Linear and differential cryptanalysis

Tim Beyne

tim@cryptanalysis.info

KU Leuven

March 11, 2025

Motivation

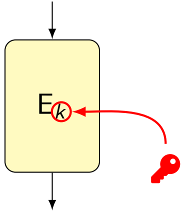
- Symmetric-key cryptography: encryption, authentication, hashing, ...
- You want to design symmetric-key cryptography
- You want to break symmetric-key cryptography

Symmetric-key primitives are not based on reductions to ‘difficult’ problems

Cryptanalysis is how we understand their design and security

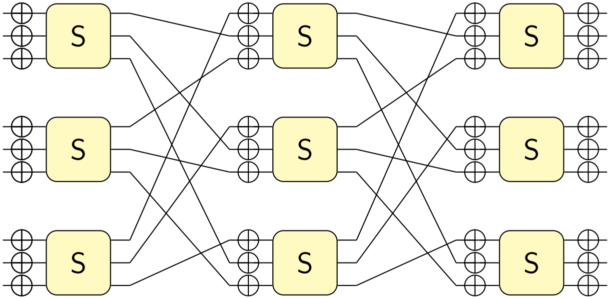
Primitives

Block ciphers, tweakable block ciphers, permutations, ...



Primitives

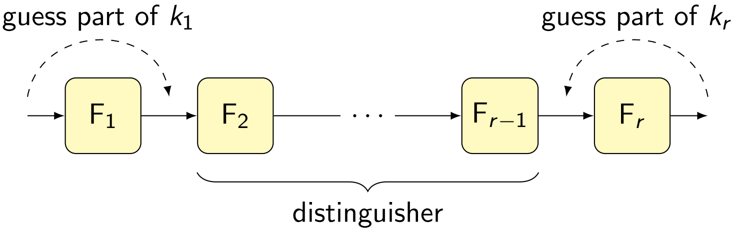
Example



Cryptanalysis

- Different goals depending on the application

- Key recovery



- Combinatorial property ('distinguisher') is used to filter out wrong key guesses

- There are several other ways to use these properties

Cryptanalysis

- Several systematic techniques have been developed since 1980s
- Most important examples:
  - Linear cryptanalysis
  - Differential cryptanalysis
  - Integral cryptanalysis
- Each of these is quite broad

Overview

- Linear cryptanalysis
  - Lecture 9:00-10:30
  - Exercises 11:00-12:30
- Differential cryptanalysis
  - Lecture 14:30-16:00
  - Exercises 16:30-18:00

https://tim.cryptanalysis.info/spring-school/

Linear cryptanalysis

based on

T. Beyne, V. Rijmen. *Linear Cryptanalysis*. Cambridge University Press. (Winter 2025)

Overview

- Linear approximations
- Correlation matrices
- Linear trails
- Cost analysis
- Key-recovery techniques
- Exercises

Linear approximations

- Function $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$, e.g. a block cipher
- Probabilistic linear relation between x and $y = \mathsf{F}(x)$

$$\underbrace{\sum_{i=1}^{m} v_i\, y_i}_{v^\mathsf{T} y} \approx \underbrace{\sum_{i=1}^{n} u_i\, x_i}_{u^\mathsf{T} x}$$

- Short notation $v^\mathsf{T} y \approx u^\mathsf{T} x$
- Pair (u, v) of masks $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$ determines the linear approximation

Linear approximations
Correlation

- If x and $\mathsf{F}(x)$ are 'unrelated', the number of x such that $v^\top \mathsf{F}(x) = u^\top x$ is $2^n/2$
- Correlation
$$c = 2 \times \left(\frac{\#\{x \in \mathbb{F}_2^n \mid v^\top \mathsf{F}(x) = u^\top x\}}{2^n} - \frac{1}{2} \right)$$
- Equivalent expression using probabilities ($\boldsymbol{x}$ uniform random on $\mathbb{F}_2^n$)
$$c = 2 \Pr_{\boldsymbol{x}} \left[v^\top \mathsf{F}(\boldsymbol{x}) = u^\top \boldsymbol{x} \right] - 1$$

Beware of probabilistic arguments

Linear approximations
Correlation

- Technical result: if $\boldsymbol{r}$ is a random variable on $\mathbb{F}_2$, then

$$2 \Pr_{\boldsymbol{r}}[\boldsymbol{r} = 0] - 1 = \Pr_{\boldsymbol{r}}[\boldsymbol{r} = 0] - \Pr_{\boldsymbol{r}}[\boldsymbol{r} = 1] = \mathsf{E}_{\boldsymbol{r}}\left[(-1)^{\boldsymbol{r}}\right]$$

- Applied to $\boldsymbol{r} = v^{\mathsf{T}}\mathsf{F}(\boldsymbol{x}) + u^{\mathsf{T}}\boldsymbol{x}$, this gives

$$c = 2 \Pr_{\boldsymbol{x}}\left[v^{\mathsf{T}}\mathsf{F}(\boldsymbol{x}) = u^{\mathsf{T}}\boldsymbol{x}\right] - 1 = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{v^{\mathsf{T}}\mathsf{F}(x) + u^{\mathsf{T}}x}$$

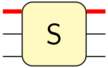
Linear approximations

Example

- 3-bit S-box $S\colon \mathbb{F}_2^3 \to \mathbb{F}_2^3$

x	000	001	010	011	100	101	110	111
$S(x)$	111	010	100	101	001	110	011	000

- Linear approximation $(u, v) = (001, 001)$

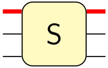


Linear approximations
Example

- 3-bit S-box $S\colon \mathbb{F}_2^3 \to \mathbb{F}_2^3$

x	000	001	010	011	100	101	110	111
$S(x)$	111	010	100	101	001	110	011	000

- Linear approximation $(u, v) = (001, 001)$



- Correlation $2\,\Pr_{\boldsymbol{x}}\left[v^\top S(\boldsymbol{x}) = u^\top \boldsymbol{x}\right] - 1 = 2 \cdot \frac{2}{8} - 1 = -\frac{1}{2}$
  $= (-1 - 1 + 1 + 1 - 1 - 1 - 1 - 1)/8$

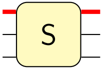
Linear approximations
Distinguishers

- Sample q inputs at random and estimate correlation
- Estimation error will be about $1/\sqrt{q}$
- $q \approx 1/c^2$ samples are enough for a distinguisher
  (assuming c is not too small/large)

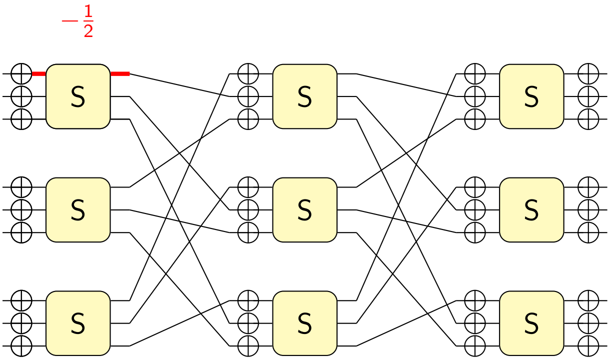
Number of samples depends on true- and false-positive probabilities (see later)

Linear approximations

$-\frac{1}{2}$



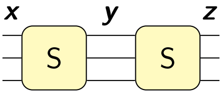
Linear approximations



Propagation through a sequence of operations?

Linear approximations

Piling up approximations



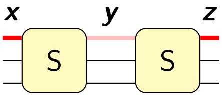
$$\begin{array}{r} \boldsymbol{r}_1 = u^\mathsf{T}\boldsymbol{x} + w^\mathsf{T}\boldsymbol{y} \\ \boldsymbol{r}_2 = w^\mathsf{T}\boldsymbol{y} + v^\mathsf{T}\boldsymbol{z} \\ \hline \boldsymbol{r}_1 + \boldsymbol{r}_2 = u^\mathsf{T}\boldsymbol{x} + v^\mathsf{T}\boldsymbol{z} \end{array}$$

Pretend that $\boldsymbol{r}_1$ and $\boldsymbol{r}_2$ are independent:

$$\underbrace{\mathrm{E}\left[(-1)^{\boldsymbol{r}_1+\boldsymbol{r}_2}\right]}_{2\,\Pr[v^\mathsf{T}\boldsymbol{z}=u^\mathsf{T}\boldsymbol{x}]-1} = \underbrace{\mathrm{E}\left[(-1)^{\boldsymbol{r}_1}\right]}_{2\,\Pr[w^\mathsf{T}\boldsymbol{y}=u^\mathsf{T}\boldsymbol{x}]-1} \times \underbrace{\mathrm{E}\left[(-1)^{\boldsymbol{r}_2}\right]}_{2\,\Pr[w^\mathsf{T}\boldsymbol{y}=v^\mathsf{T}\boldsymbol{z}]-1}$$

Linear approximations

Piling up approximations



$$\begin{aligned} \boldsymbol{r}_1 &= u^{\mathsf{T}}\boldsymbol{x} + w^{\mathsf{T}}\boldsymbol{y} \\ \boldsymbol{r}_2 &= w^{\mathsf{T}}\boldsymbol{y} + v^{\mathsf{T}}\boldsymbol{z} \\ \hline \boldsymbol{r}_1 + \boldsymbol{r}_2 &= u^{\mathsf{T}}\boldsymbol{x} + v^{\mathsf{T}}\boldsymbol{z} \end{aligned}$$

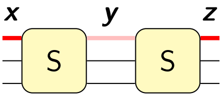
Pretend that $\boldsymbol{r}_1$ and $\boldsymbol{r}_2$ are independent:

$$\underbrace{\mathrm{E}\left[(-1)^{\boldsymbol{r}_1+\boldsymbol{r}_2}\right]}_{2\,\Pr[v^{\mathsf{T}}\boldsymbol{z}=u^{\mathsf{T}}\boldsymbol{x}]-1} \overset{\text{☠}}{=} \underbrace{\mathrm{E}\left[(-1)^{\boldsymbol{r}_1}\right]}_{2\,\Pr[w^{\mathsf{T}}\boldsymbol{y}=u^{\mathsf{T}}\boldsymbol{x}]-1} \times \underbrace{\mathrm{E}\left[(-1)^{\boldsymbol{r}_2}\right]}_{2\,\Pr[w^{\mathsf{T}}\boldsymbol{y}=v^{\mathsf{T}}\boldsymbol{z}]-1}$$

- For example: $u = w = v = 001$ gives $-1/2 \times -1/2 = 1/4$

Linear approximations

Piling up approximations



$$\begin{aligned} \boldsymbol{r}_1 &= u^\mathsf{T}\boldsymbol{x} + w^\mathsf{T}\boldsymbol{y} \\ \boldsymbol{r}_2 &= w^\mathsf{T}\boldsymbol{y} + v^\mathsf{T}\boldsymbol{z} \\ \hline \boldsymbol{r}_1 + \boldsymbol{r}_2 &= u^\mathsf{T}\boldsymbol{x} + v^\mathsf{T}\boldsymbol{z} \end{aligned}$$

Pretend that $\boldsymbol{r}_1$ and $\boldsymbol{r}_2$ are independent:

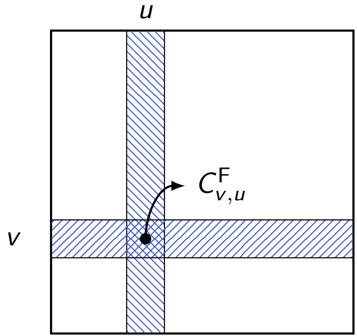
$$\underbrace{\mathrm{E}\left[(-1)^{\boldsymbol{r}_1+\boldsymbol{r}_2}\right]}_{2\,\Pr[v^\mathsf{T}\boldsymbol{z}=u^\mathsf{T}\boldsymbol{x}]-1} = \underbrace{\mathrm{E}\left[(-1)^{\boldsymbol{r}_1}\right]}_{2\,\Pr[w^\mathsf{T}\boldsymbol{y}=u^\mathsf{T}\boldsymbol{x}]-1} \times \underbrace{\mathrm{E}\left[(-1)^{\boldsymbol{r}_2}\right]}_{2\,\Pr[w^\mathsf{T}\boldsymbol{y}=v^\mathsf{T}\boldsymbol{z}]-1}$$

- For example: $u = w = v = 001$ gives $-1/2 \times -1/2 = 1/4$
- Unfortunately, this is wrong (the correct result is zero)

Correlation matrices

- $2^m \times 2^n$ matrix containing correlations of linear approximations of $\mathrm{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$

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



ℹ 'Matrix' rather than 'table' because C^{F} really does represent a linear map

Correlation matrices
Example

$$C^{S} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \color{red}{-\frac{1}{2}} & 0 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 0 & -\frac{1}{2} & \frac{1}{2} & 0 & 0 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{1}{2} & -\frac{1}{2} & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ 0 & -\frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & -\frac{1}{2} & -\frac{1}{2} & 0 & -\frac{1}{2} & 0 & 0 & \frac{1}{2} \end{bmatrix}$$

Correlation matrices

Example

$$C^{\mathsf{S}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -\frac{1}{2} & 0 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 0 & -\frac{1}{2} & \frac{1}{2} & 0 & 0 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{1}{2} & -\frac{1}{2} & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ 0 & -\frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & -\frac{1}{2} & -\frac{1}{2} & 0 & -\frac{1}{2} & 0 & 0 & \frac{1}{2} \end{bmatrix}$$

$$C^{\mathsf{F}}_{0,u} = 2\Pr[u^{\mathsf{T}}\boldsymbol{x} \quad = 0] - 1 = \begin{cases} 1 & \text{if } u = 0 \\ 0 & \text{else} \end{cases}$$

$$C^{\mathsf{F}}_{v,0} = 2\Pr[v^{\mathsf{T}}\mathsf{F}(\boldsymbol{x}) = 0] - 1 = \begin{cases} 1 & \text{if } v = 0 \\ 0 & \text{else} \end{cases}$$

(second property if F is invertible)

Correlation matrices
Multiplication property

- If $F = F_2 \circ F_1$, then
$$C^{F} = C^{F_2} C^{F_1}$$

Proof by calculation

- This is the most important property of correlation matrices

- There are more conceptual (but more abstract) proofs without calculation

Correlation matrices

Multiplication property

- If F is invertible, then $C^{\mathsf{F}^{-1}} = \left(C^{\mathsf{F}}\right)^{-1}$

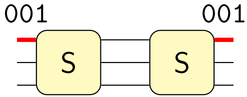
- If F is invertible, then C^{F} is orthogonal

Proof: show that $C^{\mathsf{F}^{-1}} = \left(C^{\mathsf{F}}\right)^{\mathsf{T}}$

$\boldsymbol{x} = \mathsf{F}^{-1}(\boldsymbol{y})$ is still uniform random because F is invertible

Correlation matrices

Multiplication property: example



Correlation matrices

Multiplication property: example

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -\frac{1}{2} & 0 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 0 & -\frac{1}{2} & \frac{1}{2} & 0 & 0 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{1}{2} & -\frac{1}{2} & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ 0 & -\frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & -\frac{1}{2} & -\frac{1}{2} & 0 & -\frac{1}{2} & 0 & 0 & \frac{1}{2} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -\frac{1}{2} & 0 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 0 & -\frac{1}{2} & \frac{1}{2} & 0 & 0 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{1}{2} & -\frac{1}{2} & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ 0 & -\frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & -\frac{1}{2} & -\frac{1}{2} & 0 & -\frac{1}{2} & 0 & 0 & \frac{1}{2} \end{bmatrix}$$

- Correlation of $(\mathtt{001}, \mathtt{001})$ over $\mathsf{S} \circ \mathsf{S}$:

$$\frac{1}{4} - \frac{1}{4} - \frac{1}{4} + \frac{1}{4} = 0$$

- Correct result, but this approach doesn't scale

Linear trails

- If $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_2 \circ \mathsf{F}_1$, then $C^{\mathsf{F}} = C^{\mathsf{F}_r} \cdots C^{\mathsf{F}_2} C^{\mathsf{F}_1}$
- Writing out this product of matrices gives

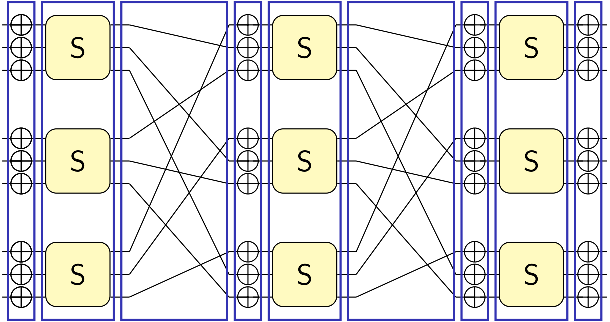
$$C^{\mathsf{F}}_{u_{r+1},u_1} = \sum_{u_2,\ldots,u_r} C^{\mathsf{F}_r}_{u_{r+1},u_r} \cdots C^{\mathsf{F}_2}_{u_3,u_2} C^{\mathsf{F}_1}_{u_2,u_1}$$

- A linear trail is a sequence $(u_1, u_2, \ldots, u_{r+1})$ and has correlation $\prod_{i=1}^{r} C^{\mathsf{F}_i}_{u_{i+1},u_i}$
- Most analysis relies on the assumption that there exist a set Λ of 'dominant trails':

$$C^{\mathsf{F}}_{u_{r+1},u_1} = \sum_{u\in\Lambda} \prod_{i=1}^{r} C^{\mathsf{F}_i}_{u_{i+1},u_i} + \varepsilon$$

Linear trails

Example



C^{k_1} $C^{\mathcal{S}}$ C^{P} C^{k_2} $C^{\mathcal{S}}$ C^{P} C^{k_3} $C^{\mathcal{S}}$ C^{k_4}

- To analyze trails we need to determine C^{k_i}, $C^{\mathcal{S}}$ and C^{P}

Correlation matrices
Bricklayer functions

- If $\mathsf{F}(x_1 \| x_2) = \mathsf{F}_1(x_1) \| \mathsf{F}_2(x_2)$, then

$$C^{\mathsf{F}}_{v_1 \| v_2, u_1 \| u_2} = C^{\mathsf{F}_1}_{v_1, u_1} C^{\mathsf{F}_2}_{v_2, u_2}$$

Proof by calculation

Correlation matrices
Bricklayer functions

- If $\mathsf{F}(x_1 \| x_2) = \mathsf{F}_1(x_1) \| \mathsf{F}_2(x_2)$, then

$$C^{\mathsf{F}}_{v_1 \| v_2, u_1 \| u_2} = C^{\mathsf{F}_1}_{v_1, u_1} C^{\mathsf{F}_2}_{v_2, u_2}$$

Proof by calculation

- Equivalently: $C^{\mathsf{F}} = C^{\mathsf{F}_1} \otimes C^{\mathsf{F}_2}$

- For the S-box layer: $C^{\mathcal{S}} = C^{\mathsf{S}} \otimes C^{\mathsf{S}} \otimes C^{\mathsf{S}}$

Correlation matrices

Translations and linear functions

- If $\mathsf{F}(x) = x + k$, then

$$C^{\mathsf{F}}_{v,u} = \begin{cases} (-1)^{v^\top k} & \text{if } u = v \\ 0 & \text{else} \end{cases}$$

Proof

Correlation matrices

Translations and linear functions

- If $\mathsf{F}(x) = x + k$, then

$$C^{\mathsf{F}}_{v,u} = \begin{cases} (-1)^{v^\top k} & \text{if } u = v \\ 0 & \text{else} \end{cases}$$

Proof

- If $\mathsf{F}(x) = Mx$ with $M \in \mathbb{F}_2^{m \times n}$ then

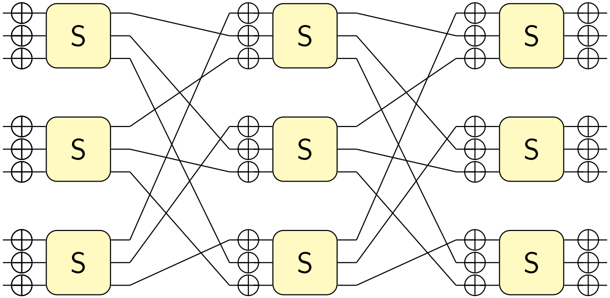
$$C^{\mathsf{F}}_{v,u} = \begin{cases} 1 & \text{if } u = M^\top v \\ 0 & \text{else} \end{cases}$$

Proof

- Bit permutation P satisfies $\mathsf{P}^\top = \mathsf{P}^{-1}$

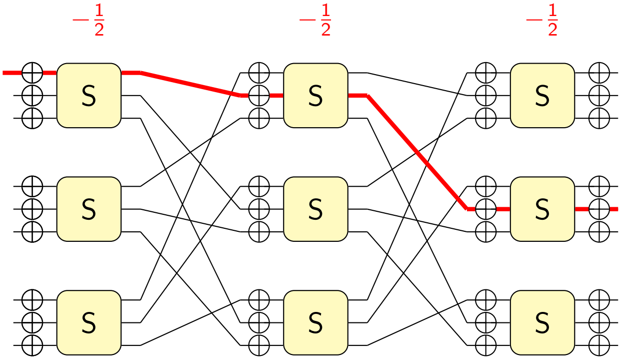
Linear trails

Example: 3-round approximation



Linear trails

Example: 3-round approximation

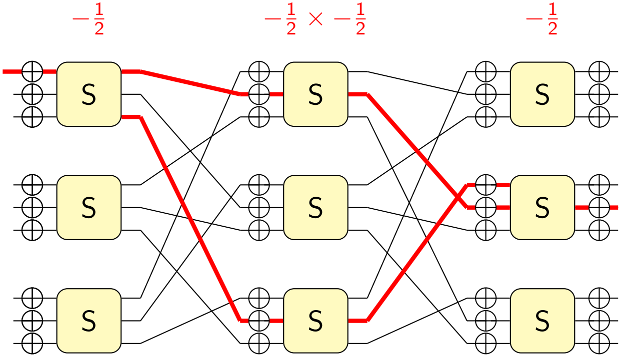


$$(-1)^{\kappa_1}/8$$

with $\kappa_1 = k_{1,1} + k_{2,2} + k_{3,5} + 1$

Linear trails

Example: 3-round approximation

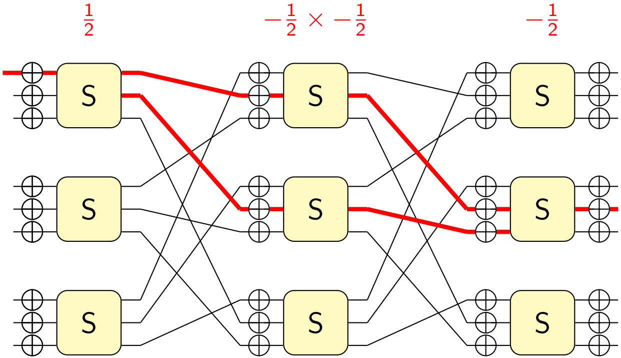


$$(-1)^{\kappa_1}/8 + (-1)^{\kappa_1+\kappa_2}/16$$

with $\kappa_1 = k_{1,1} + k_{2,2} + k_{3,5} + 1$, $\kappa_2 = k_{2,8} + k_{3,4}$

Linear trails

Example: 3-round approximation

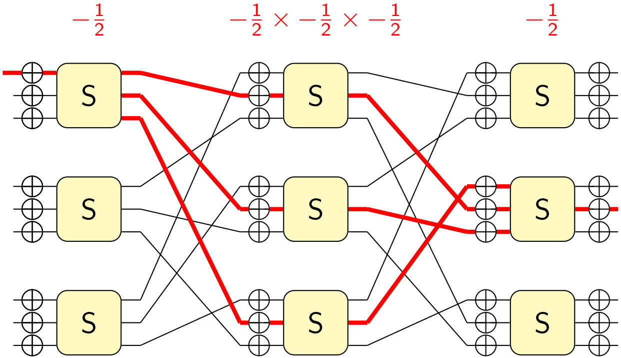


$$(-1)^{\kappa_1}/8 + (-1)^{\kappa_1+\kappa_2}/16 + (-1)^{\kappa_1+\kappa_3}/16$$

with $\kappa_1 = k_{1,1} + k_{2,2} + k_{3,5} + 1$, $\kappa_2 = k_{2,8} + k_{3,4}$ and $\kappa_3 = k_{2,5} + k_{3,6}$

Linear trails

Example: 3-round approximation

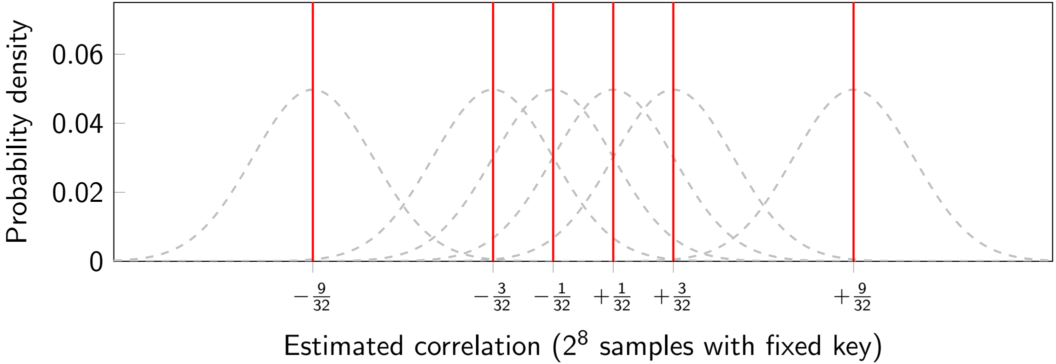


$$(-1)^{\kappa_1}/8 + (-1)^{\kappa_1+\kappa_2}/16 + (-1)^{\kappa_1+\kappa_3}/16 + (-1)^{\kappa_1+\kappa_2+\kappa_3}/32$$

with $\kappa_1 = k_{1,1} + k_{2,2} + k_{3,5} + 1$, $\kappa_2 = k_{2,8} + k_{3,4}$ and $\kappa_3 = k_{2,5} + k_{3,6}$

Linear trails

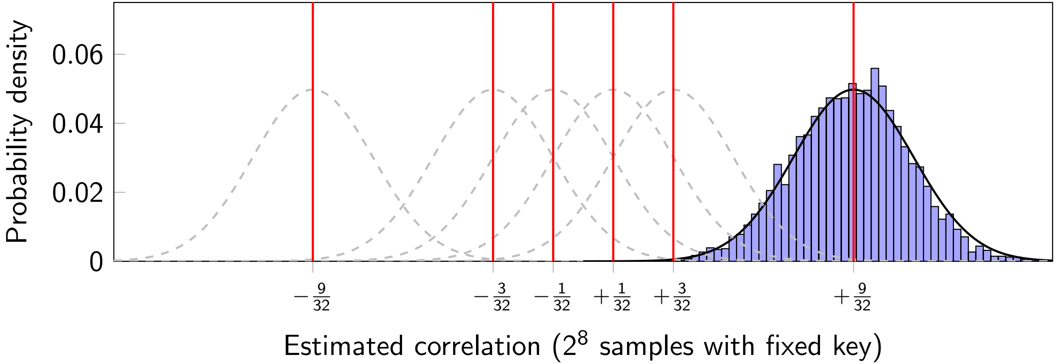
Example: 3-round approximation



- $C^{\mathsf{F}}_{001,001} = (-1)^{\kappa_1}/8\,\big(1 + (-1)^{\kappa_1+\kappa_2}/2\big)\big(1 + (-1)^{\kappa_1+\kappa_3}/2\big) \in \left\{ \pm\frac{1}{32}, \pm\frac{3}{32}, \pm\frac{9}{32} \right\}$
- Correlation reveals something about the key (but we will see better methods later)

Linear trails

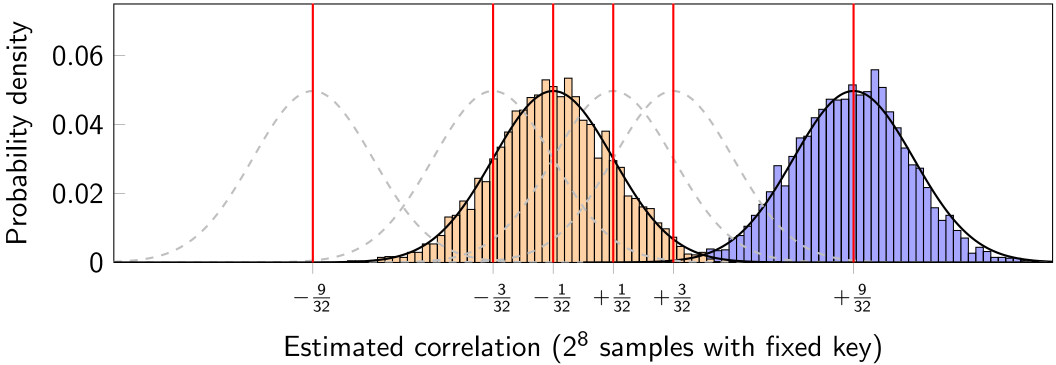
Example: 3-round approximation



- $C^{\mathsf{F}}_{001,001} = (-1)^{\kappa_1}/8\,\big(1 + (-1)^{\kappa_1+\kappa_2}/2\big)\big(1 + (-1)^{\kappa_1+\kappa_3}/2\big) \in \left\{ \pm\frac{1}{32}, \pm\frac{3}{32}, \pm\frac{9}{32} \right\}$
- Correlation reveals something about the key (but we will see better methods later)

Linear trails

Example: 3-round approximation



- $C^{\mathsf{F}}_{001,001} = (-1)^{\kappa_1}/8\left(1+(-1)^{\kappa_1+\kappa_2}/2\right)\left(1+(-1)^{\kappa_1+\kappa_3}/2\right) \in \left\{\pm\frac{1}{32}, \pm\frac{3}{32}, \pm\frac{9}{32}\right\}$
- Correlation reveals something about the key (but we will see better methods later)

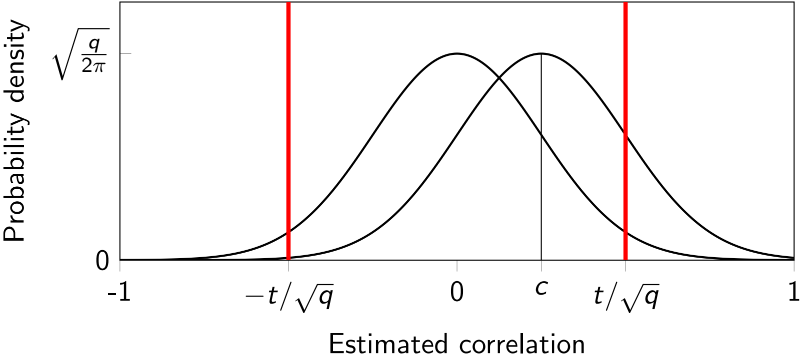
Cost analysis

- Using q independent samples:

$$\widehat{\boldsymbol{c}} = \frac{1}{q}\sum_{i=1}^{q}(-1)^{u^\top \boldsymbol{x}_i + v^\top \boldsymbol{y}_i}$$

- Simplifications:
  - q is not too small and correlation c is not too large
  - Correlation is zero for wrong key guesses
- Distribution of $\widehat{\boldsymbol{c}}$ is close to normal with mean c and variance $(1-c^2)/q \approx 1/q$
- Hypothesis test: $|\widehat{\boldsymbol{c}}| \geq t/\sqrt{q}$?

Cost analysis



- True-positive probability $P_S = \Phi(c\sqrt{q} - t) + \Phi(-c\sqrt{q} - t)$
- False-positive probability $P_F = 2\Phi(-t)$

Cost analysis

- Eliminating t gives

$$P_\mathsf{S} = \Phi\big(\Phi^{-1}(P_\mathsf{F}/2) + c\sqrt{q}\big) + \Phi\big(\Phi^{-1}(P_\mathsf{F}/2) - c\sqrt{q}\big)$$

- If $|c|\sqrt{q}$ is large enough, one of both terms is dominant so

$$q = \left(\frac{\Phi^{-1}\big(P_\mathsf{S}\big) - \Phi^{-1}(P_\mathsf{F}/2)}{c}\right)^2$$

- If c depends on the key, need to average the success probability

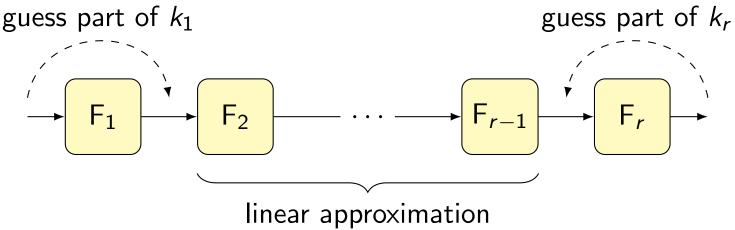
This is essentially optimal *but important assumptions are made*

Key recovery

- Correlation depends on the key, and this can be used for key-recovery
  Extreme case with one dominant trail

$$C^{\mathsf{F}}_{v,u} \approx (-1)^{w^\top k}\, c$$

- Guessing key material from the first or last round is often more powerful



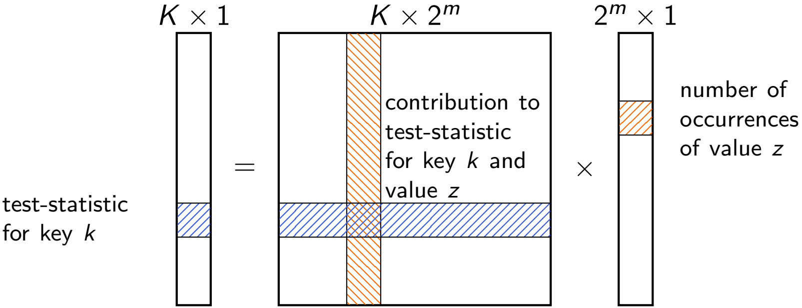
- Naive cost: $\mathcal{O}(qK)$ for K candidate keys if the distinguisher uses q data
  on average $P_{\mathsf{F}}K$ incorrect candidates remain

Key recovery

Matsui's method

- Samples $(x_1, y_1), \ldots, (x_q, y_q) \to$ reduced values $z_1, \ldots, z_q \in \mathbb{F}_2^m$
- For candidate key k, the estimated correlation is of the form

$$\widehat{c}_k = \sum_{i=1}^{q} f_k(z_i) = \sum_{z \in \mathbb{F}_2^m} f_k(z)\,\#\{1 \leq i \leq q \mid z_i = z\}$$



- Cost: $\mathcal{O}(q + K2^m)$ time and $\mathcal{O}(q + K + 2^m)$ memory

Further topics

Table of contents of *Linear Cryptanalysis*