Universal Related-Key Linear Hull Distinguishers for Key-Alternating Block Ciphers

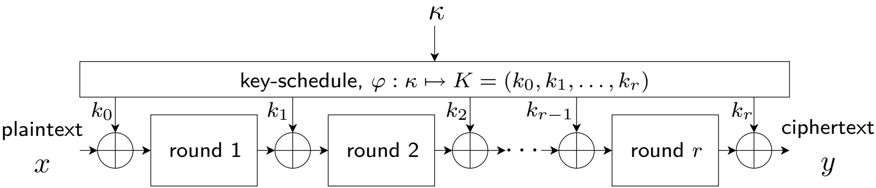
Andrey Bogdanov and Vincent Rijmen

Katholieke Universiteit Leuven, Belgium

CRYPTO'10 Rump Session

Key-Alternating Block Ciphers

AES, Serpent, PRESENT, ...



- κ = user-supplied key
- K = expanded key
- k_i = round subkeys
- n = block size in bit

Difference of Linear Correlations

For a key-alternating cipher

- U_i = a linear trail
- C_{U_i} = correlation for U_i

Difference of Linear Correlations

For a key-alternating cipher

- U_i = a linear trail
- C_{U_i} = correlation for U_i

C for a key-alternating cipher

$C = \sum_i (-1)^{U_i \diamond K + d_{U_i}} C_{U_i}$

Difference of Linear Correlations

For a key-alternating cipher

- U_i = a linear trail
- C_{U_i} = correlation for U_i

C for a key-alternating cipher

$$C = \sum_i (-1)^{U_i \diamond K + d_{U_i}} C_{U_i}$$

$C - C'$ for a key-alternating cipher

$$C - C' = \sum_i \left[(-1)^{U_i \diamond K} - (-1)^{U_i \diamond K'}\right] (-1)^{d_{U_i}} C_{U_i}$$

Difference of Linear Correlations

For a key-alternating cipher

- U_i = a linear trail
- C_{U_i} = correlation for U_i

C for a key-alternating cipher

$$C = \sum_i (-1)^{U_i \diamond K + d_{U_i}} C_{U_i}$$

$C - C'$ for a key-alternating cipher

$$C - C' = \sum_i \left[(-1)^{U_i \diamond K} - (-1)^{U_i \diamond K'} \right] (-1)^{d_{U_i}} C_{U_i}$$

Key Observation

$$(-1)^{U_i \diamond K} - (-1)^{U_i \diamond K'} = \begin{cases} 0, & \text{if } U_i \diamond K = U_i \diamond K' \Leftrightarrow U_i \diamond \Delta = 0 \\ \pm 2, & \text{if } U_i \diamond K \neq U_i \diamond K' \Leftrightarrow U_i \diamond \Delta = 1 \end{cases}$$

Distinguishers and Related-Key Conditions

Distinguisher 1

If $U_i \diamond \Delta = 0$ deterministically $\Rightarrow C - C' = 0$ deterministically

Distinguishers and Related-Key Conditions

Distinguisher 1

If $U_i \diamond \Delta = 0$ deterministically $\Rightarrow C - C' = 0$ deterministically

- $\Pr\{C - C' = 0\} = \frac{1}{\sqrt{2\pi}} 2^{-\frac{n-4}{2}}$ for an ideal cipher

Distinguishers and Related-Key Conditions

Distinguisher 1

If $U_i \diamond \Delta = 0$ deterministically $\Rightarrow C - C' = 0$ deterministically

- $\Pr\{C - C' = 0\} = \frac{1}{\sqrt{2\pi}} 2^{-\frac{n-4}{2}}$ for an ideal cipher
- Data and computational complexity: $\mathcal{O}(2^{n+1})$

Distinguishers and Related-Key Conditions

Distinguisher 1

If $U_i \diamond \Delta = 0$ deterministically $\Rightarrow C - C' = 0$ deterministically

- $\Pr\{C - C' = 0\} = \frac{1}{\sqrt{2\pi}} 2^{-\frac{n-4}{2}}$ for an ideal cipher
- Data and computational complexity: $\mathcal{O}(2^{n+1})$

Distinguisher 2 (more general)

If $U_i \diamond \Delta = 0$ with probability $p \Rightarrow C - C' \sim \mathcal{N}\left(0, \sqrt{\frac{8}{3} 2^{-n}(1 - p^2)}\right)$

Distinguishers and Related-Key Conditions

Distinguisher 1

If $U_i \diamond \Delta = 0$ deterministically $\Rightarrow C - C' = 0$ deterministically

- $\Pr\{C - C' = 0\} = \frac{1}{\sqrt{2\pi}} 2^{-\frac{n-4}{2}}$ for an ideal cipher
- Data and computational complexity: $\mathcal{O}(2^{n+1})$

Distinguisher 2 (more general)

If $U_i \diamond \Delta = 0$ with probability $p \Rightarrow C - C' \sim \mathcal{N}\left(0, \sqrt{\frac{8}{3} 2^{-n}(1-p^2)}\right)$

- $C - C' \sim \mathcal{N}(0, 2^{(1-n)/2})$ for an ideal cipher

Distinguishers and Related-Key Conditions

Distinguisher 1

If $U_i \diamond \Delta = 0$ deterministically $\Rightarrow C - C' = 0$ deterministically

- $\Pr\{C - C' = 0\} = \frac{1}{\sqrt{2\pi}} 2^{-\frac{n-4}{2}}$ for an ideal cipher
- Data and computational complexity: $\mathcal{O}(2^{n+1})$

Distinguisher 2 (more general)

If $U_i \diamond \Delta = 0$ with probability $p \Rightarrow C - C' \sim \mathcal{N}\left(0, \sqrt{\frac{8}{3} 2^{-n}(1 - p^2)}\right)$

- $C - C' \sim \mathcal{N}(0, 2^{(1-n)/2})$ for an ideal cipher
- Data and computational complexity: $\mathcal{O}(M 2^{n+1})$

Distinguishers and Related-Key Conditions

Distinguisher 1

If $U_i \diamond \Delta = 0$ deterministically $\Rightarrow C - C' = 0$ deterministically

- $\Pr\{C - C' = 0\} = \frac{1}{\sqrt{2\pi}} 2^{-\frac{n-4}{2}}$ for an ideal cipher
- Data and computational complexity: $\mathcal{O}(2^{n+1})$

Distinguisher 2 (more general)

If $U_i \diamond \Delta = 0$ with probability $p \Rightarrow C - C' \sim \mathcal{N}\left(0, \sqrt{\frac{8}{3} 2^{-n}(1 - p^2)}\right)$

- $C - C' \sim \mathcal{N}(0, 2^{(1-n)/2})$ for an ideal cipher
- Data and computational complexity: $\mathcal{O}(M 2^{n+1})$
  - M growing exponentially in HW(active positions of Δ)

Features of the Distinguishers

- Low-weight related-key condition

Features of the Distinguishers

- Low-weight related-key condition
  - Relation between κ and κ' is such that Δ has a low Hamming weight

Features of the Distinguishers

- Low-weight related-key condition
  - Relation between κ and κ' is such that Δ has a low Hamming weight
- Heavy-tail related-key condition

Features of the Distinguishers

- Low-weight related-key condition
  - Relation between κ and κ' is such that Δ has a low Hamming weight
- Heavy-tail related-key condition
  - Relation between κ and κ' is such that Δ is arbitrary in first/last subkeys and of a low Hamming weight elsewhere

Features of the Distinguishers

- Low-weight related-key condition
  - Relation between κ and κ' is such that Δ has a low Hamming weight
- Heavy-tail related-key condition
  - Relation between κ and κ' is such that Δ is arbitrary in first/last subkeys and of a low Hamming weight elsewhere

$$\Downarrow$$

- Complexity:
  - mainly depends on the key schedule

Features of the Distinguishers

- Low-weight related-key condition
  - Relation between κ and κ' is such that Δ has a low Hamming weight
- Heavy-tail related-key condition
  - Relation between κ and κ' is such that Δ is arbitrary in first/last subkeys and of a low Hamming weight elsewhere

$$\Downarrow$$

- Complexity:
  - mainly depends on the key schedule
  - to a large extent independent of $\#$ rounds