Multiple Differential Cryptanalysis of Round-Reduced Prince

Anne Canteaut[1], **Thomas Fuhr**[2], Henri Gilbert[2], María Naya-Plasencia[1], Jean-René Reinhard[2]

[1]INRIA, France

[2]ANSSI, France

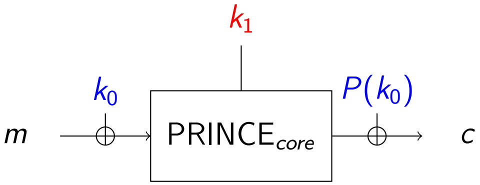
FSE 2014 - March 5, 2014

PRINCE

- Low latency lightweight blockcipher
- Published by Borghoff *et al.* at Asiacrypt 2012
- 64-bit blocks, 128-bit keys
- 12-round SP Network
- Security claim:
  - No attack with $\mathit{Data} \times \mathit{Time} \leq 2^{126}$
  - Due to the specific structure of the cipher

PRINCE - General structure

- FX Construction



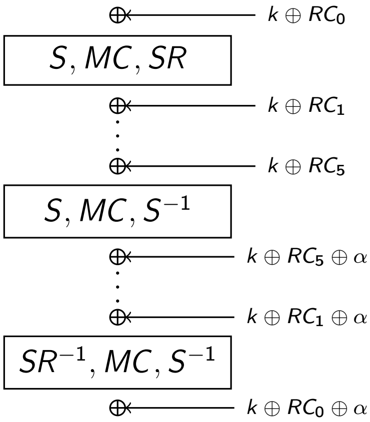
- PRINCE_{core}: Internal keyed permutation using a 64-bit key
- $P(k_0) = (k_0 \ggg 1) \oplus (k_0 \gg 63)$
- $2 \times 64 = 128$-bit key (k_0, k_1)
- Generic attack in $DT = 2^{126}$

Cryptanalyses of PRINCE

- Several related publication
  - [AbedLL12]: Biclique attack on 12 rounds of PRINCE$_{core}$
  - [JeanNPWW13]: integral attack on 6 rounds
  - [SoleimanyBYWNZZW13]: reflection attack on 6 rounds
  - [CanteautNV13]: sieve-in-the-middle on 8 rounds
  - [LiJW13]: meet-in-the-middle on 9 rounds
- Our results
  - 9-round PRINCE: $DT = 2^{98.1}$
  - 10-round PRINCE: $DT = 2^{118.6}$
  - 11-round PRINCE with modified S-box: up to $DT = 2^{122.2}$
  - S-box choice allowed by the designers

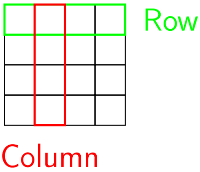
PRINCE$_{core}$ - Description

- No key schedule
- 5 rounds, 2 middle rounds, 5 inverse rounds
  - S: 4 $\rightarrow$ 4 S-box layer
  - MC: Involutive linear diffusion layer
  - SR: Wire-crossing operation
- Use of a constant α
- $E_k = E^{-1}_{k \oplus \alpha}$

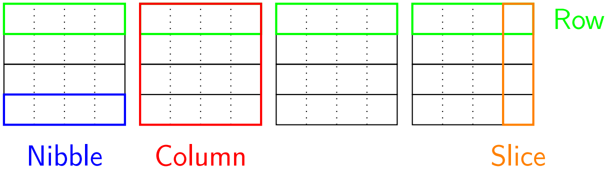


PRINCE block representation

- Representation of the block using a 4×4 nibble array ...



- ... or using a 4×16 bit array



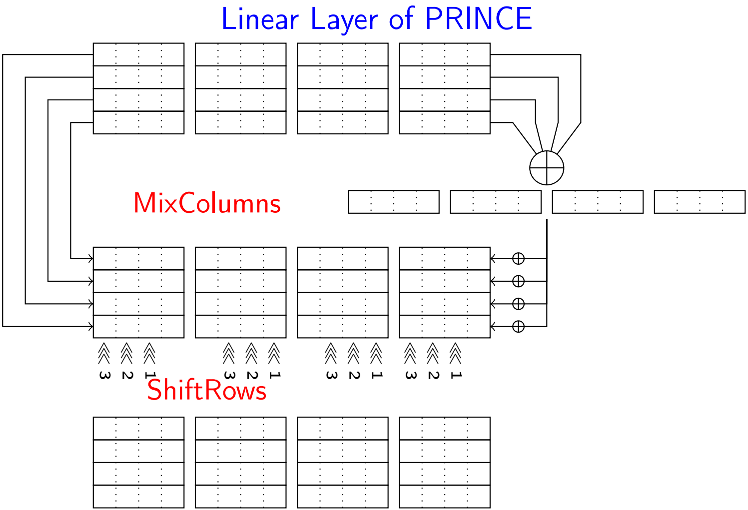
PRINCE_{core} round transformation

- Substitution layer $\mathcal{S}$
  - 16 identical 4-bit to 4-bit S-boxes working on nibbles
  - A specific choice for PRINCE
  - 8 affine equivalent classes allowed by the authors (family of ciphers)
- Linear layer $\mathcal{L}$ composed of
  - Involutive linear diffusion (MixColumns): composition of
    - "Mirror" on the rows: $(r_0, r_1, r_2, r_3) \leftarrow (r_3, r_2, r_1, r_0)$
    - Addition of a parity bit: $r_i \leftarrow r_i \oplus (r_0 \oplus r_1 \oplus r_2 \oplus r_3)$
    - Slice-wise rotations by 0,1,2 or 3 positions
  - Wire-crossing (ShiftRows): similar to AES ShiftRows

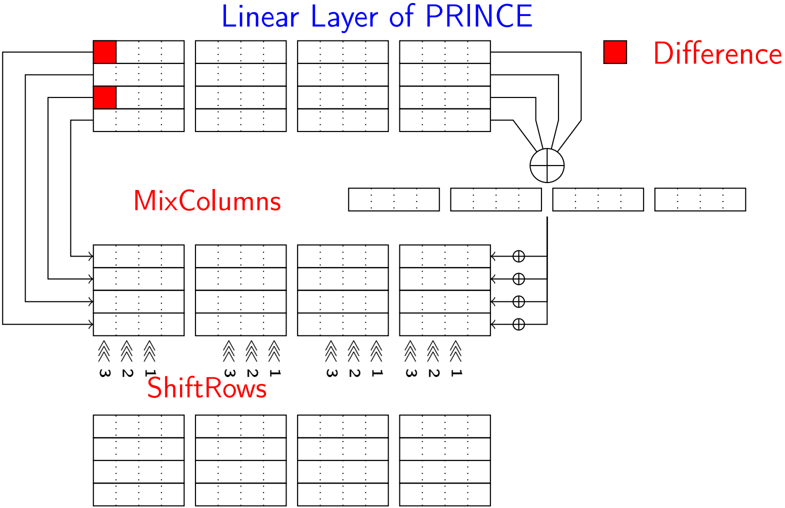
Principle of our attack

- Study of the differential properties of PRINCE$_{core}$
- Aggregation of several differentials on up 6 rounds
  - Cancellation of differences on the parity bits
  - Use of iterative differential patterns
- Extension to a key recovery attack on 10 rounds
- Generalization with different S-boxes

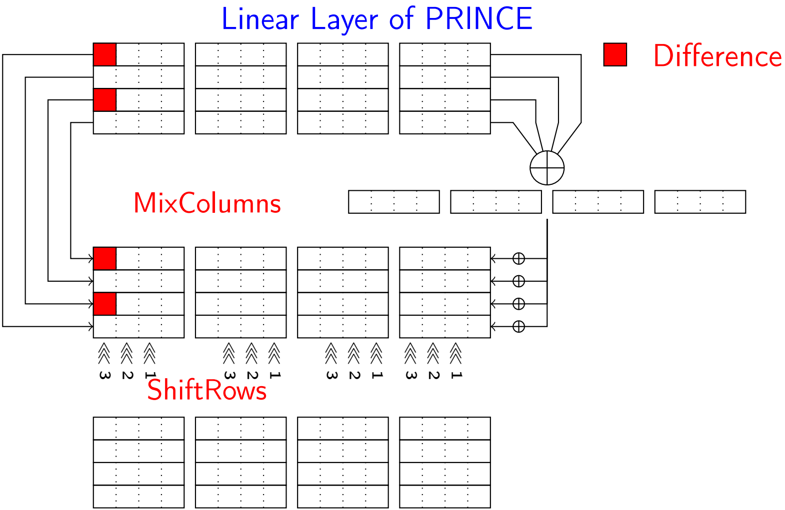
A key observation on differences



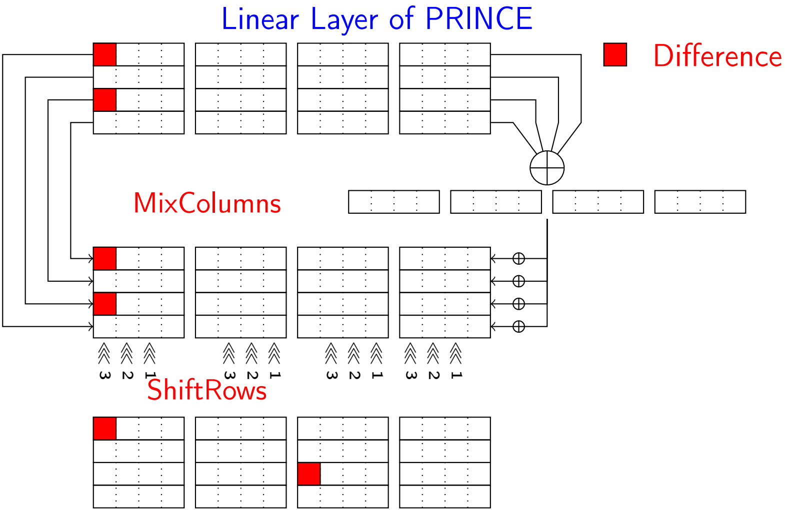
A key observation on differences



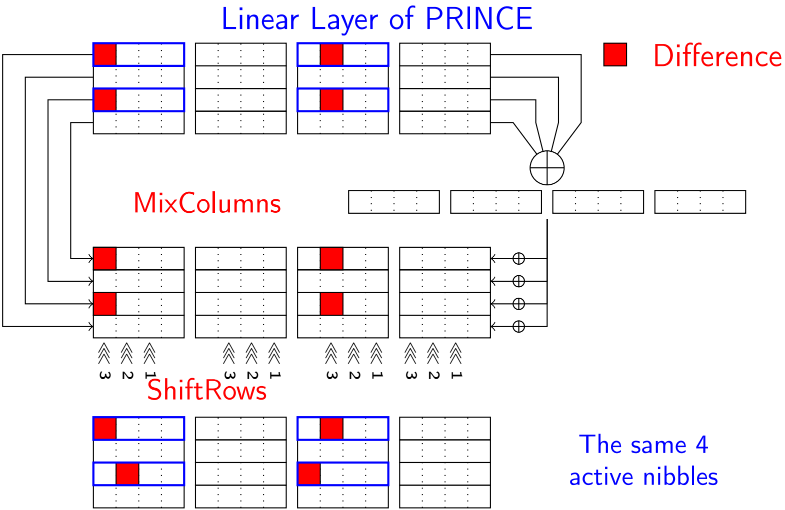
A key observation on differences



A key observation on differences

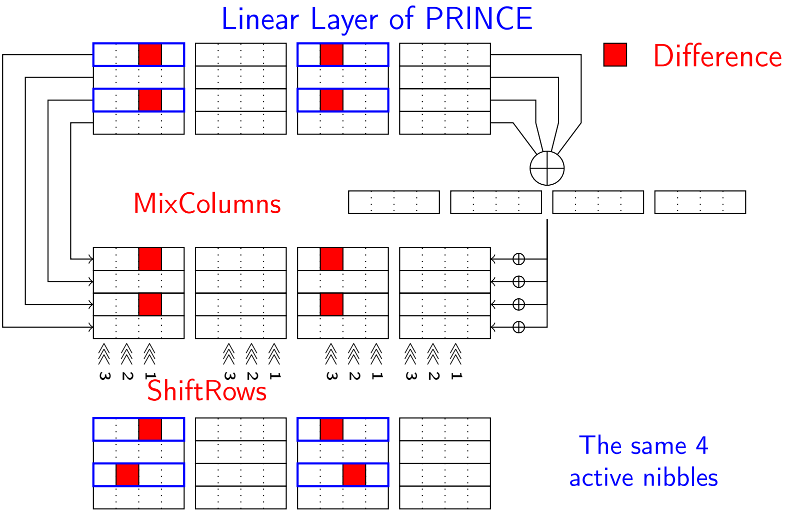


A key observation on differences

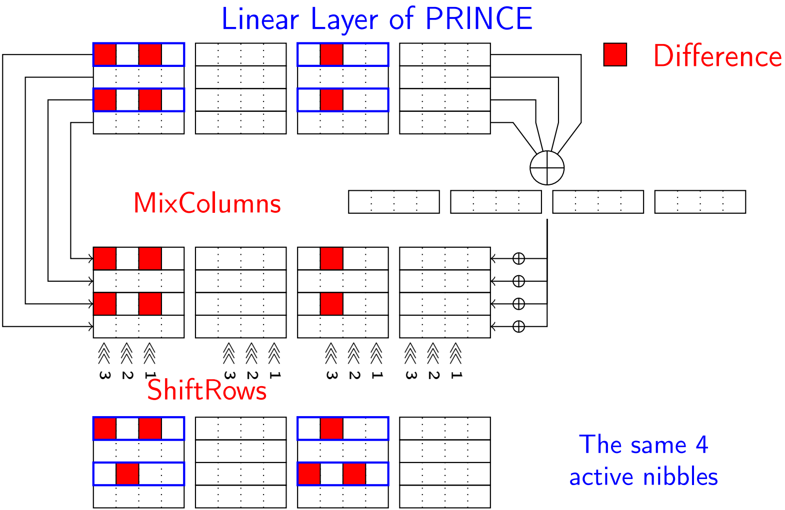


The same 4 active nibbles

A key observation on differences

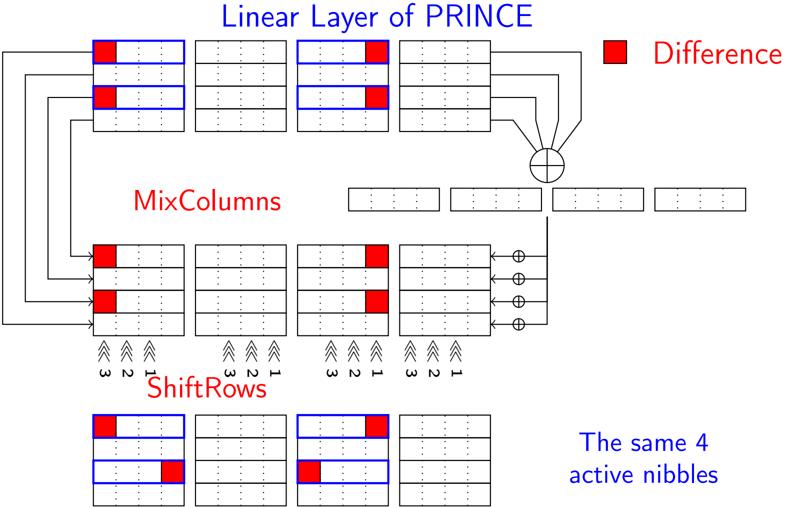


A key observation on differences

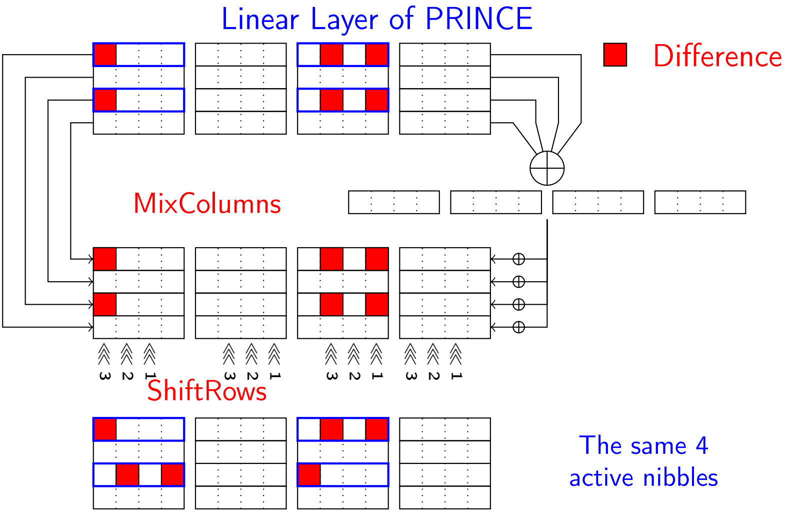


The same 4 active nibbles

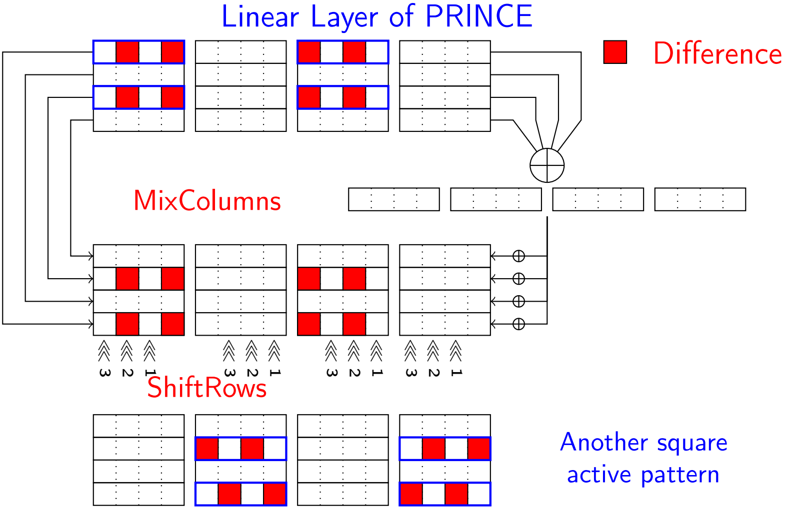
A key observation on differences



A key observation on differences

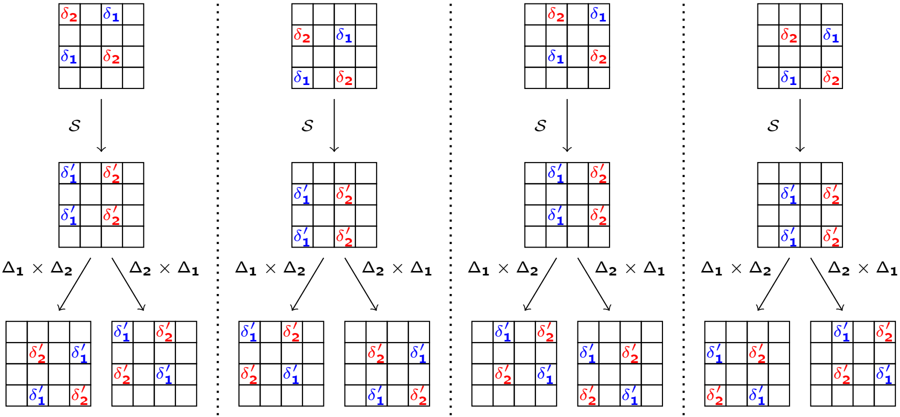


A key observation on differences



1-round differentials on square patterns

- $\delta_1, \delta_2 \in (\Delta_1 \times \Delta_2) \cup (\Delta_2 \times \Delta_1)$ with $\Delta_1 = \{1, 4, 5\}, \Delta_2 = \{2, 8, 10\}$
- 18 admissible differences after each S-box layer



Differentials over several rounds

- On several rounds: aggregation of differential trails on square patterns
- Complexity evaluation
  - Under the classical assumption that round keys are independent
  - Multiplication of probabilities of 1-round differentials
  - Addition of probabilities of aggregated trails
  - Middle rounds: no key addition between 2 S-box layers
    $\Rightarrow$ treated as a layer of 4 S-boxes on 16 bits

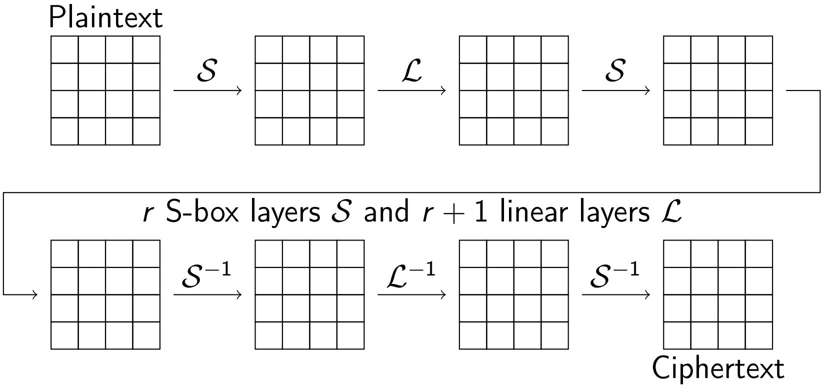
Differentials for round-reduced PRINCE

- Most probable differentials found
  - Original PRINCE: $2^{-47.42}$ on 5 rounds, $2^{-56.42}$ on 6 rounds
  - PRINCE, modified S-box: 2^{-50} on 6 rounds, 2^{-58} on 7 rounds

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S[x]	0	A	6	5	8	D	3	4	7	C	2	E	9	F	B	1

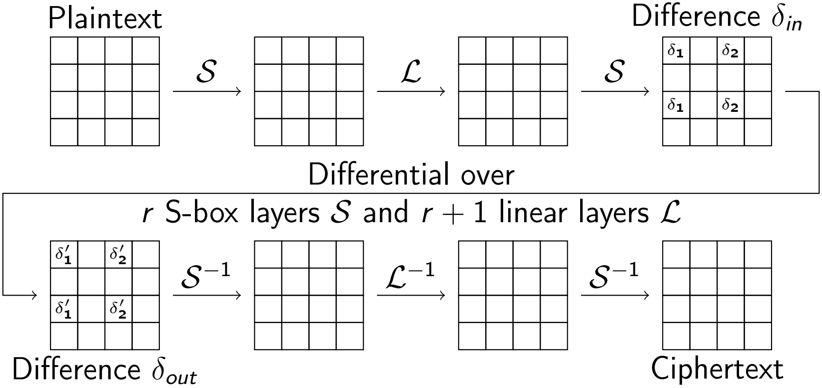
- Experimental validation
  - Random choice of keys
  - Exhaustive search for pairs following one of our differential trails

Extension by four rounds



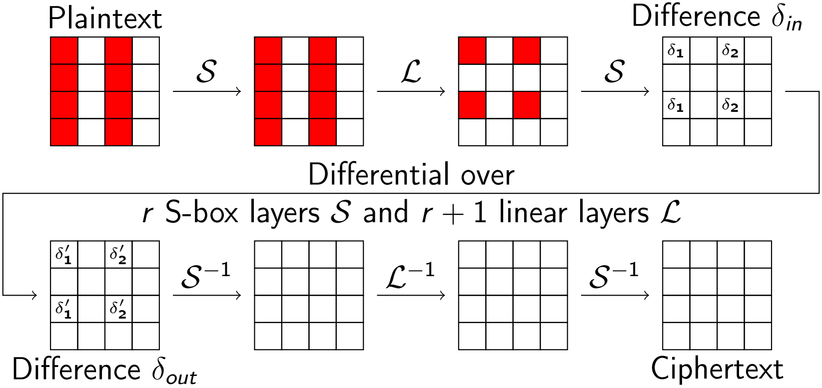
- Key additions do not modify differences
- Observation: no full diffusion after two rounds

Extension by four rounds



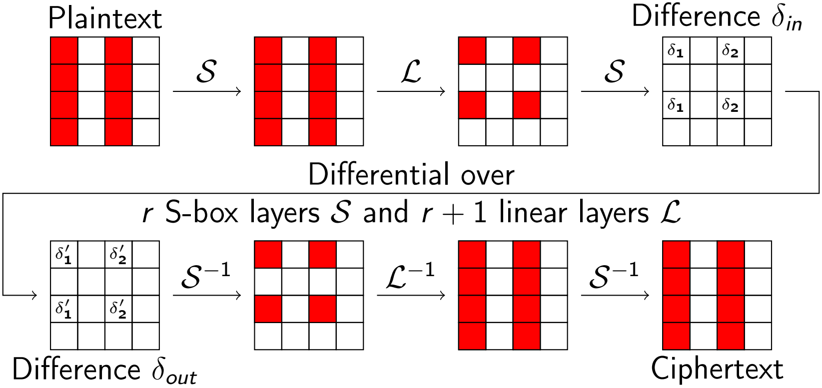
- Key additions do not modify differences
- Observation: no full diffusion after two rounds

Extension by four rounds



- Key additions do not modify differences
- Observation: no full diffusion after two rounds

Extension by four rounds



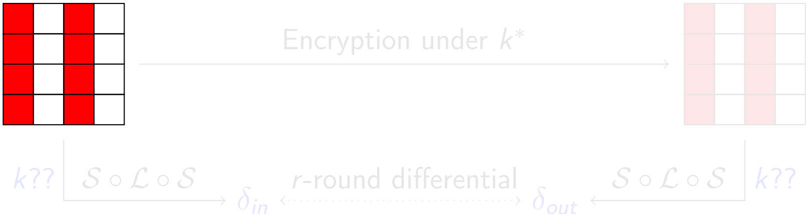
- Key additions do not modify differences
- Observation: no full diffusion after two rounds

A criterion for key recovery

- Input: a differential $(\delta_{in}, \delta_{out})$ and encryption under k^*
- Build structures of 2^{32} plaintexts P_i
  - Exhaustive on columns 0 and 2, fixed value on columns 1 and 3
  - Consider pairs (P_i, P_j) s.t. ciphertexts (C_i, C_j) collide on columns 1 and 3
- In N_s structures: $N_s \times 2^{63} \times 2^{-32} = 2^{31} N_s$ such pairs
- For each key guess k: how many pairs lead to $(\delta_{in}, \delta_{out})$?

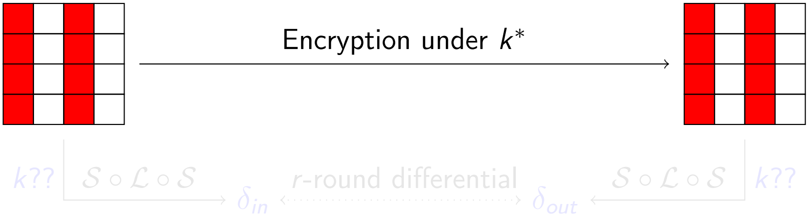
A criterion for key recovery

- Input: a differential $(\delta_{in}, \delta_{out})$ and encryption under k^*
- Build structures of 2^{32} plaintexts P_i
  - Exhaustive on columns 0 and 2, fixed value on columns 1 and 3
  - Consider pairs (P_i, P_j) s.t. ciphertexts (C_i, C_j) collide on columns 1 and 3
- In N_s structures: $N_s \times 2^{63} \times 2^{-32} = 2^{31} N_s$ such pairs
- For each key guess k: how many pairs lead to $(\delta_{in}, \delta_{out})$?



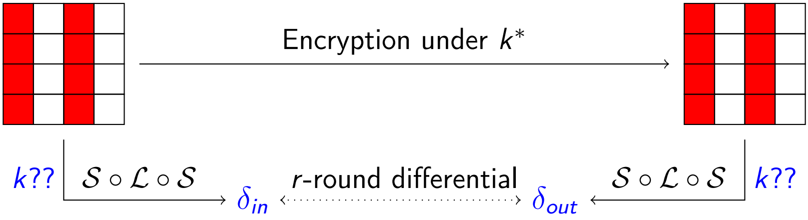
A criterion for key recovery

- Input: a differential $(\delta_{in}, \delta_{out})$ and encryption under k^*
- Build structures of 2^{32} plaintexts P_i
  - Exhaustive on columns 0 and 2, fixed value on columns 1 and 3
  - Consider pairs (P_i, P_j) s.t. ciphertexts (C_i, C_j) collide on columns 1 and 3
- In N_s structures: $N_s \times 2^{63} \times 2^{-32} = 2^{31} N_s$ such pairs
- For each key guess k: how many pairs lead to $(\delta_{in}, \delta_{out})$?



A criterion for key recovery

- Input: a differential $(\delta_{in}, \delta_{out})$ and encryption under k^*
- Build structures of 2^{32} plaintexts P_i
    - Exhaustive on columns 0 and 2, fixed value on columns 1 and 3
    - Consider pairs (P_i, P_j) s.t. ciphertexts (C_i, C_j) collide on columns 1 and 3
- In N_s structures: $N_s \times 2^{63} \times 2^{-32} = 2^{31} N_s$ such pairs
- For each key guess k: how many pairs lead to $(\delta_{in}, \delta_{out})$?



A criterion for key recovery

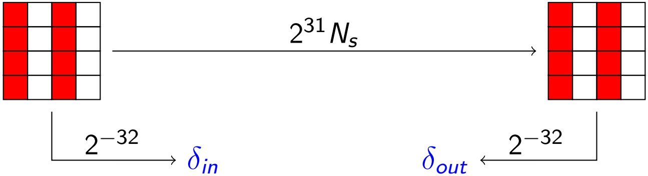
- For a wrong guess:

- For k^*:

- Useful property if $Pr[\delta_{in} \to \delta_{out}] \gg 2^{-64}$

A criterion for key recovery

- For a wrong guess: $2^{-33} N_s$ pairs

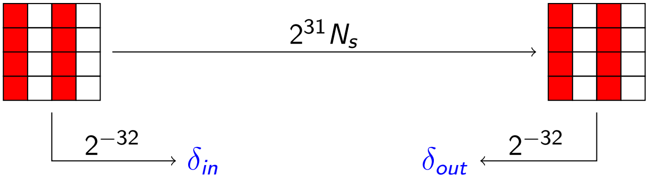


- For k^*:

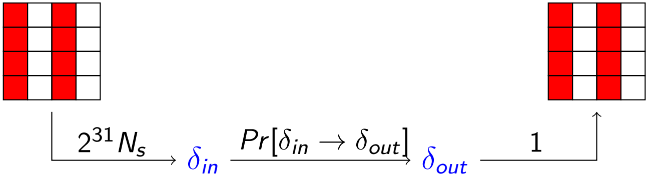
- Useful property if $Pr[\delta_{in} \rightarrow \delta_{out}] \gg 2^{-64}$

A criterion for key recovery

- For a wrong guess: $2^{-33} N_s$ pairs



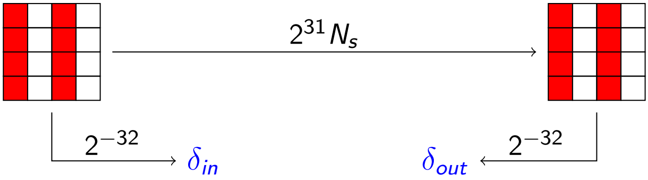
- For k^*: $2^{31} N_s \times Pr[\delta_{in} \rightarrow \delta_{out}]$ pairs



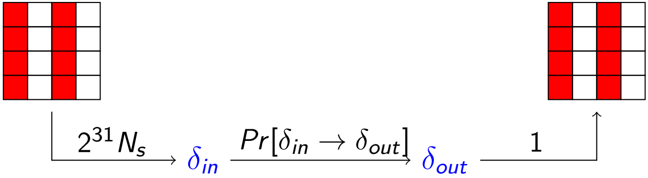
- Useful property if $Pr[\delta_{in} \rightarrow \delta_{out}] \gg 2^{-64}$

A criterion for key recovery

- For a wrong guess: $2^{-33} N_s$ pairs



- For k^*: $2^{31} N_s \times Pr[\delta_{in} \rightarrow \delta_{out}]$ pairs



- Useful property if $Pr[\delta_{in} \rightarrow \delta_{out}] \gg 2^{-64}$

Key recovery - Putting it together

- Only 66 out of 128 bits involved in the guess
- An efficient precomputation-based algorithm to recover 66 bit possible partial keys from (P_i, P_j, C_i, C_j)
- Use of several ($|\delta|$) differentials to limit the amount of data
- A similar distinguisher with differences on columns 1 and 3
  $\rightarrow$ Second iteration of the previous step
- Try all possible keys which score reach some threshold τ in both steps

Our results

- Estimation of the number of remaining wrong keys: based on [BlondeauGerard12]
- Theoretical evaluation, success probability of 0.5 in each selection step

Cipher	Rounds	$\|\delta\|$	τ	Data	Time	Memory	$D \times T$
Original	9	40	3	$2^{46.9}$	$2^{51.2}$	$2^{51.2}$	$2^{98.1}$
Original	10	12	6	$2^{57.9}$	$2^{60.7}$	$2^{60.5}$	$2^{118.6}$
Modified	10	12	3	$2^{50.4}$	$2^{53.6}$	2^{53}	2^{104}
Modified	11	12	8	$2^{59.8}$	$2^{62.4}$	$2^{62.4}$	$2^{122.2}$

- Best known attack on PRINCE
  - Breaks up to 10 rounds of the original cipher
  - and up to 11 rounds for some other S-box choice
- Enlightens that the security margin offered is small