Note on Impossible Differential Attacks

Patrick Derbez

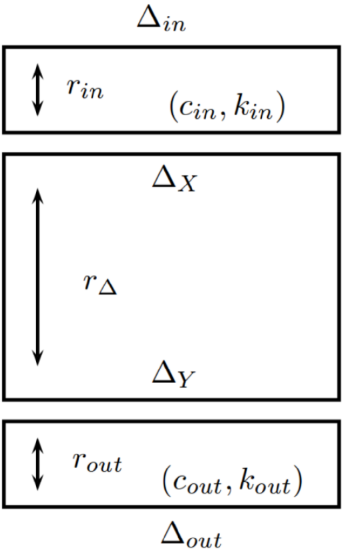
IRISA / University of Rennes 1

March 22, 2016

Outline

Outline for section 1

Impossible Differential Cryptanalysis



Setup

top $P[\Delta_{in} \to \Delta_X] = 2^{-c_{in}}$

middle $P[\Delta_X \to \Delta_Y] = 0$

bottom $P[\Delta_{out} \to \Delta_Y] = 2^{-c_{out}}$

Main idea

If a candidate key partially encrypts/decrypts a given pair to an impossible differential then this key is wrong.

Early Abort Technique Algorithm

Let $k_1, k_2, \ldots, k_b$ be key bits $k_{in} \cup k_{out}$ and σ a permutation.

Early abort

- Discard pairs which cannot follow the impossible differential
- Guess $k_{\sigma(1)}$
- Partially encrypt/decrypt pairs and discard pairs which cannot follow the impossible differential
- Guess $k_{\sigma(2)}$

$$\vdots$$

- Guess $k_{\sigma(b)}$
- Partially encrypt/decrypt pairs and discard pairs which cannot follow the impossible differential
- If all pairs have been discarded then perform an exhaustive search over remaining key bits.

Early Abort Technique Algorithm

Early abort without final exhaustive search - complexity

$$T_\sigma \geq \sum_{1 \leq i \leq b} 2^{|k_{\sigma(1)} \cup \ldots \cup k_{\sigma(i)}| - \sum_{1 \leq j < i} r_j^\sigma} \cdot N \cdot C'_E$$

- N: number of pairs
- r_i^σ: proportion of pairs discarded at step i
- C'_E: ratio of the cost of partial encryption to full encryption

Early Abort Technique Algorithm

Early abort without final exhaustive search - complexity

$$T_\sigma \geq \sum_{1 \leq i \leq b} 2^{|k_{\sigma(1)} \cup \ldots \cup k_{\sigma(i)}| - \sum_{1 \leq j < i} r_j^\sigma} \cdot N \cdot C_E'$$

- N: number of pairs
- r_i^σ: proportion of pairs discarded at step i
- C_E': ratio of the cost of partial encryption to full encryption

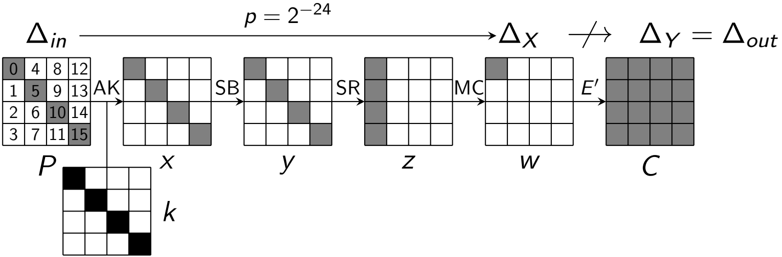
Boura *et al*'s assumption (ASIACRYPT 2014):

$$\min_\sigma T_\sigma \approx (1 + 2^{|k_{in} \cup k_{out}| - c_{in} - c_{out}}) \cdot N \cdot C_E'$$

Outline for section 2

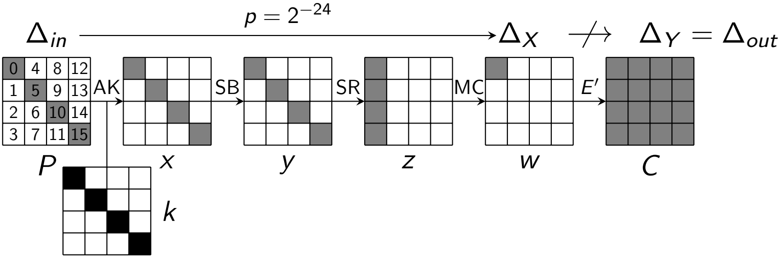
Toy Cipher

- First round based on AES



How key schedule relations do affect time complexity?

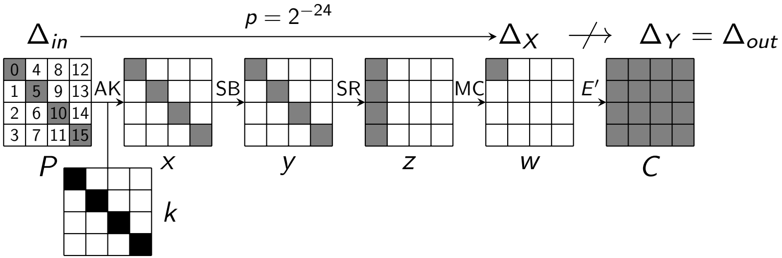
Independent Subkeys



- k_0, k_5, k_{10} and k_{15} independent
- Boura *et al*'s formula:

$$(1 + 2^{|k_{in}| - c_{in}}) \cdot N \cdot C'_E = (1 + 2^{32-24}) \cdot N \cdot 4S_E^{-1} \approx 2^{10} \cdot N \cdot S_E^{-1}$$

Independent Subkeys



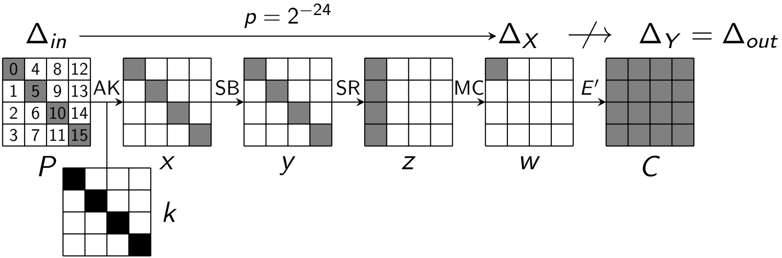
Early abort technique:

- Guess k_0 and keep only pairs for which transitions $\Delta x_5 \to \Delta y_5$, $\Delta x_{10} \to \Delta y_{10}$ and $\Delta x_{15} \to \Delta y_{15}$ are possible
- Guess k_5 and keep only pairs satisfying $\Delta x_5 \to \Delta y_5$
- Guess k_{10} and keep only pairs satisfying $\Delta x_{10} \to \Delta y_{10}$
- Guess k_{15} and keep only pairs satisfying $\Delta x_{15} \to \Delta y_{15}$

Real complexity:

$$(2^8 + 2^{8+8-3} + 2^{8+8+8-3-7} + 2^{8+8+8+8-3-7-7}) \cdot N \cdot S_E^{-1} \approx 2^{15.8} \cdot N \cdot S_E^{-1}$$

Independent Subkeys



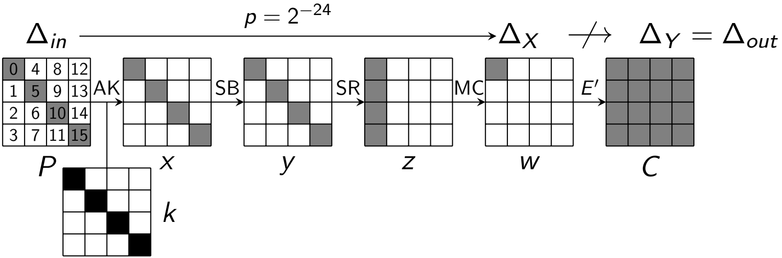
- k_0, k_5, k_{10} and k_{15} independent
- Boura *et al*'s formula:

$$(1+2^{|k_{in}|-c_{in}}) \cdot N \cdot C'_E = (1+2^{32-24}) \cdot N \cdot 4S_E^{-1} \approx 2^{10} \cdot N \cdot S_E^{-1}$$

- Real complexity:

$$(2^8+2^{8+8-3}+2^{8+8+8-3-7}+2^{8+8+8+8-3-7-7}) \cdot N \cdot S_E^{-1} \approx 2^{15.8} \cdot N \cdot S_E^{-1}$$

Related Subkeys I



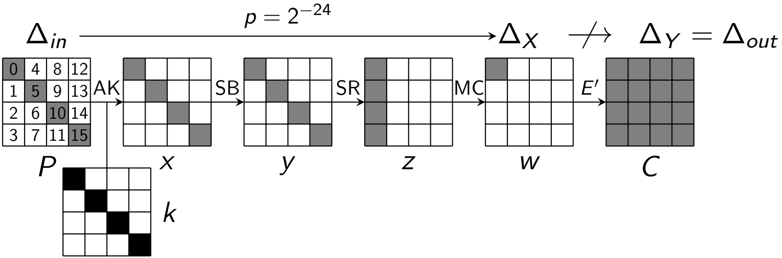
- one key schedule equation: $k_0 = k_5$
- Boura *et al*'s formula:

$$(1 + 2^{|k_{in}| - c_{in}}) \cdot N \cdot C'_E = (1 + 2^{24-24}) \cdot N \cdot 4S_E^{-1} = 2^3 \cdot N \cdot S_E^{-1}$$

- Real complexity:

$$(2^8 + 2^{8-3} + 2^{8+8-3-7} + 2^{8+8+8-3-7-7}) \cdot N \cdot S_E^{-1} \approx 2^{8.9} \cdot N \cdot S_E^{-1}$$

Related Subkeys II



- one key schedule equation: $k_0 \oplus k_5 \oplus k_{10} \oplus k_{15} = 0$
- Boura *et al*'s formula:

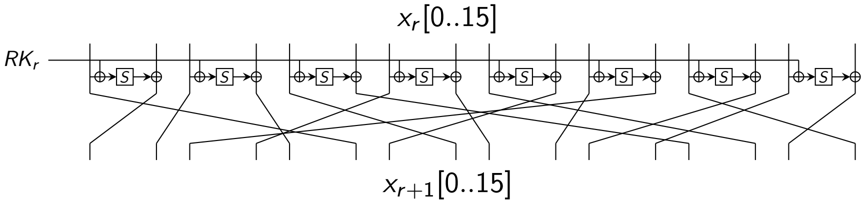
$$(1 + 2^{|k_{in}| - c_{in}}) \cdot NC'_E = (1 + 2^{24-24}) \cdot N \cdot 4S_E^{-1} = 2^3 \cdot N \cdot S_E^{-1}$$

- Real complexity:

$$(2^8 + 2^{8+8-3} + 2^{8+8+8-3-7} + 2^{8+8+8-3-7-7}) \cdot N \cdot S_E^{-1} \approx 2^{14.6} \cdot N \cdot S_E^{-1}$$

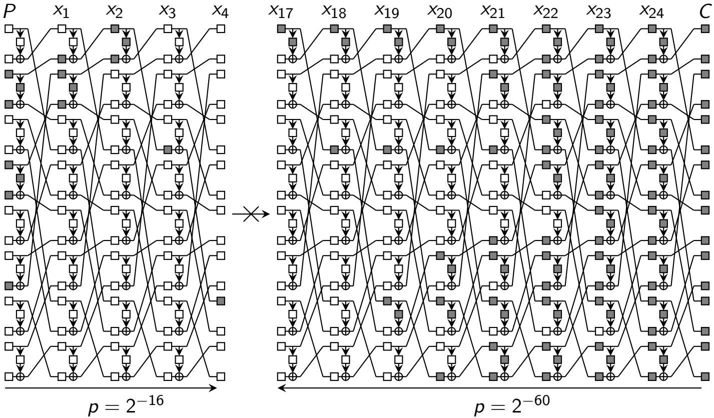
Outline for section 3

TWINE



- Nibble-oriented Feistel
- state size: 64 bits (16 4-bit branches)
- 2 key sizes: 64 and 128 bits

Biryukov et al's attack (FSE 2015)



- 52 subkey nibbles involved but only 2^{124} possible values

Methodology

- 52 subkey nibbles involved $\rightarrow$ $52! \approx 2^{225}$ orders for the early abort technique

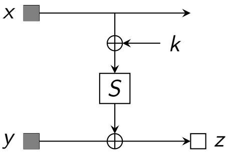
Methodology

- 52 subkey nibbles involved $\rightarrow$ $52! \approx 2^{225}$ orders for the early abort technique

If between two guesses no pairs are discarded then the order in which they are guessed does not matter.

When do pairs are discarded?

Discarding pairs



Proportion of pairs:

- Δx, Δy: probability of transition $\Delta x \to \Delta y \approx 2^{-1}$
- Δx, Δy, $x \oplus k$: 2^{-4}

Exhausting Early Abort Technique

- Biryukov *et al*'s attack:
  - 19 tuples (x, y, z)
    $\rightarrow$ 19 tuples $(\Delta x, \Delta y)$ + 19 tuples $(\Delta x, \Delta y, x \oplus k)$
  - Easy to determine corresponding subkey nibbles
  - But brute force still infeasible:

$$(19 + 19)! = 38! \approx 2^{148}$$

Exhausting Early Abort Technique

- Biryukov *et al*'s attack:
  - 19 tuples (x, y, z)
    $\rightarrow$ 19 tuples $(\Delta x, \Delta y)$ + 19 tuples $(\Delta x, \Delta y, x \oplus k)$
  - Easy to determine corresponding subkey nibbles
  - But brute force still infeasible:

$$(19 + 19)! = 38! \approx 2^{148}$$

- Search:
  - $K_i \subseteq K_j \Rightarrow$ guess K_i before K_j
  - Generic formula:

$$\text{Best}(K_1, \ldots) = \min_i \left(\text{Best}(K_1, \ldots, K_{i-1}, K_{i+1}, \ldots) + 2^{|K_1 \cup \ldots| - \sum_{j \neq i} r(K_j)}\right)$$

Exhausting Early Abort Technique

- Biryukov *et al*'s attack:
  - 19 tuples (x, y, z)
    $\rightarrow$ 19 tuples $(\Delta x, \Delta y)$ + 19 tuples $(\Delta x, \Delta y, x \oplus k)$
  - Easy to determine corresponding subkey nibbles
  - But brute force still infeasible:

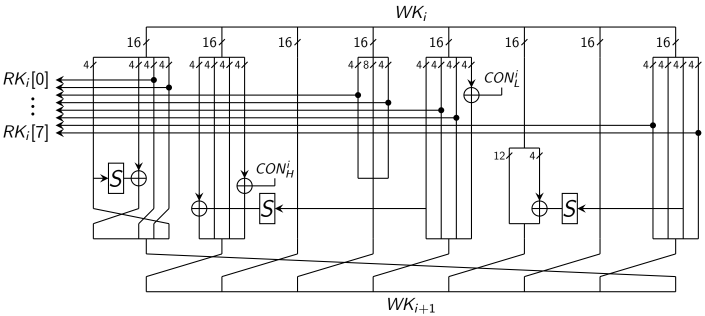
$$(19 + 19)! = 38! \approx 2^{148}$$

- Search:
  - $K_i \subseteq K_j \Rightarrow$ guess K_i before K_j
  - Generic formula:

$$\mathrm{Best}(K_1, \ldots) = \min_i \left(\mathrm{Best}(K_1, \ldots, K_{i-1}, K_{i+1}, \ldots) + 2^{|K_1 \cup \ldots| - \sum_{j \neq i} r(K_j)}\right)$$

How to compute $2^{|K_1 \cup \ldots|}$?

TWINE-128 Key Schedule

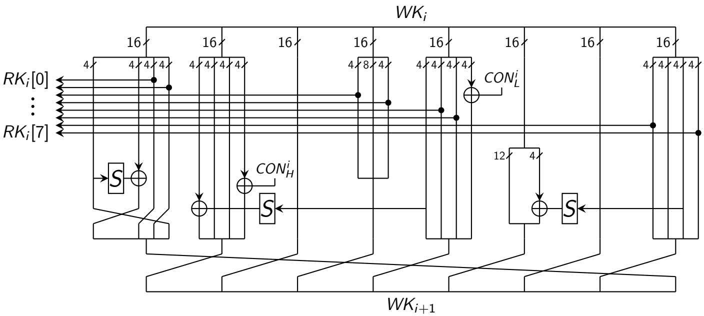


- Shape of key schedule equations:

$$\bigoplus \alpha_i k_i \oplus \beta_i S(k_i) = \gamma,$$

where α_i's, β_i's and γ are constant

TWINE-128 Key Schedule



- Shape of key schedule equations:

$$\bigoplus \alpha_i k_i \oplus \beta_i S(k_i) = \gamma,$$

where α_i's, β_i's and γ are constant
- Use Derbez *et al*'s tool (FSE 2013)

Result

- Computation of real complexity: 1h on personal computer
- Result:

$$\min_{\sigma} T_{\sigma} \geq 2^{54} \cdot N_{\alpha} \cdot C_{E'}$$

- Time complexity of whole attack higher than:

$$C_{N_{\alpha}} + \alpha \cdot 2^{127.6} + 2^{128-\alpha}$$

- Higher than 2^{128} for all $\alpha > 0$.

Outline for section 4

Conclusion

In this paper:

- Boura *et al*'s formula too optimistic
  - reaching it is, if not impossible, very tricky
- Construction of simple counter-examples:
  $\longrightarrow$ deviation up to a factor $2^{11.6}$
- Algorithm computing real complexity for TWINE
  - complexity of Biryukov *et al*'s attack higher than 2^{128}
  - applicable to more ciphers

Open problems:

- Improve the formula
- Find an example with time complexity smaller than expected

Thanks

Thank you for your attention!