A Geometric Approach to Linear Cryptanalysis

Tim Beyne

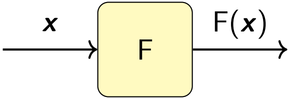
imec-COSIC, ESAT, KULeuven

December 6, 2021

KU LEUVEN

COSIC

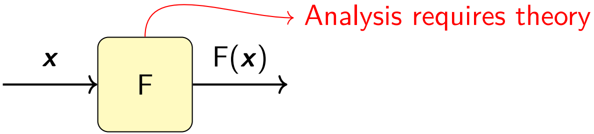
Linear cryptanalysis



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

- 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

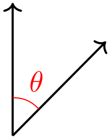
Inner product space $\mathbb{C}^G$

- $\mathbb{C}^G$ = vector space of all functions $G \to \mathbb{C}$ with $G = \{g_1, \ldots, g_l\}$

$$\begin{array}{ccc} \mathbb{C}^G & \cong & \mathbb{C}^{|G|} \\ f & \mapsto & \begin{bmatrix} f(g_1) \\ \vdots \\ f(g_l) \end{bmatrix} \end{array}$$

- Inner product between $f, g \in \mathbb{C}^G$:

$$\langle f, g \rangle = \sum_{x \in G} \overline{f(x)} g(x)$$

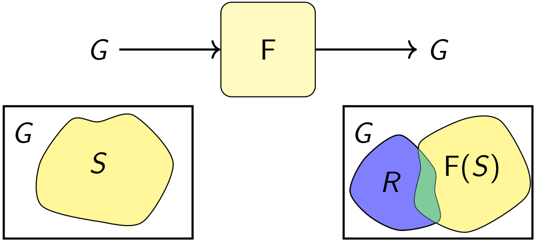


$|\langle f, g \rangle| = \cos \theta$

- Orthogonality: $f \perp g \Leftrightarrow \langle f, g \rangle = 0$

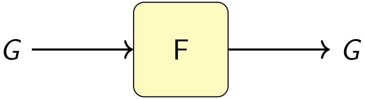
Input and output properties

Subset $S \subseteq G$

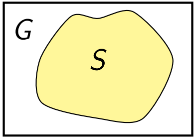


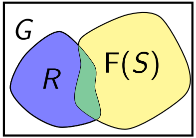
Count values in
$R \cap \mathsf{F}(S) \subseteq G$

Input and output properties



Subset $S \subseteq G$





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

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

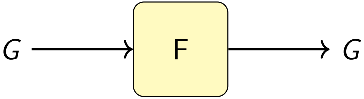
$$\mathbb{1}_S(x) = \begin{cases} 1 \text{ if } x \in S \\ 0 \text{ else} \end{cases}$$

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

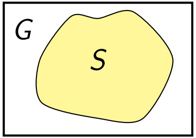
$$\mathbb{1}_R^*(f) = \sum_{x \in R} f(x) = \langle \mathbb{1}_R, f \rangle$$

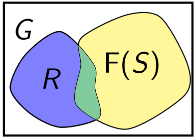
$$\mathbb{1}_R^*(\mathbb{1}_{\mathsf{F}(S)}) = |R \cap \mathsf{F}(S)|$$

Input and output properties



Subset $S \subseteq G$





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

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

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

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

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

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

State

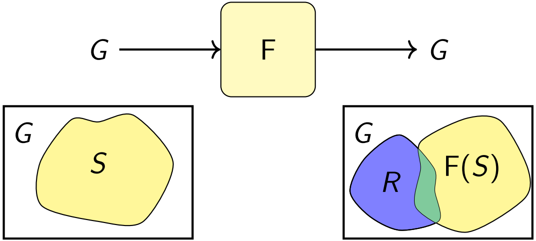
function
$f \in \mathbb{C}^G$

'Observation' of state

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

Input and output properties

Subset $S \subseteq G$



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

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

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

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

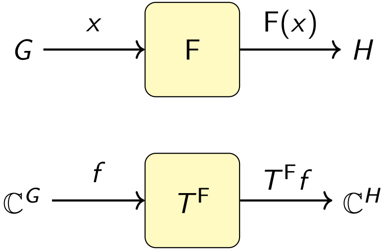
$$\mathbb{1}_R^*(f) = \textstyle\sum_{x \in R} f(x) = \langle \mathbb{1}_R, f \rangle$$

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

State	‘Observation’ of state
function	linear functional
$f \in \mathbb{C}^G$	$g^* \in \mathbb{C}^{G^*} \cong \mathbb{C}^G$
	$g^*(f) = \langle g, f \rangle$

Input and output properties

Transition matrices

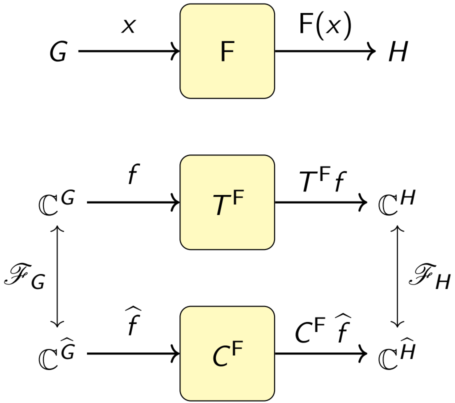


Transformation T^{F}: $T^{\mathsf{F}} \delta_x = \delta_{\mathsf{F}(x)}$

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

Input and output properties

Transition matrices and correlation matrices



Transformation 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 [Wagner, 2004, Baignères et al., 2004]

! Independence from the choice of basis for V

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

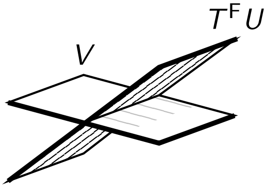
3. Alternative motivation for trails and the general piling-up principle

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



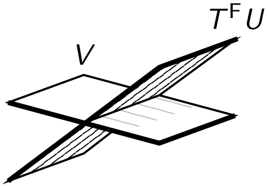
Cosines of principal angles (F injective)

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



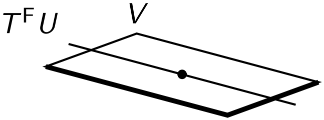
Cosines of principal angles (F injective)

- Linear cryptanalysis ($\dim U = \dim V = 1$):
  principal correlation coincides with absolute value of ordinary correlation

Approximations

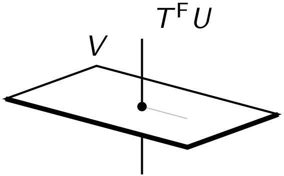
Perfect ⇄ Zero-correlation (Theorem 4.2)

General



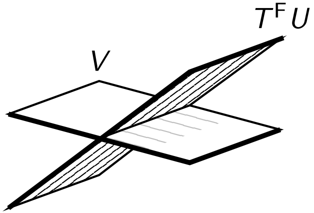
$$T^{\mathsf{F}} U \subseteq V$$

- Integral attacks
- Invariant subspaces
- Nonlinear invariants



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

- Zero-correlation linear approximations
- Multidimensional ∼



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

- (Non)linear approximations
- Multiple ∼
- Multidimensional ∼
- Partitioning

Goals

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

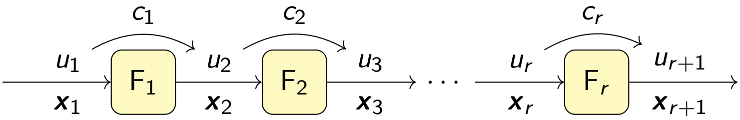
2. Generalization of approximations and the links between them
   pairs of subspaces $U \subseteq \mathbb{C}^G$, $V \subseteq \mathbb{C}^H$ with approximation map $\langle V, U \rangle_{\mathsf{F}} : U \to V$

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

Trails*

Traditional piling-up principle

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



- Piling-up principle: $c \approx \prod_{i=1}^{r} c_i$ (correlation of trail)

- Motivation:

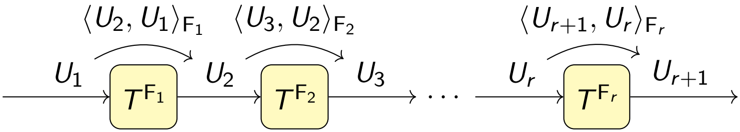
  - Markov cipher assumption (equivalent to averaging over independent round keys)
    ℹ *Requires taking into account round key masks*

  - Dominant trail hypothesis (follows from [Daemen et al., 1995])

Trails*

General piling-up principle

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



- 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)

- 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/geometric`

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.

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.

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.