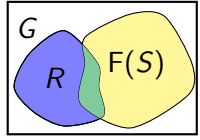
Count values in $R \cap \mathrm{F}(S) \subseteq G$

Input and output properties



Subset $S \subseteq G$





Count values in $R \cap \mathsf{F}(S) \subseteq G$

$\mathbb{1}_S : G \to \mathbb{C}$ $(\mathbb{1}_S \in \mathbb{C}^G)$

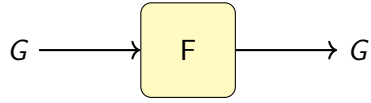
$$\mathbb{1}_S(x) = \begin{cases} 1 \text{ if } x \in S \\ 0 \text{ else} \end{cases}$$

$\mathbb{1}^*_R : \mathbb{C}^G \to \mathbb{C}$ $(\mathbb{1}_R \in \mathbb{C}^{G^*})$

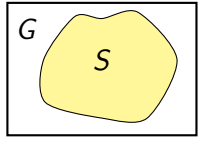
$\mathbb{1}^*_R(f) = \sum_{x \in R} f(x) = \langle \mathbb{1}_R,\, f \rangle$

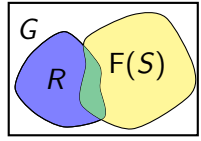
$\mathbb{1}^*_R(\mathbb{1}_{\mathsf{F}(S)}) = |R \cap \mathsf{F}(S)|$

Input and output properties



Subset $S \subseteq G$





Count values in $R \cap \mathsf{F}(S) \subseteq G$

$\mathbb{1}_S : G \to \mathbb{C}$ $(\mathbb{1}_S \in \mathbb{C}^G)$

$$\mathbb{1}_S(x) = \begin{cases} 1 \text{ if } x \in S \\ 0 \text{ else} \end{cases}$$

$\mathbb{1}^*_R : \mathbb{C}^G \to \mathbb{C}$ $(\mathbb{1}_R \in \mathbb{C}^{G^*})$

$\mathbb{1}^*_R(f) = \sum_{x \in R} f(x) = \langle \mathbb{1}_R,\, f \rangle$

$\mathbb{1}^*_R(\mathbb{1}_{\mathsf{F}(S)}) = |R \cap \mathsf{F}(S)|$

State

function

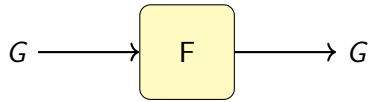
$f \in \mathbb{C}^G$

'Observation' of state

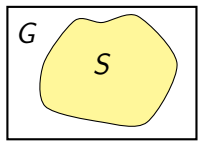
linear functional

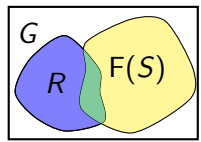
$g^* \in \mathbb{C}^{G^*}$

Input and output properties



Subset $S \subseteq G$





Count values in $R \cap \mathrm{F}(S) \subseteq G$

$\mathbb{1}_S : G \to \mathbb{C}$ $(\mathbb{1}_S \in \mathbb{C}^G)$

$$\mathbb{1}_S(x) = \begin{cases} 1 \text{ if } x \in S \\ 0 \text{ else} \end{cases}$$

$\mathbb{1}^*_R : \mathbb{C}^G \to \mathbb{C}$ $(\mathbb{1}_R \in \mathbb{C}^{G^*})$

$\mathbb{1}^*_R(f) = \sum_{x \in R} f(x) = \langle \mathbb{1}_R,\, f \rangle$

$\mathbb{1}^*_R(\mathbb{1}_{\mathrm{F}(S)}) = |R \cap \mathrm{F}(S)|$

State

function

$f \in \mathbb{C}^G$

'Observation' of state

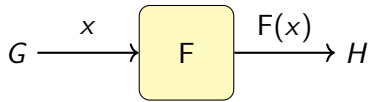
linear functional

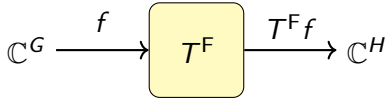
$g^* \in \mathbb{C}^{G^*} \cong \mathbb{C}^G$

$g^*(f) = \langle g, f \rangle$

Input and output properties

Transition matrices



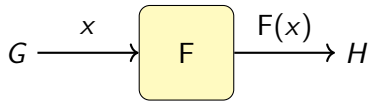


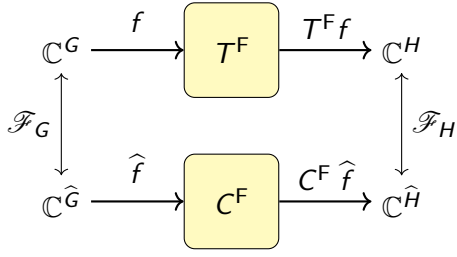
Operator T^F: $T^F \delta_x = \delta_{F(x)}$

with $\delta_x(z) = \begin{cases} 1 \text{ if } z = x \\ 0 \text{ else} \end{cases}$

Input and output properties

Transition matrices and correlation matrices





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

with $\delta_x(z) = \begin{cases} 1 \text{ if } z = x \\ 0 \text{ else} \end{cases}$

Fourier transformation: $\mathscr{F}_G : \mathbb{C}^G \to \mathbb{C}^{\widehat{G}}$

$\mathscr{F}_G \chi = |G|\, \delta_\chi$

Diagonalizes translations ($\mathsf{F}(x) = x + t$).

Group character χ

Homomorphism $\chi : G \to \mathbb{C} \setminus \{0\}$

$\chi(x + y) = \chi(x)\chi(y)$

Input and output properties

Higher-dimensional properties

- Generalization: subspace $V \subseteq \mathbb{C}^G$ as input (output) property
- Consider all states (observation functions) $f \in V$ at once
- Common examples:
  - Multiple linear cryptanalysis
  - Projection functions

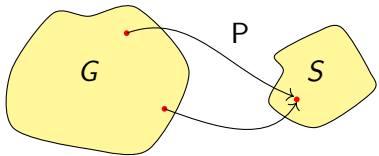
! Independence from the choice of basis for V

Input and output properties

Example: projection functions

- Projection function framework [Wagner, 2004, Baignères et al., 2004]

- Distinguisher based on a function $\mathrm{P} : G \to S$ of the input (similar for output)

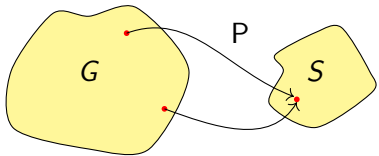


$$\longleftrightarrow V = \{f \circ \mathrm{P} \mid f \in \mathbb{C}^S\}$$

Input and output properties

Example: projection functions

- Projection function framework [Wagner, 2004, Baignères et al., 2004]
- Distinguisher based on a function $\mathrm{P} : G \to S$ of the input (similar for output)



$$\longleftrightarrow V = \{f \circ \mathrm{P} \mid f \in \mathbb{C}^S\}$$

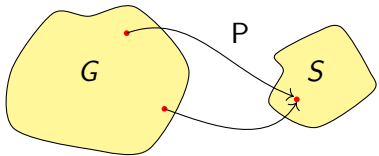
- Linear cryptanalysis: $G = \mathbb{F}_2^n$, $S = \mathbb{F}_2$ and $\mathrm{P}(x) = u^\top x$

$$V = \mathrm{span}\{\delta_0 \circ \mathrm{P}, \delta_1 \circ \mathrm{P}\} = \mathrm{span}\{\chi_0, \chi_u\} \quad \text{with } \chi_w(x) = (-1)^{w^\top x}$$

Input and output properties

Example: projection functions

- Projection function framework [Wagner, 2004, Baignères et al., 2004]
- Distinguisher based on a function $\mathrm{P} : G \to S$ of the input (similar for output)



$$\longleftrightarrow V = \{f \circ \mathrm{P} \mid f \in \mathbb{C}^S\}$$

- Linear cryptanalysis: $G = \mathbb{F}_2^n$, $S = \mathbb{F}_2$ and $\mathrm{P}(x) = u^\top x$

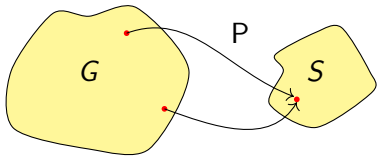
$$V = \mathrm{span}\{\delta_0 \circ \mathrm{P}, \delta_1 \circ \mathrm{P}\} = \mathrm{span}\{\chi_0, \chi_u\} \quad \text{with } \chi_w(x) = (-1)^{w^\top x}$$

Subspace $\mathrm{span}\{\chi_u\}$
(equivalent for permutations)

Input and output properties

Example: projection functions

- Projection function framework [Wagner, 2004, Baignères et al., 2004]
- Distinguisher based on a function $\mathrm{P} : G \to S$ of the input (similar for output)



$$\longleftrightarrow V = \{f \circ \mathrm{P} \mid f \in \mathbb{C}^S\}$$

- Linear cryptanalysis: $G = \mathbb{F}_2^n$, $S = \mathbb{F}_2$ and $\mathrm{P}(x) = u^\top x$

$$V = \mathrm{span}\{\delta_0 \circ \mathrm{P}, \delta_1 \circ \mathrm{P}\} = \mathrm{span}\{\chi_0, \chi_u\} \quad \text{with } \chi_w(x) = (-1)^{w^\top x}$$

Subspace $\mathrm{span}\{\chi_u\}$
(equivalent for permutations)

- Multidimensional linear cryptanalysis
- ! *Not* for multiple linear cryptanalysis

Goals

1. Uniform description of different variants of linear cyptanalysis
   vector spaces of functions $G \to \mathbb{C}$ (subspaces of $\mathbb{C}^G$)

2. Generalization of approximations and the links between them

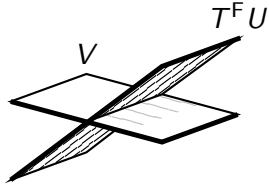
3. Alternative motivation for trails and the general piling-up principle

Approximations

- Pair of subspaces $U \subseteq \mathbb{C}^G$, $V \subseteq \mathbb{C}^H$ with 'approximation map' $\langle V, U\rangle_{\mathsf{F}} : U \to V$

$$\langle V, U\rangle_{\mathsf{F}} := \pi_V \circ T^{\mathsf{F}} \circ \iota_U = \pi_{\mathscr{F}(V)} \circ C^{\mathsf{F}} \circ \iota_{\mathscr{F}(U)}$$

- *Principal correlations*: $\min\{\dim U, \dim V\}$-largest singular values of $\langle V, U\rangle_{\mathsf{F}}$



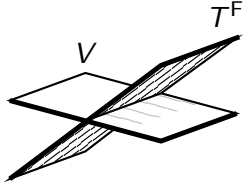
Cosines of principal angles (F injective)

Approximations

- Pair of subspaces $U \subseteq \mathbb{C}^G$, $V \subseteq \mathbb{C}^H$ with 'approximation map' $\langle V, U\rangle_{\mathsf{F}} : U \to V$

$$\langle V, U\rangle_{\mathsf{F}} := \pi_V \circ T^{\mathsf{F}} \circ \iota_U = \pi_{\mathscr{F}(V)} \circ C^{\mathsf{F}} \circ \iota_{\mathscr{F}(U)}$$

- *Principal correlations*: $\min\{\dim U, \dim V\}$-largest singular values of $\langle V, U\rangle_{\mathsf{F}}$



Cosines of principal angles (F injective)

- Linear cryptanalysis: $U = \operatorname{span}\{\chi_0, \chi_u\}$ and $V = \operatorname{span}\{\chi_0, \chi_v\}$, F permutation with $\chi_w(x) = (-1)^{w^\top x}$ for $w \in \mathbb{F}_2^n$

$$\langle V, U\rangle_{\mathsf{F}} = \frac{1}{2^n} \begin{pmatrix} \langle \chi_0, T^{\mathsf{F}}\chi_0\rangle & \langle \chi_0, T^{\mathsf{F}}\chi_u\rangle \\ \langle \chi_v, T^{\mathsf{F}}\chi_0\rangle & \langle \chi_v, T^{\mathsf{F}}\chi_u\rangle \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}$$

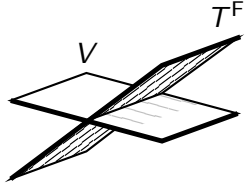
Singular values $\sigma_1 = 1$ and $\sigma_2 = |c|$

Approximations

- Pair of subspaces $U \subseteq \mathbb{C}^G$, $V \subseteq \mathbb{C}^H$ with 'approximation map' $\langle V, U\rangle_{\mathsf{F}} : U \to V$

$$\langle V, U\rangle_{\mathsf{F}} := \pi_V \circ T^{\mathsf{F}} \circ \iota_U = \pi_{\mathscr{F}(V)} \circ C^{\mathsf{F}} \circ \iota_{\mathscr{F}(U)}$$

- *Principal correlations*: $\min\{\dim U, \dim V\}$-largest singular values of $\langle V, U\rangle_{\mathsf{F}}$



Cosines of principal angles (F injective)

- Linear cryptanalysis: $U = \operatorname{span}\{\chi_0, \chi_u\}$ and $V = \operatorname{span}\{\chi_0, \chi_v\}$, F permutation with $\chi_w(x) = (-1)^{w^\top x}$ for $w \in \mathbb{F}_2^n$

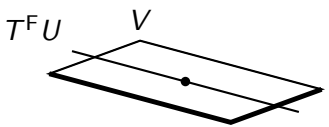
$$\langle V, U\rangle_{\mathsf{F}} = \frac{1}{2^n}\begin{pmatrix} \langle \chi_0, T^{\mathsf{F}}\chi_0\rangle & \langle \chi_0, T^{\mathsf{F}}\chi_u\rangle \\ \langle \chi_v, T^{\mathsf{F}}\chi_0\rangle & \langle \chi_v, T^{\mathsf{F}}\chi_u\rangle \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}$$

Correlation of linear approximation

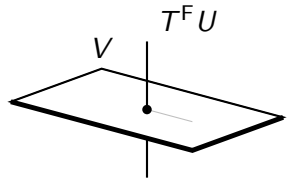
Singular values $\sigma_1 = 1$ and $\sigma_2 = |c|$

Approximations

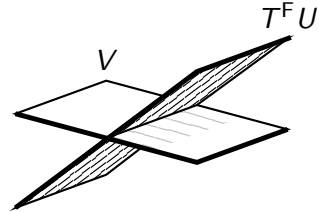
Perfect



Zero-correlation



General



Approximations

Perfect approximations and invariants

- $T^{\mathsf{F}} U \subseteq V$
  If F is a permutation: all principal correlations equal to one

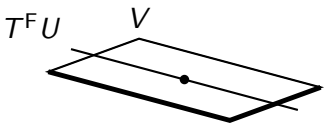
- Invariants: $V = U$

  - T^{F} (equivalently C^{F}) is diagonalizable

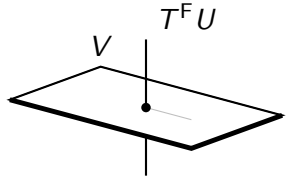
  - So $V = \text{span}\{v_1, \ldots, v_d\}$ with v_i eigenvectors of T^{F}
    $\mathscr{F}(V) = \text{span}\{\widehat{v}_1, \ldots, \widehat{v}_d\}$ with $\widehat{v}_i$ eigenvectors of C^{F} [Beyne, 2018]

Approximations

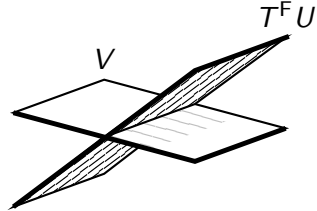
Perfect



Zero-correlation



General



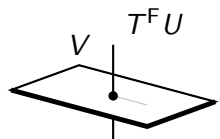
$$T^F U \subseteq V$$

- Integral attacks
- Invariant subspaces
- Nonlinear invariants

Approximations

Zero-correlation approximations

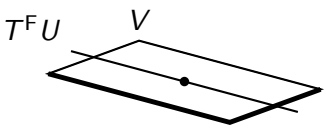
- $T^{\mathsf{F}} U \perp V \iff$ All principal correlations are equal to zero
- (U, V) is a zero-correlation approximation iff $(U, V^{\perp})$ is a perfect approximation

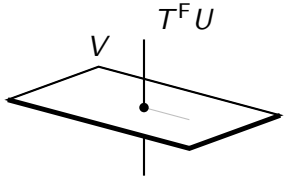


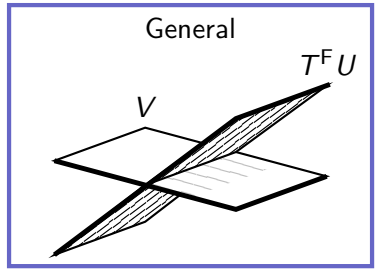
Approximations

Theorem 4.2

Perfect ⇄ Zero-correlation







$T^F U \subseteq V$

- Integral attacks
- Invariant subspaces
- Nonlinear invariants

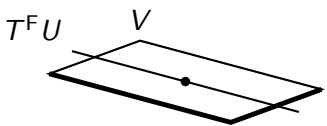
$T^F U \perp V$

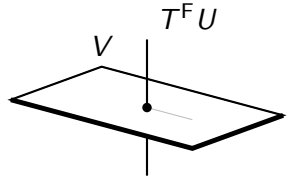
- Zero-correlation linear approximations
- Multidimensional $\sim$

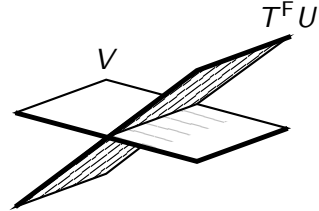
Approximations

Perfect ⟷ Zero-correlation (Theorem 4.2)

General







$T^{\mathsf{F}}U \subseteq V$

- Integral attacks
- Invariant subspaces
- Nonlinear invariants

$T^{\mathsf{F}}U \perp V$

- Zero-correlation linear approximations
- Multidimensional $\sim$

$\langle V, U \rangle_{\mathsf{F}}$

- (Non)linear approximations
- Multiple $\sim$
- Multidimensional $\sim$
- Partitioning

Goals

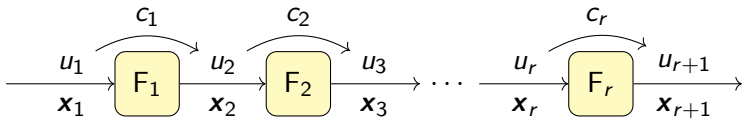
1. Uniform description of different variants of linear cyptanalysis
   vector spaces of functions $G \to \mathbb{C}$ (subspaces of $\mathbb{C}^G$)

2. Generalization of approximations and the links between them
   pairs of subspaces $U \subseteq \mathbb{C}^G$, $V \subseteq \mathbb{C}^H$ with approximation map $\langle V, U \rangle_{\mathsf{F}} : U \to V$

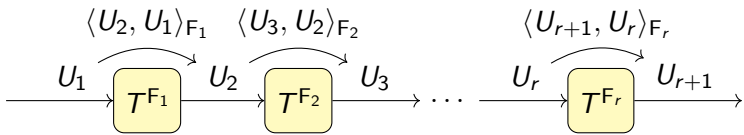
3. Alternative motivation for trails and the general piling-up principle

Trails

Correlation $c = 2\Pr[u_1^\top \boldsymbol{x}_1 + u_{r+1}^\top \boldsymbol{x}_{r+1} = 0] - 1$?

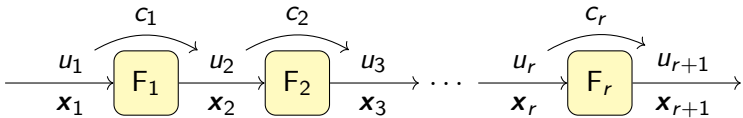


Approximation map $\langle U_{r+1}, U_1 \rangle_{\mathsf{F}_r \circ \cdots \circ \mathsf{F}_1}$?



Trails

Traditional piling-up principle



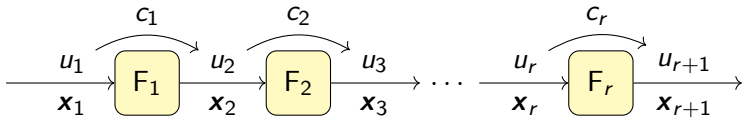
- Piling up principle:

$$u_1^\top x_1 + u_{r+1}^\top x_{r+1} = \sum_{i=1}^{r} \underbrace{u_i^\top x_i + u_{i+1}^\top x_{i+1}}_{z_i}$$

- 'Independent' z_i, $i = 1, \ldots, r$: $c \approx \prod_{i=1}^{r} c_i$ (correlation of trail)

Trails

Traditional piling-up principle



- Piling up principle:

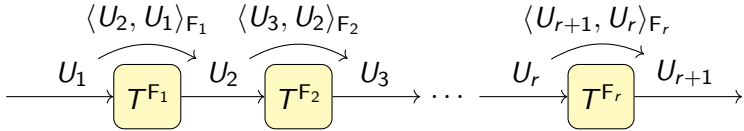
$$u_1^\top x_1 + u_{r+1}^\top x_{r+1} = \sum_{i=1}^{r} \underbrace{u_i^\top x_i + u_{i+1}^\top x_{i+1}}_{z_i}$$

- 'Independent' z_i, $i = 1, \ldots, r$: $c \approx \prod_{i=1}^{r} c_i$ (correlation of trail)

- Motivation:
  - Markov cipher assumption (equivalent to averaging over independent round keys)
    ❶ *Requires taking into account round key masks*
  - Dominant trail hypothesis (follows from [Daemen et al., 1995])

Trails

General piling-up principle



- Piling-up principle:

$$\langle U_{r+1}, U_1\rangle_{\mathsf{F}_r\circ\cdots\circ\mathsf{F}_1} = \langle U_{r+1}, U_r\rangle_{\mathsf{F}_r} \circ \cdots \circ \langle U_3, U_2\rangle_{\mathsf{F}_2} \circ \langle U_2, U_1\rangle_{\mathsf{F}_1} + E$$

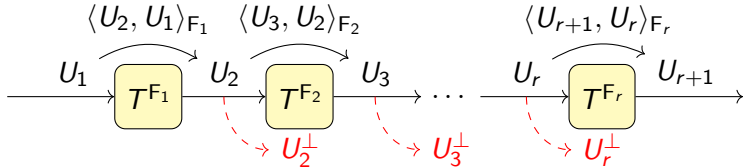
  (see Theorem 5.1 for error term E)

- Recall that $\langle U_{i+1}, U_i\rangle_{\mathsf{F}_i} = \pi_{U_{i+1}} \circ T^{\mathsf{F}_i} \circ \iota_{U_i}$

- Geometric motivation: successive orthogonal projection

Trails

General piling-up principle



- Piling-up principle:

$$\langle U_{r+1}, U_1\rangle_{\mathsf{F}_r\circ\cdots\circ\mathsf{F}_1} = \langle U_{r+1}, U_r\rangle_{\mathsf{F}_r} \circ \cdots \circ \langle U_3, U_2\rangle_{\mathsf{F}_2} \circ \langle U_2, U_1\rangle_{\mathsf{F}_1} + E$$

  (see Theorem 5.1 for error term E)

- Recall that $\langle U_{i+1}, U_i\rangle_{\mathsf{F}_i} = \pi_{U_{i+1}} \circ T^{\mathsf{F}_i} \circ \iota_{U_i}$

- Geometric motivation: successive orthogonal projection

Conclusion

1. Uniform description of different variants of linear cyptanalysis
   vector spaces of functions $G \to \mathbb{C}$ (subspaces of $\mathbb{C}^G$)
2. Generalization of approximations and the links between them
   pairs of subspaces $U \subseteq \mathbb{C}^G$, $V \subseteq \mathbb{C}^H$ with approximation map $\langle V, U \rangle_{\mathsf{F}} : U \to V$
3. Alternative motivation for trails and the general piling-up principle
   process of successive orthogonal projection

- More results and applications in the paper

https://homes.esat.kuleuven.be/~tbeyne/
tim.beyne@esat.kuleuven.be

References I


Baignères, T., Junod, P., and Vaudenay, S. (2004).
How far can we go beyond linear cryptanalysis?
In Lee, P. J., editor, *ASIACRYPT 2004*, volume 3329 of *LNCS*, pages 432–450, Jeju Island, Korea. Springer, Heidelberg, Germany.


Beyne, T. (2018).
Block cipher invariants as eigenvectors of correlation matrices.
In Peyrin, T. and Galbraith, S., editors, *ASIACRYPT 2018, Part I*, volume 11272 of *LNCS*, pages 3–31, Brisbane, Queensland, Australia. Springer, Heidelberg, Germany.


Daemen, J., Govaerts, R., and Vandewalle, J. (1995).
Correlation matrices.
In Preneel, B., editor, *FSE'94*, volume 1008 of *LNCS*, pages 275–285, Leuven, Belgium. Springer, Heidelberg, Germany.

References II

Wagner, D. (2004).
Towards a unifying view of block cipher cryptanalysis.
In Roy, B. K. and Meier, W., editors, *FSE 2004*, volume 3017 of *LNCS*, pages 16–33, New Delhi, India. Springer, Heidelberg, Germany.