Linear Cryptanalysis

Maria Eichlseder

Applied Cryptography 2 – ST 2020

Outline

Linear Approximations and Characteristics

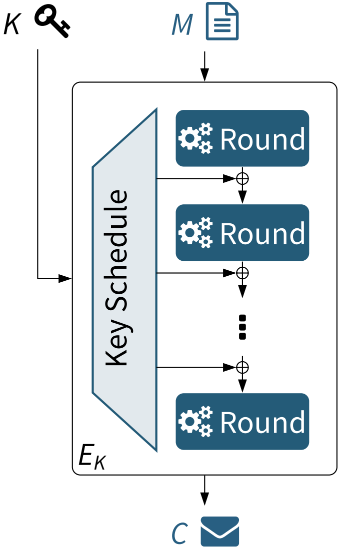
Finding paths through the cipher

Linear Cryptanalysis – Overview

- Proposed by Matsui [Mat93]
- Broke `DES` with 2^{47} known plaintext-ciphertext pairs
- One of the two major statistical attack techniques and design criteria for block ciphers (and other primitives)

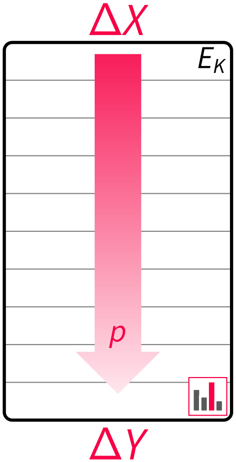
- Main idea:
  1. Find approximate equation about `xor` of selected bits M_i, C_i, and K_i
  2. Use equation as distinguisher to recover the key

Reminder: The Key-Alternating Construction

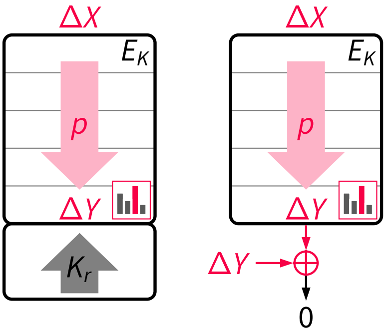


Reminder: Differential Cryptanalysis – Idea

Method



Attack Goals



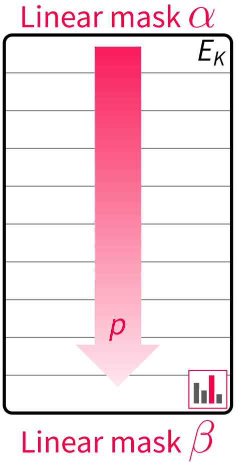
key recovery

collision, forgery

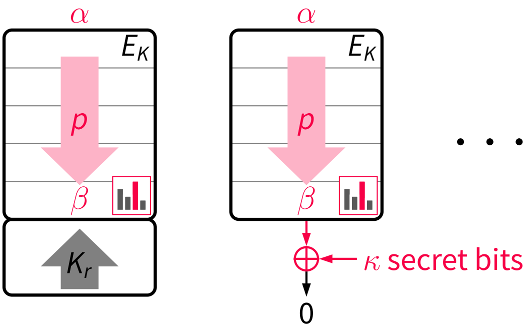
. . .

Linear Cryptanalysis – Idea [Mat93]

Method



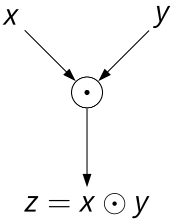
Attack Goals



key recovery confidentiality

Approximating nonlinear functions by linear functions

Example: AND-gate



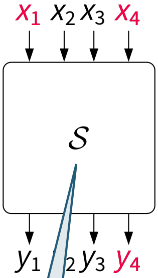
In		Out	Linear functions			
x	y	$x \odot y$	0	x	y	$x \oplus y$
0	0	0	0	0	0	0
0	1	0	0	0	1	1
1	0	0	0	1	0	1
1	1	1	0	1	1	0
Probability			$\frac{3}{4}$	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{1}{4}$

We get four different equally efficient approximations for $z = x \odot y$ that are correct with probability $\frac{3}{4}$:

$z \approx 0, \quad z \approx x, \quad z \approx y, \quad z \approx x \oplus y \oplus 1.$

Linear Approximation of S-boxes

Example: an output bit of the PRESENT S-box



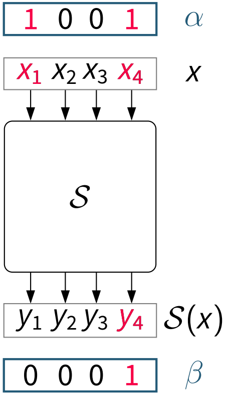
x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$\mathcal{S}(x)$	c	5	6	b	9	0	a	d	3	e	f	8	4	7	1	2

$x_1\ x_2\ x_3\ x_4$	$y_1\ y_2\ y_3\ y_4$	$y_4 = x_1 \oplus x_4$
0 0 0 0	1 1 0 0	✓
0 0 0 1	0 1 0 1	✓
0 0 1 0	0 1 1 0	✓
0 0 1 1	1 0 1 1	✓
0 1 0 0	1 0 0 1	✗
0 1 0 1	0 0 0 0	✗
0 1 1 0	1 0 1 0	✓
0 1 1 1	1 1 0 1	✓
1 0 0 0	0 0 1 1	✓
1 0 0 1	1 1 1 0	✓
1 0 1 0	1 1 1 1	✓
1 0 1 1	1 0 0 0	✓
1 1 0 0	0 1 0 0	✗
1 1 0 1	0 1 1 1	✗
1 1 1 0	0 0 0 1	✓
1 1 1 1	0 0 1 0	✓
Probability		12 / 16

Linear Masks

We are interested in *any* linear equation of the b input and b output bits
$\rightarrow$ select bits with masks $\alpha, \beta \in \mathbb{F}_2^b$ and the inner product $\alpha \cdot x := \bigoplus \alpha_i \cdot x_i$:

Alternative notation: $\alpha \cdot x^T$ or $\langle \alpha, x \rangle$ or $\ell_\alpha(x)$



Linear approximation:

$$\alpha \cdot x = \beta \cdot \mathcal{S}(x)$$

$$x_1 \oplus x_4 = y_4$$

Measuring the Quality of the Approximation: Bias & co.

The quality of the approximation (α, β) of the b-bit S-box $\mathcal{S}$ can be described equivalently using the following metrics:

- Solutions $s = |\{x \in \mathbb{F}_2^b \mid \alpha \cdot x = \beta \cdot \mathcal{S}(x)\}|$ $= 12$
- Probability $p = \mathbb{P}_x[\alpha \cdot x = \beta \cdot \mathcal{S}(x)] = s/2^b$ $= \frac{12}{16}$
- Bias $\varepsilon = p - \frac{1}{2}$ $= \frac{12}{16} - \frac{1}{2} = \frac{4}{16} = \frac{1}{4}$
- Correlation $\mathrm{cor} = 2 \cdot \varepsilon$ $= 2 \cdot \frac{1}{4} = \frac{1}{2} = 2^{-1}$

Assume we have a linear approximation $\alpha \cdot x = \beta \cdot \mathcal{S}(x)$ that holds with bias ε:

- If $\varepsilon = 0$, we learn nothing (as good as random guess, correct half the time)
- If $\varepsilon > 0$, the approximation $\alpha \cdot x = \beta \cdot \mathcal{S}(x)$ is good
- If $\varepsilon < 0$, the approximation $\alpha \cdot x = \beta \cdot \mathcal{S}(x) \oplus 1$ is good

Linear Approximation Table (LAT)

The LAT lists the quality of every possible mask: $\mathsf{LAT}[\alpha, \beta] = s - 2^{b-1} = 2^b \varepsilon$

$\alpha \setminus \beta$	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	−4	0	−4	0	0	0	0	0	−4	0	4
2	0	0	2	2	−2	−2	0	0	2	−2	0	4	0	4	−2	2
3	0	0	2	2	2	−2	−4	0	−2	2	−4	0	0	0	−2	−2
4	0	0	−2	2	−2	−2	0	4	−2	−2	0	−4	0	0	−2	2
5	0	0	−2	2	−2	2	0	0	2	2	−4	0	4	0	2	2
6	0	0	0	−4	0	0	−4	0	0	−4	0	0	4	0	0	0
7	0	0	0	4	4	0	0	0	0	−4	0	0	0	0	4	0
8	0	0	2	−2	0	0	−2	2	−2	2	0	0	−2	2	4	4
9	0	4	−2	−2	0	0	2	−2	−2	−2	−4	0	−2	2	0	0
a	0	0	4	0	2	2	2	−2	0	0	0	−4	2	2	−2	2
b	0	−4	0	0	−2	−2	2	−2	−4	0	0	0	2	2	2	−2
c	0	0	0	0	−2	−2	−2	−2	4	0	0	−4	−2	2	2	−2
d	0	4	4	0	−2	−2	2	2	0	0	0	0	2	−2	2	−2
e	0	0	2	2	−4	4	−2	−2	−2	−2	0	0	−2	−2	0	0
f	0	4	−2	2	0	0	−2	−2	−2	2	4	0	2	2	0	0

Linear Approximations of (Affine) Linear Functions

Consider a linear function (e.g., part of the diffusion layer)

$$y = \mathcal{L}(x).$$

Then any approximation is either perfect ($\mathrm{cor} = \pm 1$) or useless ($\mathrm{cor} = 0$).
Which approximations (α, β) are good?

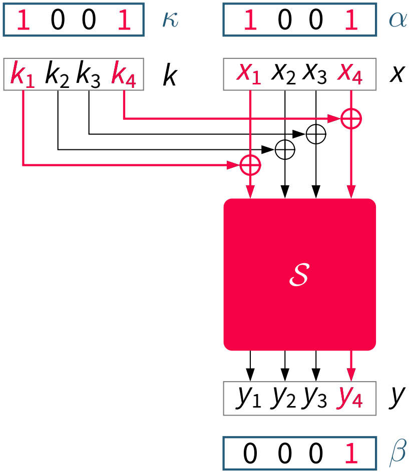
Write $\mathcal{L}$ as a matrix multiplication $y = \mathcal{L}(x) = L \cdot x$, then

$$\mathrm{cor}_{\mathcal{L}}(\alpha, \beta) = \begin{cases} 1 & \text{if } \alpha = L^\top \cdot \beta \\ 0 & \text{else.} \end{cases}$$

If $\mathcal{L}$ is affine linear (linear function $\oplus$ constant), the correlation may be ± 1, depending on the constant.

In particular, the key addition in a key-alternating cipher may change the sign $\pm$!

Key Addition + S-box



Linear approximation:

$$\alpha \cdot x \oplus \kappa \cdot k = \beta \cdot y$$

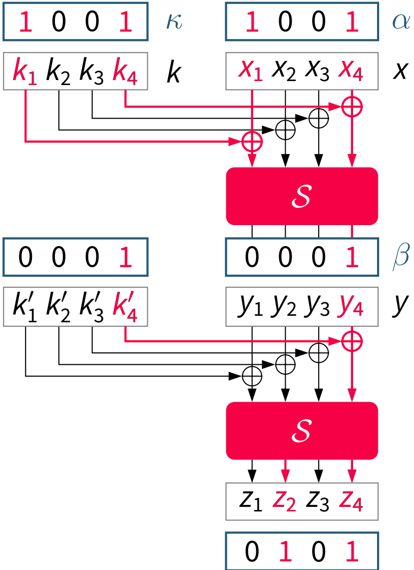
$$x_1 \oplus x_4 \oplus k_1 \oplus k_4 = y_4$$

or

$$x_1 \oplus x_4 \oplus y_4 = k_1 \oplus k_4$$

$\rightarrow$ 1-bit equation about the key!

Key Addition + S-box + Key Addition + S-box



Linear approximations:

$$\alpha \cdot x \oplus \kappa \cdot k = \beta \cdot y$$
$$x_1 \oplus x_4 \oplus k_1 \oplus k_4 = y_4$$

and

$$\beta \cdot y \oplus \kappa' \cdot k' = \gamma \cdot z$$
$$y_4 \oplus k'_4 = z_2 \oplus z_4$$

$$\Downarrow$$

$$\alpha \cdot x \oplus \kappa \cdot k \oplus \kappa' \cdot k' = \gamma \cdot z$$
$$x_1 \oplus x_4 \oplus k_1 \oplus k_4 \oplus k'_4 = z_2 \oplus z_4$$

What's the bias of this approximation?

The two approximations hold with probabilities
$p_1 = \frac{1}{2} + \varepsilon_1 = \frac{1}{2} + \frac{4}{16} = \frac{3}{4}$ (see LAT[$9, 1$]) and
$p_2 = \frac{1}{2} + \varepsilon_2 = \frac{1}{2} - \frac{4}{16} = \frac{1}{4}$ (see LAT[$1, 5$]).

The combined approximation is correct if both are correct *or both are wrong*; so, assuming the two probabilities are independent:

$$
\begin{aligned}
p &= p_1 \cdot p_2 + (1 - p_1) \cdot (1 - p_2) \\
&= 2 \cdot p_1 \cdot p_2 - p_1 - p_2 + 1 \\
&= 2 \cdot \left(\frac{1}{2} + \varepsilon_1\right) \cdot \left(\frac{1}{2} + \varepsilon_2\right) - \left(\frac{1}{2} + \varepsilon_1\right) - \left(\frac{1}{2} + \varepsilon_2\right) + 1 \\
&= \frac{1}{2} + 2 \cdot \varepsilon_1 \cdot \varepsilon_2
\end{aligned}
$$

The Piling-Up Lemma

Theorem (Piling-up Lemma)

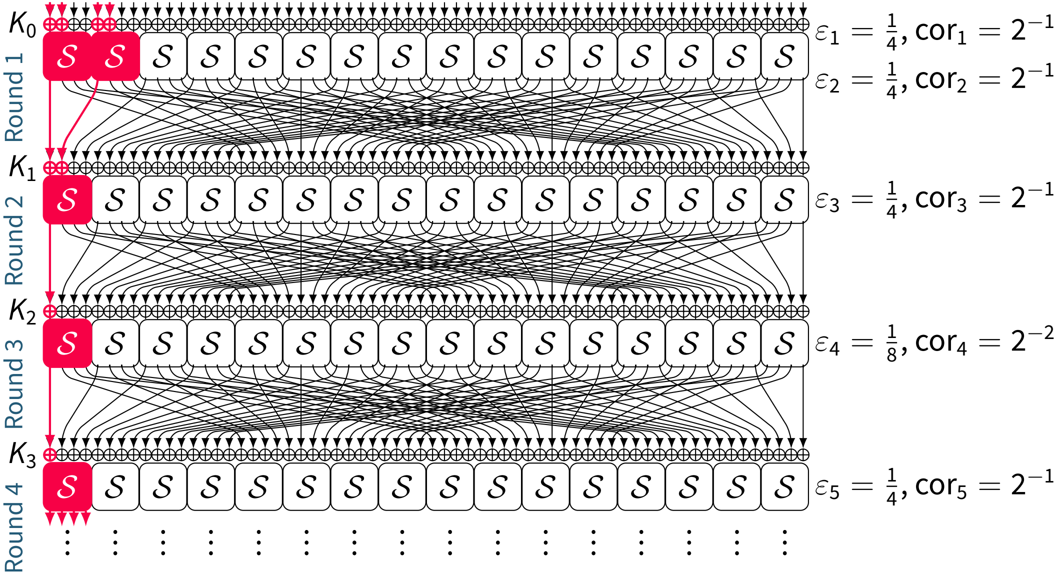
Let X_i $(1 \leq i \leq n)$ be independent Boolean expressions (corresponding to the individual approximations) with probabilities $p_i = \mathbb{P}(X_i = 0) = \frac{1}{2} + \varepsilon_i$. Then

$$\mathbb{P}(X_1 \oplus X_2 \oplus \cdots \oplus X_n = 0) = \frac{1}{2} + 2^{n-1} \prod_{i=1,\ldots,n} \varepsilon_i$$

Or in terms of the correlation $\mathrm{cor} = 2\varepsilon$:

$$\mathrm{cor} = \prod_{i=1,\ldots,n} \mathrm{cor}_i \, .$$

Example: A 4-Round Linear Characteristic for PRESENT with $\varepsilon = 2^{-7}$



Key Recovery

The Correlation

The correlation $\text{cor}_F(\alpha, \beta)$ of an approximation (α, β) for a function $F : \mathbb{F}_2^b \to \mathbb{F}_2^{b'}$ can be represented in several useful ways:

$$\begin{aligned}
\text{cor}_F(\alpha, \beta) &= 2 \cdot \varepsilon \\
&= 2 \cdot \mathbb{P}[\alpha \cdot x = \beta \cdot F(x)] - 1 \\
&= \mathbb{P}_x[\alpha \cdot x \oplus \beta \cdot F(x) = 0] - \mathbb{P}_x[\alpha \cdot x \oplus \beta \cdot F(x) = 1] \\
&= \frac{1}{2^b} \sum_{x \in \mathbb{F}_2^b} (-1)^{\alpha \cdot x \oplus \beta \cdot F(x)} \qquad \text{(Fourier transform)}
\end{aligned}$$

The correlation takes values between -1 and 1.

The Correlation and the Key

Consider an approximation for the full-round block cipher $C = E_K(P)$:

$$\alpha \cdot P \oplus \beta \cdot C \oplus \kappa \cdot K = 0$$

This gives us an equation on the key that holds with some probability:

$$\alpha \cdot P \oplus \beta \cdot C = \kappa \cdot K$$

Different keys only change the sign of this approximation's correlation.

We can also consider the "linear hull" without the key masks:

$$\alpha \cdot P \oplus \beta \cdot C = 0$$

Key Recovery – Matsui's Algorithm 1 [Mat93]

Assume we have an approximation $\alpha \cdot P \oplus \beta \cdot C \oplus \kappa \cdot K = 0$ with positive bias ε and have collected "enough" known plaintext-ciphertext pairs (P_i, C_i):

Key Recovery with Algorithm 1

- Initialize two counters $T_0 = 0$ and $T_1 = 0$.
- For each plaintext/ciphertext pair (P_i, C_i) do
  - If $\alpha \cdot P_i \oplus \beta \cdot C_i = 0$, increase counter T_0 👍
  - If $\alpha \cdot P_i \oplus \beta \cdot C_i = 1$, increase counter T_1 👎
- We learn the following 1-bit information about the key:
  - If $T_0 > T_1 \quad \Rightarrow \quad \kappa \cdot K = 0$
  - If $T_1 > T_0 \quad \Rightarrow \quad \kappa \cdot K = 1$

Algorithm 1 – Discussion

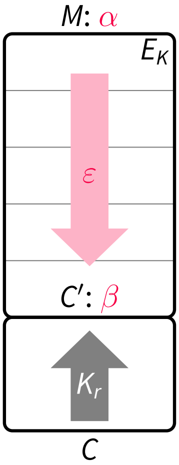
Disadvantages:

- Requires an approximation for all R rounds of the cipher
- We learn only one bit of key information
- Need several approximations for more key information

Advantages:

- The bit of key information can directly be used to attack confidentiality (biased information about unknown plaintexts)

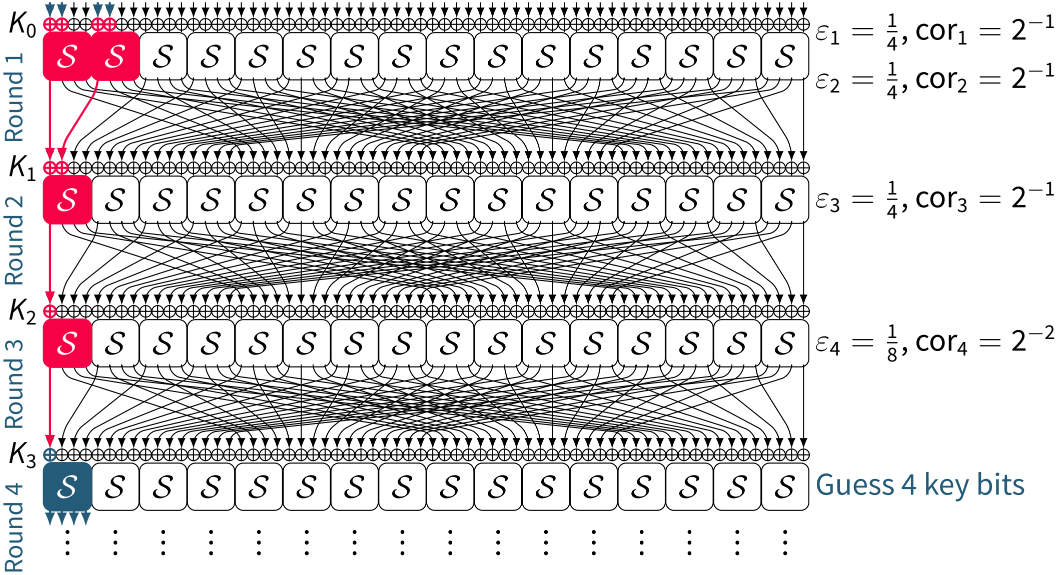
Key Recovery – Matsui's Algorithm 2 [Mat93]



- Obtain enough (about $1/\varepsilon^2$) known-plaintext pairs $M_i \to C_i$
- For each possible candidate value K_r of last round key:
  - Initialize counters $T_0^{K_r} = 0$ 👍 and $T_1^{K_r} = 0$ 👎
  - Decrypt each C_i 1 round to get intermediate C'
  - If $\alpha \cdot M = \beta \cdot C'$, increase $T_0^{K_r}$ 👍, else $T_1^{K_r}$ 👎
- The right key will have a large difference $T_0^{K_r} - T_1^{K_r}$ (cor)

K_r	Upvote counter
0000	👍👍👍 | 👎👎👎
0001	👍👍👎 | 👎👎👎
0002	👍👍👍 | 👍👍👎
...	...

Example: A 3-Round Linear Characteristic for PRESENT with $\varepsilon = 2^{-6}$



Algorithm 2 – Discussion

Advantages:

- Requires an approximation (α, β) for only $R - 1$ rounds of the cipher
- We learn more bits of key information at once
- Still a known-ciphertext attack (unlike differential cryptanalysis)

Disadvantages:

- Unlike differential attacks, we cannot filter out “bad (P_i, C_i) pairs”
- Need to guess more key bits, which may be expensive

How much Data is "enough"?

Squared Correlation

Let $F : \mathbb{F}_2^b \to \mathbb{F}_2^b$ be a function and (α, β) a linear approximation. The Squared Correlation (aka Linear Probability, LP) of this approximation is

$$\mathrm{cor}_F^2(\alpha, \beta) = (2 \cdot \mathbb{P}_x[\alpha \cdot x = \beta \cdot F(x)] - 1)^2 \,.$$

For a keyed function $E_K : \mathbb{F}_2^b \to \mathbb{F}_2^b$, the Average Square Correlation (aka Expected Linear Probability ELP) of (α, β) is the expected value

$$\mathbb{E}_K \left[\mathrm{cor}_{E_K}^2(\alpha, \beta)\right] \,.$$

- The bias can be distinguished using about $1/\mathrm{cor}_F^2(\alpha, \beta)$ data
- For a detailed analysis of the success probability, see [SB02]

Caveats and Assumptions

- **Hypothesis of Fixed-Key Equivalence:**
  - $\mathrm{cor}^2_{E_K}(\alpha, \beta)$ depends on the key K and is hard to evaluate
  - We need to assume that the target key behaves roughly like the average key
- **Linear Hull Effect** [Nyb94]:
  - We usually only evaluate a single characteristic $(\alpha = \alpha_0, \alpha_1, \ldots, \alpha_R = \beta)$
  - The correlation of the linear hull (α, β) depends on all compatible chars
  - $\mathrm{cor}^2(\alpha, \beta)$ may be lower than individual $\mathrm{cor}^2(\alpha_0, \alpha_1, \ldots, \alpha_R)$ if there are several strong characteristics (aka trails) with different sign $(\pm)$ and their effects cancel out!
  - Assumption: One "dominant trail" contributes most of the correlation

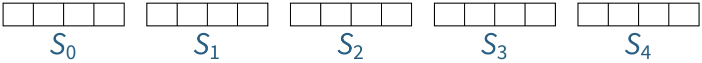
Other Applications

Keystream Biases in Stream Ciphers

Example: Keystream Biases in `MORUS`

Target design:

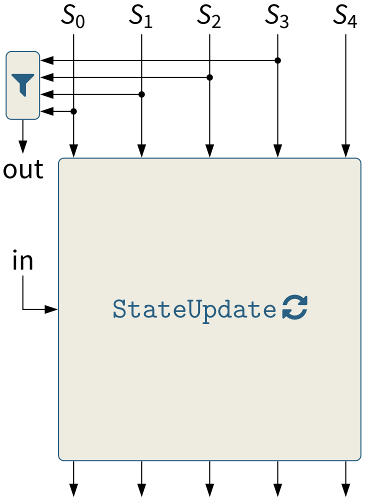
- Authenticated cipher `MORUS-1280`, a CAESAR finalist
- High-performance stream cipher with a state of $5 \times 4 \times 64 = 1280$ bits



Analysis: [AEL+18]

- Keystream correlation based on linear cryptanalysis
- Does not recover the key, but breaks confidentiality
- Full-round attack, but requires *a lot of* data

(Mini)MORUS Authenticated Cipher (simplified)



1 Initialization:

- **a** $S_0 = N, \quad S_1 = K$
- **b** $16 \times$ `StateUpdate`(0)
- **c** $S_1 = S_1 \oplus K$

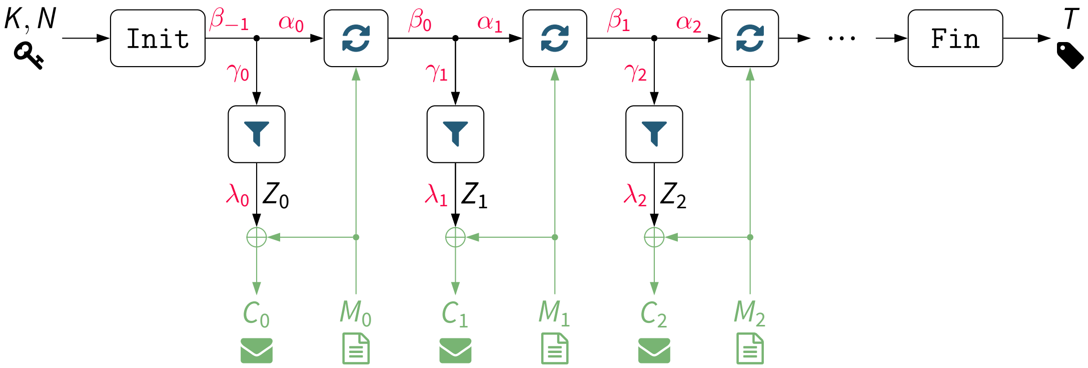
2 Encryption: For each msg block M_i:

- **a** $C_i = M_i \oplus \blacktriangledown(S_0, \ldots, S_3)$
- **b** `StateUpdate`(M_i)

3 Finalization:

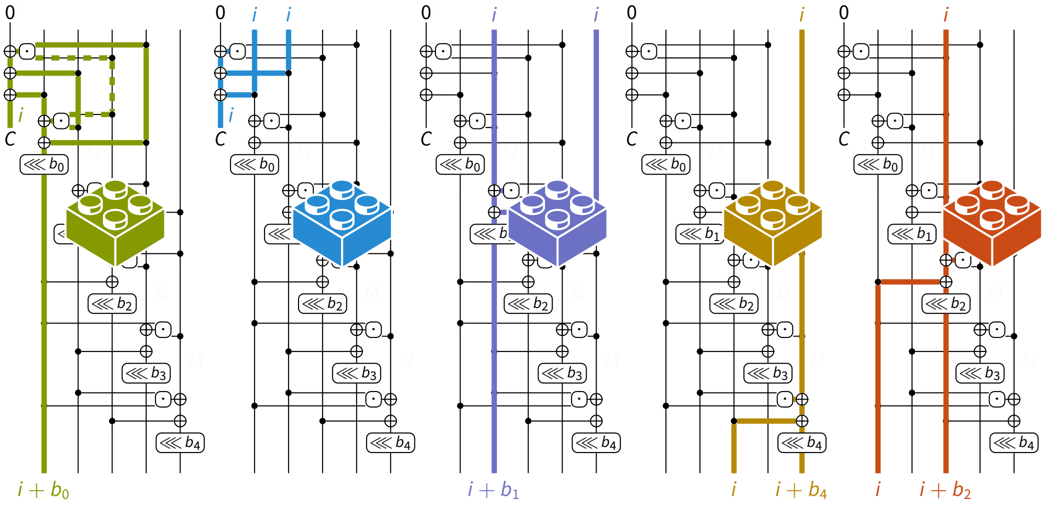
- **a** $S_4 = S_4 \oplus S_0$
- **b** $10 \times$ `StateUpdate`$(\mathrm{len}(M))$
- **c** $T = \blacktriangledown(S_0, \ldots, S_3)$

Linear Keystream Approximation

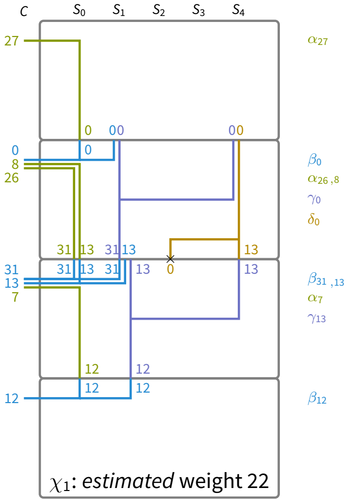


- Exploit keystream bias of $\lambda_0 \cdot Z_0 \oplus \lambda_1 \cdot Z_1 \oplus \lambda_2 \cdot Z_2$
- Correlation cor $= \prod_i (2p_i - 1) \to$ data complexity about cor^{-2} KP

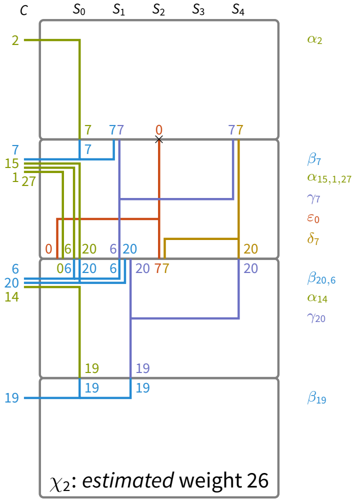
MiniMORUS: Approximation fragments $\alpha, \beta, \gamma, \delta, \varepsilon$



weight(α_i^t) = 2 (not 4) weight(β_i^t) = 2 weight(γ_i^t) = 2 weight(δ_i^t) = 2 weight(ε_i^t) = 2



$$C^1_2 \oplus C^2_1 \oplus C^2_7 \oplus C^2_{15} \oplus C^2_{27} \oplus C^3_6 \oplus C^3_{14} \oplus C^3_{20} \oplus C^4_{19} \to S^2_{2,0}$$



$$C^0_{27} \oplus C^1_0 \oplus C^1_8 \oplus C^1_{26} \oplus C^2_7 \oplus C^2_{13} \oplus C^2_{31} \oplus C^3_{12} \to S^2_{2,0}$$

Attack Results for MORUS

- **Keystream correlation**
  - We have a linear approximation linking the keystream bits
  - The bias is *independent* of key or nonce
  - Known plaintexts $\rightarrow$ Distinguisher
  - Fixed, unknown plaintext $\rightarrow$ Plaintext recovery
  - Similarities to RC4, BEAST (man-in-the-browser) attack on TLS
- **Data complexity**
  - Requires 2^{146} blocks for `MORUS-1280-256` (for any keys) – not practical ;-)
  - Attack was later drastically improved using automated tools
- Attack with similar effect on `AEGIS`, another finalist for high performance

Finding and Bounding Linear Characteristics

Arguing Security against LC

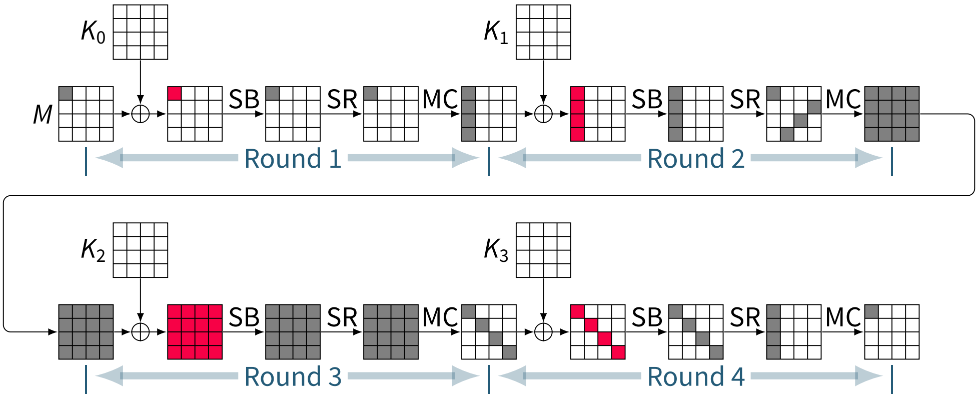
Arguing Security against Linear Cryptanalysis

- Designer wants to ensure that there are no good approximations
  - A “good” approximation has high squared correlation $\mathrm{cor}^2 \gg 2^{-\mathrm{blocksize}}$
  - Then it can be distinguished / measured with the available data
- This is hard; instead show that there are no good characteristics
  - “Dominant trail assumption”
  - Choose strong S-box and diffusion layer, then tune the nr of rounds
  - Plan a sufficient security margin
    (note: key recovery rounds, linear hull effect, multiple differentials, …)
- This is not a proof of security against LC!

Example: Application to Linear Cryptanalysis of PRESENT

- The designers prove that any 4-round characteristic has bias $|\varepsilon| \leq 2^{-7}$ ($\mathrm{cor}^2 \leq 2^{-12}$) by manually evaluating possible patterns of active S-boxes
- Thus, 28 (of the 31) rounds have $|\varepsilon| \leq 2^{7-1} \cdot 2^{-7\times 7} = 2^{-43} \rightarrow 1/\varepsilon^2 \gg 2^{64}$ ($\mathrm{cor}^2 \leq 2^{-12\times 7} = 2^{-84} \ll 2^{-64}$)
- Nevertheless, linear attacks on up to 28 (of the 31) rounds are known
  - Using multiple differentials, linear hull effect, complex key recovery, …
  - Only a narrow security margin remains

Example: Application to Linear Cryptanalysis of AES [DR02]



- `MixColumns` also has a linear branch number of 5
- `SubBytes` has a max squared correlation of $\mathrm{cor}^2 \leq 2^{-6}$
- Characteristics for 4 rounds have ≥ 25 lin. active S-boxes and $\mathrm{cor}^2 \leq 2^{-150}$

How to Find the Best Characteristics?

Finding linear characteristics (“trails”) works similarly as differential characteristics:

- By hand
  - Using strong structural properties, like MDS matrices in AES
  - Using detailed manual evaluation of patterns, like PRESENT
- With a computer’s help
  - Using off-the-shelf tools, such as MILP and SAT solvers ($\rightarrow$ next week)
  - Using dedicated tools, such as https://github.com/iaikkrypto/lineartrails

Conclusion

- Linear cryptanalysis is a powerful statistical attack on block ciphers (+more)
- Many parallels to differential cryptanalysis, but it's a known-plaintext attack

- Need to find good linear approximations for non-linear steps in each round.
- A "good" characteristic needs to be found in order to combine them.
- Use Algorithm 2 to distinguish between right and wrong key guesses in the last round.
- A secure cipher needs to ensure that there are no good linear characteristics.

Questions

Questions you should be able to answer

1. Describe the basic idea of linear approximations in linear cryptanalysis. What is the linear approximation table (LAT)?
2. How is the secret key recovered in linear cryptanalysis? Discuss Algorithm 1 and Algorithm 2.
3. Explain the Piling-up Lemma. What is it used for?
4. What are the bias and correlation of a linear approximation? How are they linked to the necessary data complexity of a successful linear attack?
5. What is the difference between Linear (Characteristic) Probability and Expected Linear (Characteristic) Probability? What is the hypothesis of fixed-key equivalence? What is the linear hull effect?

Bibliography I

[AEL+18] Tomer Ashur, Maria Eichlseder, Martin M. Lauridsen, Gaëtan Leurent, Brice Minaud, Yann Rotella, Yu Sasaki, and Benoît Viguier. **Cryptanalysis of MORUS.** Advances in Cryptology – ASIACRYPT 2018. Vol. 11273. LNCS. Springer, 2018, pp. 35–64. DOI: 10.1007/978-3-030-03329-3_2.

[BKL+07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. **PRESENT: An Ultra-Lightweight Block Cipher.** Cryptographic Hardware and Embedded Systems – CHES 2007. Vol. 4727. LNCS. Springer, 2007, pp. 450–466. DOI: 10.1007/978-3-540-74735-2_31.

[DR02] Joan Daemen and Vincent Rijmen. **The Design of Rijndael: AES – The Advanced Encryption Standard.** Information Security and Cryptography. Springer, 2002. ISBN: 3-540-42580-2. DOI: 10.1007/978-3-662-04722-4.

Bibliography II

[Mat93] Mitsuru Matsui. **Linear Cryptanalysis Method for DES Cipher.** Advances in Cryptology – EUROCRYPT 1993. Vol. 765. LNCS. Springer, 1993, pp. 386–397. DOI: 10.1007/3-540-48285-7_33.

[Nyb94] Kaisa Nyberg. **Linear Approximation of Block Ciphers.** Advances in Cryptology – EUROCRYPT '94. Vol. 950. LNCS. Springer, 1994, pp. 439–444. DOI: 10.1007/BFb0053460.

[SB02] Ali Aydın Selçuk and Ali Bıçak. **On Probability of Success in Linear and Differential Cryptanalysis.** Security in Communication Networks – SCN 2002. Vol. 2576. LNCS. Springer, 2002, pp. 174–185. DOI: 10.1007/3-540-36413-7_13.