Selected Areas in Cryptology
Cryptanalysis
Week 5

Marc Stevens

stevens@cwi.nl

https://homepages.cwi.nl/~stevens/mastermath/2021/

Differential Cryptanalysis

Consider two related encryptions

1. $C = Enc_K(P)$ (with internal variables $X, Y, \ldots$)

2. $C' = Enc_K(P')$ (with internal variables $X', Y', \ldots$)

- Define difference $\Delta X = X \oplus X'$
- Study relations between input difference ΔP and output difference ΔC:
  - $p_{\Delta P,\Delta C} \coloneqq \Pr[\,\Delta C \mid \Delta P\,] = \Pr_P[Enc_K(P) \oplus Enc_K(P \oplus \Delta P) = \Delta C]$
  - Ideal secure situation:
    for every ΔP every ΔC is equally likely: $p_{\Delta P,\Delta C} \approx 2^{-n}$

- Differences are not affected by:
  - Key-addition:
    $Y = X \oplus K,\ Y' = X' \oplus K$
    $\Rightarrow \Delta Y = X \oplus K \oplus X' \oplus K = \Delta X$
  - State permutation:
    $Y[i] = X[\pi_P(i)],\ Y'[i] = X'[\pi_P(i)]$
    $\Rightarrow \Delta Y[i] = \Delta X[\pi_P(i)]$

Key-recovery attack

$(\Delta P, \Delta O_3) = ([0000\ 1011\ 0000\ 0000], [0000\ 0110\ 0110\ 0000])$

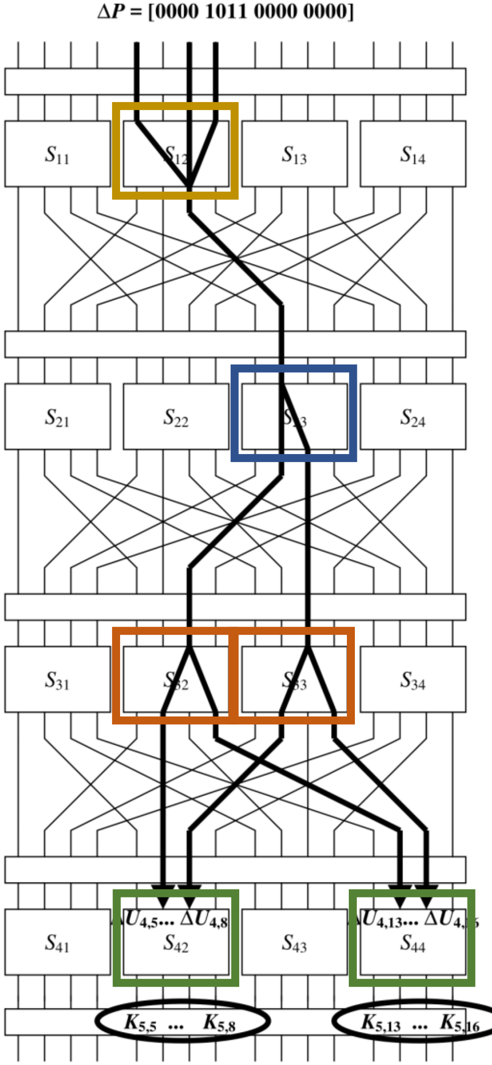
Probability: $\mathrm{p}_{\mathrm{diff}} \geq \frac{1}{2}\left(\frac{3}{8}\right)^3 = \frac{27}{1024} \approx 0.026$

Build distinguisher for 3 rounds (w/ 4 key additions)

- Over many (P_1, P_2, C_1, C_2)-tuples with $\mathrm{P}_1 \oplus P_2 = \Delta P$ measure probability of $C_1 \oplus C_2 = \Delta O_3$
- Is $\approx \frac{27}{1024} \approx 0.026 \Rightarrow$ is blockcipher oracle with 3 rounds
- Is $\approx 2^{-16} \approx 0.000015 \Rightarrow$ random oracle

Key-recovery attack idea:

1. Obtain many PPCC-tuples
2. Guess last round key => decrypt last round
   - Note how we only need to guess 8 key bits of K_5
3. Do distinguishing check
   - Outputs blockcipher oracle
     $\Rightarrow$ right key guess, stop
   - Outputs random oracle
     $\Rightarrow$ wrong key guess, try again with another guess



Other differential attacks

Key-recovery: any efficient distinguisher works

So any high probability relation that is easily checkable works

Three variant attacks based on differential cryptanalysis

1. Truncated differential cryptanalysis
   - Instead of one chosen difference for internal variables allow sets of differences
   - Potentially higher probabilities
2. Impossible differential cryptanalysis
   - Use a differential relation with probability 0
   - Have to prove no trail exists
3. Boomerang distinguishers
   - 2^{nd} order differential: P_a, P_a', P_b, P_b' with $\Delta P_a = \Delta P_b$
   - Analyze difference $\Delta X_a \oplus \Delta X_b$ between differences ΔX_a and ΔX_b

Truncated differential cryptanalysis

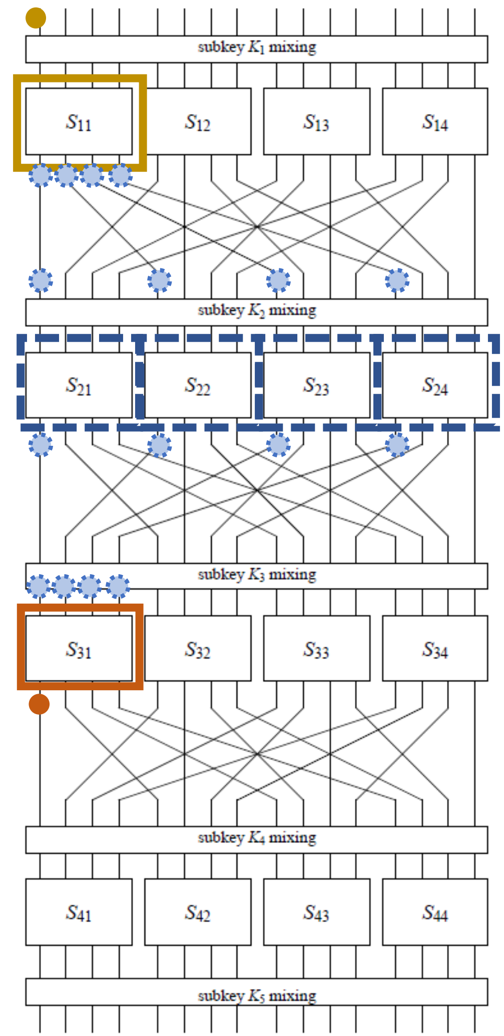
- Main idea: difference sets relations
- E.g.: $\Delta X \in \{3,7,14\} \to \Delta Y \in \{2,4\}$
- This has probability ¼ since $DDT(3,2) = \cdots = DDT(14,4) = 2$ and so
$$\Pr[\Delta Y \in \{2,4\} | \Delta X \in \{3,7,14\}] = \frac{2}{16} + \frac{2}{16} = \frac{4}{16}$$
- Or e.g.: $\Delta X \in \{1,2,3,4,5,6,7\} \to \Delta Y \in \{3,5,6,9,10,12,15\}$
with probability ¾

- Truncated differential cryptanalysis works best
with permutation layers that are:
  - 'slow': Round $i+1$ S-Box input depends on output *few* Round i S-Boxes
  - 'word'-based: F_s-linear where S-Box has s-bits

- So, not for our ToyCipher, except when applied on last round
which is equivalent to using multiple differential relations with same ΔP

Impossible differential cryptanalysis

- Idea: find differential relations with probability 0
- Since differential 'trails' probability add up for a relation, one needs to prove no differential trail exists with p>0
- E.g.:
  - $(\Delta P, \Delta O_3) = (1000\ 0 \ldots \ldots \ldots 0, 1000\ 0 \ldots \ldots \ldots 0)$
  - Note that ΔY_{11} & ΔX_{31} are unknown
    so unknown which round 2 S-Boxes are active
  - However, any active round 2 S-Box must use $DDT(1000_b, 1000_b) = DDT(8{,}8) = 0$
  - Hence, no $p > 0$ differential trail exists
- Similar for any $\Delta P = (**** \ 0000\ 0000\ 0000)$
- Similar for any ΔO_3 based on $\Delta Y_{31} = (****)$ and $\Delta Y_{32} = \Delta Y_{33} = \Delta Y_{34} = 0$



Impossible differential cryptanalysis

- Set of $(\Delta P, \Delta O_3)$:
  - $\Delta P = (1000\ 0000\ 0000\ 0000)$
  - $\Delta O_3 \in \mathcal{O} \coloneqq \{(a000\ b000\ c000\ d000)\}$
- Distinguisher:
  - Set of n $PPCC$-tuples with given ΔP
  - For each possible guess K_5:
    - Decrypt last round of C, C' of each tuple
    - If any $\Delta O_3 \in \mathcal{O}$ is observed $\Rightarrow$ wrong key guess
- Analysis:
  - Correct key guess: $\Delta O_3 \in \mathcal{O}$ never occurs
  - Wrong key guess:

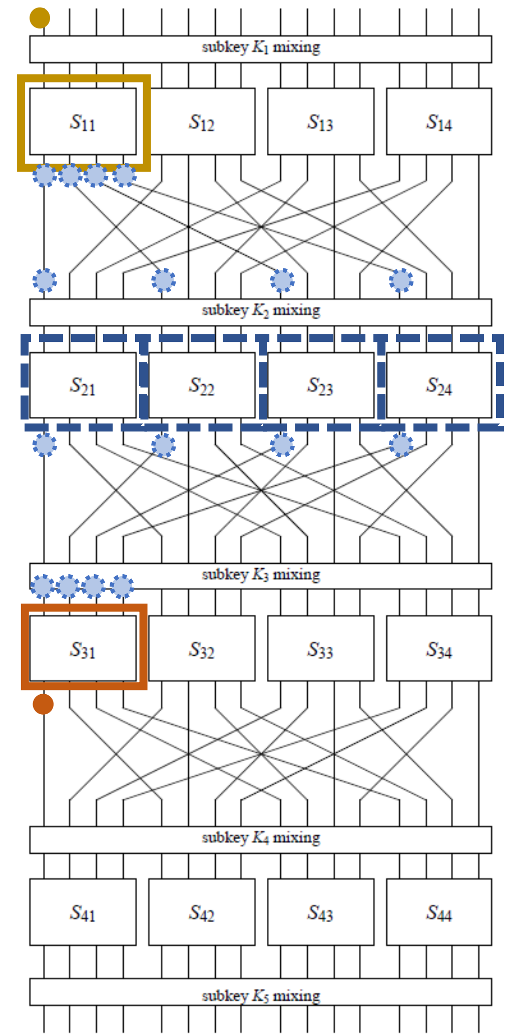
    Assume each $\Delta O_3 \in \mathcal{O}$ occurs with $p \approx n \cdot 2^{-16}$

    Observing any $\Delta O_3 \in \mathcal{O}$ occurs with $p \approx n \cdot 2^{-12}$

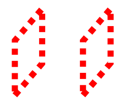
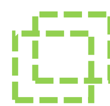
    $\Rightarrow n = O(2^{12})$ needed to filter wrong guesses

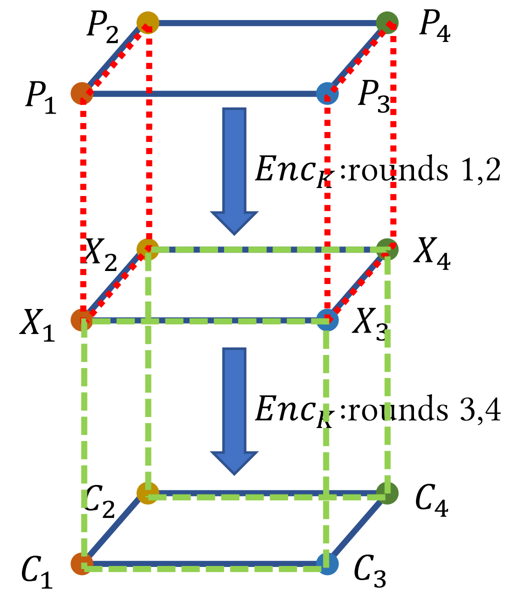
  - Improve using many $\Delta P \in (efgh\ 0000\ 0000\ 0000)$

    $\Rightarrow n = O(2^{8})$ needed



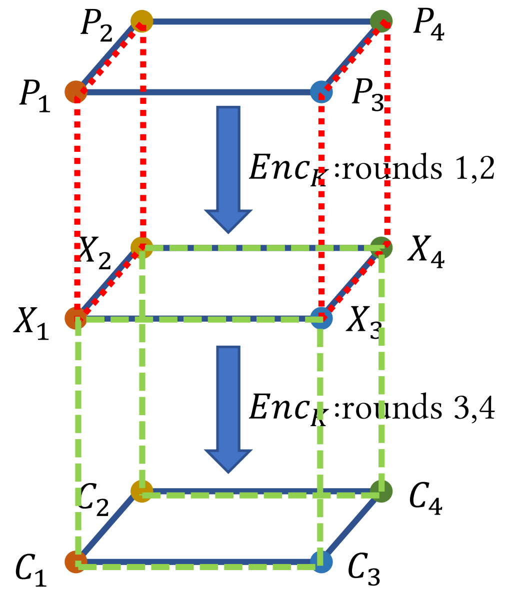
Boomerang distinguishers

- Boomerang distinguishers are based on 2nd order differential cryptanalysis
- Involves 4 PC-pairs: $(P_1, C_1), (P_2, C_2), (P_3, C_3), (P_4, C_4)$
- These are studied in 2 combinations:
  - $(P_1, C_1)\&(P_2, C_2)$ and $(P_3, C_3)\&(P_4, C_4)$ with $P_1 \oplus P_2 = \Delta P$ and $P_3 \oplus P_4 = \Delta P$ for rounds 1 & 2 
  - $(P_1, C_1)\&(P_3, C_3)$ and $(P_2, C_2)\&(P_4, C_4)$ with $C_1 \oplus C_3 = \Delta C$ and $C_2 \oplus C_4 = \Delta C$ for rounds 3 & 4 
  - Note how ΔC is used orthogonal to ΔP



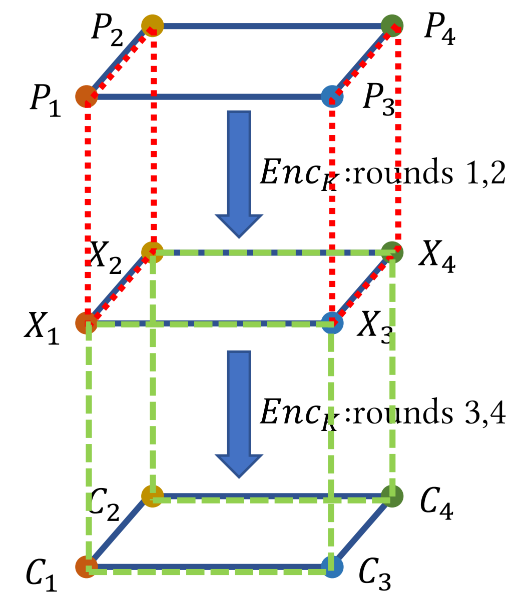
Boomerang distinguishers

- Find two high probability differential relations
  - Rounds 1&2: $\Delta P \rightarrow \Delta O_2$ with probability $p_1 := p_{(\Delta P, \Delta O_2)}$
  - Rounds 3&4: $\Delta I_3 \rightarrow \Delta C$ with probability $p_2 := p_{(\Delta I_3, \Delta C)}$
  - (X, O_2, I_3 describe the same variable, but different names are used to keep the 2 relations apart)
- Two combinations:
  - $(P_1, C_1)\&(P_2, C_2)$ and $(P_3, C_3)\&(P_4, C_4)$
    - with $P_1 \oplus P_2 = \Delta P$ and $P_3 \oplus P_4 = \Delta P$
    - then $X_1 \oplus X_2 = \Delta O_2$ with probability p_1
    - and $X_3 \oplus X_4 = \Delta O_2$ with probability p_1
  - $(P_1, C_1)\&(P_3, C_3)$ and $(P_2, C_2)\&(P_4, C_4)$
    - with $C_1 \oplus C_3 = \Delta C$ and $C_2 \oplus C_4 = \Delta C$
    - then $X_1 \oplus X_3 = \Delta I_3$ with probability p_2
    - and $X_2 \oplus X_4 = \Delta I_3$ with probability p_2



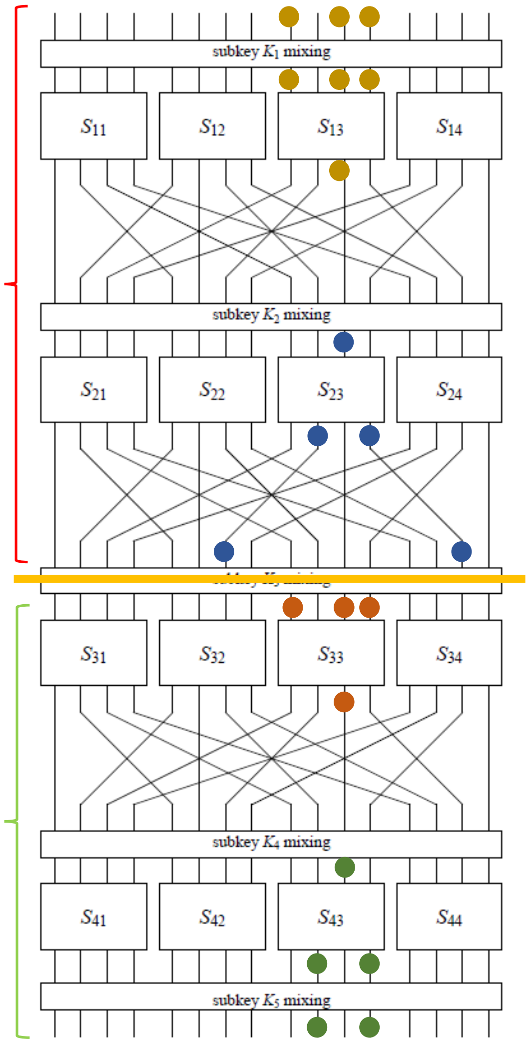
Boomerang distinguishers

- Constructing a boomerang tuple
  1. Pick $P_1 \leftarrow \{0,1\}^{16}$, set $P_2 \coloneqq P_1 \oplus \Delta P$
  2. Ask to encrypt $C_1 \coloneqq Enc(P_1), C_2 \coloneqq Enc(P_2)$
  3. Set $C_3 \coloneqq C_1 \oplus \Delta C$, $C_4 \coloneqq C_2 \oplus \Delta C$
  4. Ask to decrypt $P_3 \coloneqq Dec(C_3)$, $P_4 \coloneqq Dec(C_4)$
  5. Repeat until $P_3 \oplus P_4 = \Delta P$
- Success probability (first approximation):
  - $X_1 \oplus X_2 = \Delta O_2$ with probability p_1
  - $X_1 \oplus X_3 = \Delta I_3$ with probability p_2
  - $X_2 \oplus X_4 = \Delta I_3$ with probability p_2
  - $\Rightarrow X_3 \oplus X_4 = \Delta O_2$ with probability 1
  - $\Rightarrow P_3 \oplus P_4 = \Delta P$ with probability p_1
  - Total probability $p_1^2 \cdot p_2^2$
- Similarly any other choice for ΔO_2 & ΔI_3
  - These are all disjoint events $\Rightarrow$ probabilities add up:
  - $p_{success} = \sum_{\Delta O_2} \sum_{\Delta I_3} p^2_{(\Delta P, \Delta O_2)} \cdot p^2_{(\Delta I_3, \Delta C)}$
- Success probability random oracle:
  - $P_3 \oplus P_4$ is random
  - $\Pr[P_3 \oplus P_4 = \Delta P] = 2^{-N}$



Example Boomerang

- Use the same 2-round differential
  - For round 1&2
  - For round 3&4 (but round 4 does not use π_P)
- 2-round differential:
  - $\Delta I_1, \Delta I_3 = (0000\ 0000\ 1011\ 0000)$
  - S-Box S_{13}, S_{33} active:
    $DDT(1011_b, 0010_b) = DDT(11,2) = 8$
    $\Rightarrow$ probability $1/2$
  - $\Delta I_2, \Delta I_4 = (0000\ 0000\ 0010\ 0000)$
  - S-Box S_{23}, S_{43} active:
    $DDT(0010_b, 0101_b) = DDT(2,5) = 6$
    $\Rightarrow$ probability $3/8$
  - $\Delta O_2 = (0000\ 0010\ 0000\ 0010)$ for rounds 1&2
    or $\Delta C = (0000\ 0000\ 0101\ 0000)$ for rounds 3&4
  - Probability: $3/16$
- Boomerang prob $\geq (3/16)^4 \approx 0.001236 \approx 1/809$
- Measured boomerang prob: ≈ 0.01



Wrap-up

- Differential cryptanalysis variants
  - Any efficient distinguisher is an attack
  - So any easily checkable relation with high probability works
- Truncated differential cryptanalysis
  - Use sets of differences instead of a chosen difference
  - Larger differential probabilities:
    add probabilities of several output differences
- Impossible differential cryptanalysis
  - Use relations that have proven probability 0
  - Distinguisher:
    - When relation is observed ⇒ random oracle / wrong key guess
- Boomerang distinguishers
  - 2^{nd} order differential cryptanalysis: 4 encryptions
  - Find tuple satisfying ΔP for 1-2 & 3-4 and ΔC for 1-3 & 2-4
  - Short & open-ended trails: lots & lots of trails
  - ⇒ very high probability