Structural Evaluation of AES and Chosen-Key Distinguisher of 9-round AES−128

Pierre-Alain Fouque[1] Jérémy Jean[2] Thomas Peyrin[3]

[1]Université de Rennes 1, France

[2]École Normale Supérieure, France

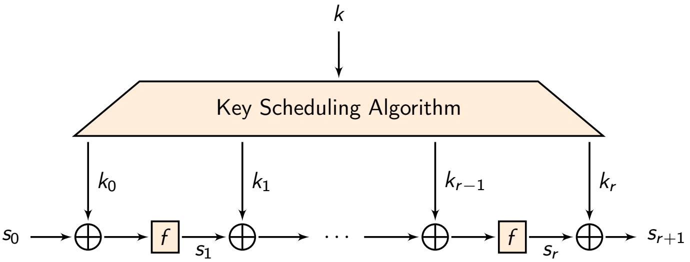
[3]Nanyang Technological University, Singapore

CRYPTO'2013 – August 19, 2013

Block Ciphers

Iterated SPN Block Ciphers

- Internal Permutation : f
- Number of Iterations : r
- SPN : $f = \mathrm{P} \circ \mathrm{S}$ applies Substitution (S) and Permutation (P) layers.
- Secret Key : k
- Key Scheduling Algorithm : $k \to (k_0, \ldots, k_r)$
- Ex : AES, PRESENT, SQUARE, Serpent, etc.

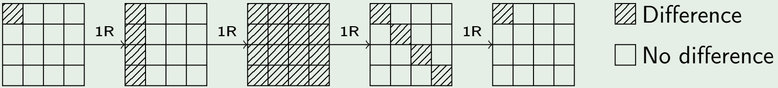


Differentials and Differential Characteristics

Differential Characteristics

- Used in differential cryptanalysis
- Sequence of differences at each round for an iterated primitive
- The success probability of a differential attack depends on the differential with maximal differential probability p.

Example : 4-round AES



- 4-round characteristic with 25 active S-Boxes (minimal).
- AES S-Box : $p_{max} = 2^{-6}$.
- Differential probability : $p \leq 2^{-6\times 25} = 2^{-150}$.

AES

Design of the AES

- AES Permutation : structurally bounded diffusion for any rounds
- Provably resistant to non-RK differential attacks
- Ad-hoc key schedule
  $\Longrightarrow$ RK Attacks [BKN-C09], [BK-A09], [BN-E10].

Minimal Number of Active S-Boxes for AES

Rounds	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
min	1	5	9	25	26	30	34	50	51	55

Question : Similar numbers for AES structure in the RK model ?

Our Contributions

- We propose an algorithm finding all the “smallest” RK characteristics
- It improves previous works : runs in time linear in the number of rounds
- We focus on AES−128
- We provide a distinguisher for 9-round AES−128

Existing Algorithms (1/2)

Matsui's Algorithm (e.g., for DES)

- Works by **induction** :
  derive best *n*-round char. from best chars. on $1, \dots, n-1$ rounds
- Compute best char. for 1R
- Traverse a **tree** of depth 2 for 2R
- Pruning possible (A^* optim.)

Tree Example

$$p_i^j \stackrel{\text{def}}{=} \mathbb{P}(\Delta_i \to \Delta_j)$$

Δ_1

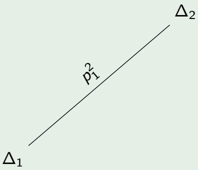
Existing Algorithms (1/2)

Matsui's Algorithm (e.g., for DES)

- Works by **induction** :
  derive best n-round char. from best chars. on $1, \ldots, n-1$ rounds
- Compute best char. for 1R
- Traverse a **tree** of depth 2 for 2R
- Pruning possible (A^* optim.)

Tree Example

$$p_i^j \stackrel{\text{def}}{=} \mathbb{P}(\Delta_i \to \Delta_j)$$



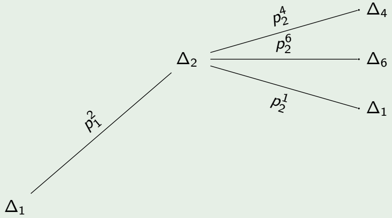
Existing Algorithms (1/2)

Matsui's Algorithm (e.g., for DES)

- Works by **induction** :
  derive best n-round char. from best chars. on $1, \ldots, n-1$ rounds
- Compute best char. for 1R
- Traverse a **tree** of depth 2 for 2R
- Pruning possible (A^* optim.)

Tree Example

$$p_i^j \stackrel{\text{def}}{=} \mathbb{P}(\Delta_i \to \Delta_j)$$



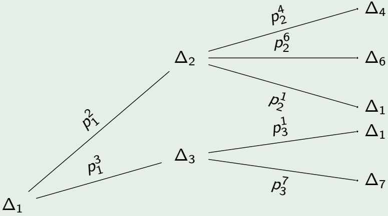
Existing Algorithms (1/2)

Matsui's Algorithm (e.g., for DES)

- Works by **induction** : derive best n-round char. from best chars. on $1, \ldots, n-1$ rounds
- Compute best char. for 1R
- Traverse a **tree** of depth 2 for 2R
- Pruning possible (A^* optim.)

Tree Example

$$p_i^j \stackrel{\text{def}}{=} \mathbb{P}(\Delta_i \to \Delta_j)$$



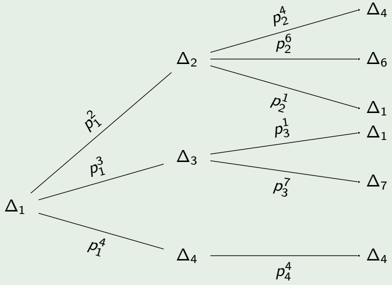
Existing Algorithms (1/2)

Matsui's Algorithm (e.g., for DES)

- Works by **induction** :
  derive best n-round char. from best chars. on $1, \ldots, n-1$ rounds
- Compute best char. for 1R
- Traverse a **tree** of depth 2 for 2R
- Pruning possible (A^* optim.)

Tree Example

$$p_i^j \overset{\text{def}}{=} \mathbb{P}(\Delta_i \to \Delta_j)$$



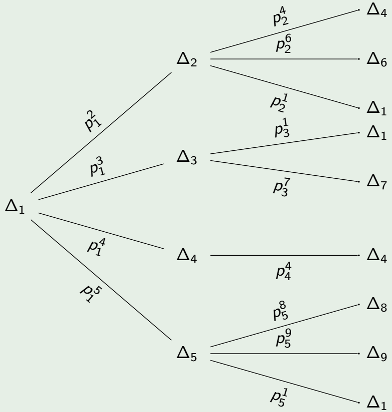
Existing Algorithms (1/2)

Matsui's Algorithm (e.g., for DES)

- Works by **induction** : derive best n-round char. from best chars. on $1, \ldots, n-1$ rounds
- Compute best char. for 1R
- Traverse a **tree** of depth 2 for 2R
- Pruning possible (A^* optim.)

Tree Example

$$p_i^j \stackrel{\text{def}}{=} \mathbb{P}(\Delta_i \to \Delta_j)$$



Existing Algorithms (1/2)

Matsui's Algorithm (e.g., for DES)

- Works by **induction** : derive best n-round char. from best chars. on $1, \dots, n-1$ rounds
- Compute best char. for 1R
- Traverse a **tree** of depth 2 for 2R
- Pruning possible (A^* optim.)

Pros

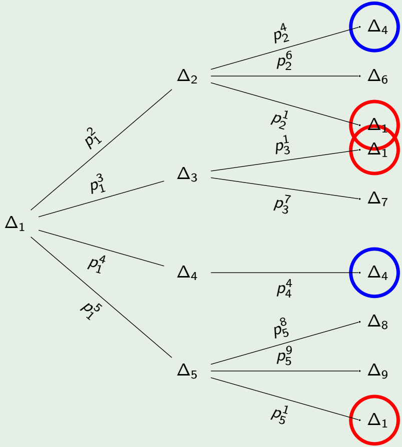
- Very efficient on DES

Drawbacks

- Rely on non-equivalent differential probabilities
- Need for dominant characteristic(s)
- Poor performances for AES
- Differences visited several times

Tree Example

$$p_i^j \overset{\text{def}}{=} \mathbb{P}(\Delta_i \to \Delta_j)$$



Existing Algorithms (2/2)

Biryukov-Nikolic [BN-E10]

- Adapt Matsui's algorithm
- Different algos for several KS

Pros

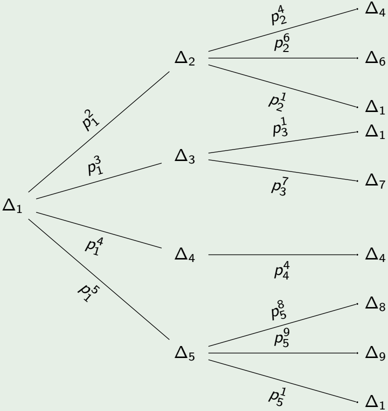
- No need for a predominant char.
- Switch to truncated differences
  $\Longrightarrow$ less edges
- Representation of trunc. differences
  $\Longrightarrow$ handle branching in the KS
- Work on AES

Cons

- Differences visited several times
- Nodes visited exponential in the number of rounds

Tree Example

$$p_i^j \stackrel{\text{def}}{=} \mathbb{P}(\Delta_i \to \Delta_j)$$

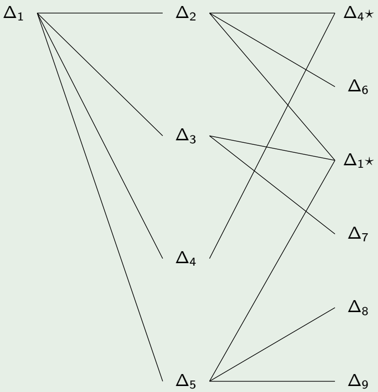


Our Algorithm

Algorithm

- Switch to a graph representation

Graph Example

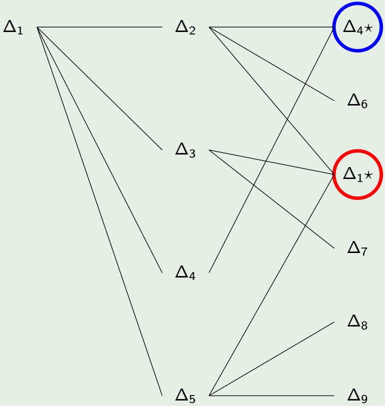


Our Algorithm

Algorithm

- Switch to a graph representation
- Merge equal diff. of the same round

Graph Example

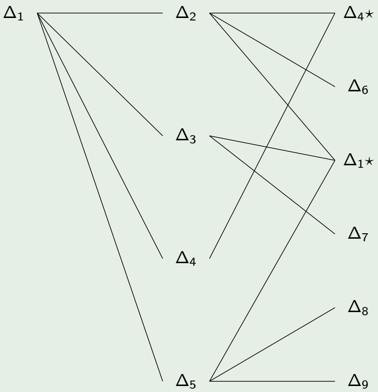


Our Algorithm

Algorithm

- Switch to a graph representation
- Merge equal diff. of the same round
- Graph traversal similar as Dijkstra
- Dynamic programming approach

Graph Example



Our Algorithm

Algorithm

- Switch to a graph representation
- Merge equal diff. of the same round
- Graph traversal similar as Dijkstra
- Dynamic programming approach

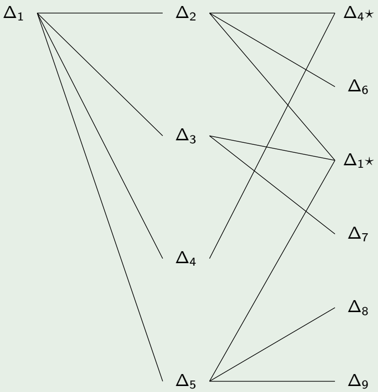
Pros

- Path search seen as Markov process
- Each difference in each round is visited only once
- Numbers of nodes and edges are linear in the number of rounds
- A^* optimization still applies

Notes

- Only partial information propagated
- Need to adapt the Markov process

Graph Example



Different Levels of Analysis

Truncated Differences

- Basic Markov process
- Apply to any SPN cipher : we focus on AES-like ciphers
- Provide a structural evaluation of the cipher in regard to RK attacks
- For AES, similar results as the seminal work [DR-02] (for non-RK)

Actual Differences

- Enhanced Markov process :
  - More complete representation of differences
  - Add information for local system resolutions
- Need to be adapted to a particular cipher
- For AES, recover all the truncated results from [BN-E10]
- Full instantiation of characteristics while maximizing its probability
- Running time linear in the number of rounds

In reality : Mixing the two concepts

Application to the Structure of AES−128

Structural Analysis

- We ignore the semantic definition of the S-Box and the MDS matrix
- We count the number of active S-Boxes (truncated differences)
- Do not apply to AES−128 with the instantiated S and P
- Give an estimation of the structural quality of the AES family

Related-Key Model (XOR difference of the keys)

Rounds	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
min	0	1	3	9	11	13	15	21	23	25

Impossibility Results for the Structure of AES−128 (1/2)

There exists a characteristic on 10 rounds with only 25 active S-Boxes
$\Longrightarrow$ best RK differential attack in p_{max}^{-25} computations.

Result 1

It is impossible to prove the security of the full AES−128 against **related-key differential attacks** without considering the differential property of the S-Box.

Notes

- With a random S-Box, p_{max}^{-25} might be smaller than 2^{128}
  $\Longrightarrow$ when $p_{max} \geq 2^{-5}$
- AES structure on its own not enough for RK security
- For a specified S-Box with bounded $p_{max} \leq 2^{-6}$
  $\Longrightarrow$ security against RK attacks

Impossibility Results for the Structure of AES-128 (2/2)

There exists a characteristic on 8 rounds with only 21 active S-Boxes
$\Longrightarrow$ best RK differential attack in p_{max}^{-21} computations.

Result 2

It is impossible to prove the security of 8-round AES-128 against **related-key differential attacks** without considering both the differential property of the S-Box and the P layer.

Notes

- With a random S-Box, same reason as before
- For a specified S-Box with bounded $p_{max} \leq 2^{-6}$:
  - Best attack might be $2^{6\times 21} = 2^{126} \leq 2^{128}$
  - For AES, we have exhausted all the possible attacks, no valid one
  - P layer and KS introduce linear dependencies in the characteristic
  - P can be chosen such that there is/isn't solutions

Related-Key attacks on AES−128

RK attacks against AES−128

- After 6 rounds, there is no RK characteristic for AES−128 with a probability greater than 2^{-128}.
- For $1, \ldots, 5$ rounds, our algorithm has found the best characteristics
- Same truncated characteristics as [BN-E10]
- Best instantiations of differences : maximal probabilities.

Best RK attacks on AES−128

Rounds	**1**	**2**	**3**	**4**	**5**
#S-Boxes	0	1	5	13	17
[BN-E10]	0	-6	-30	-78	-102
$\max \log_2(p)$	0	-6	-31	-81	-105

Distinguishing model [KR-A07, BKN-C09]

Solve Open-Problem

We can use the best 5-round characteristic to construct a chosen-key distinguisher for 9-round AES−128.

Let $\mathcal{E}_k$ be the 9-round AES−128 block cipher using key k.

Limited Birthday Problem [GP-FSE10]

Given

- a fully instantiated difference δ in the key,
- a partially instantiated difference Δ_{IN} in the plaintext,
- a partially instantiated difference Δ_{OUT} in the ciphertext,

find

- a key k,
- a pair of messages (m, m'),

such that :

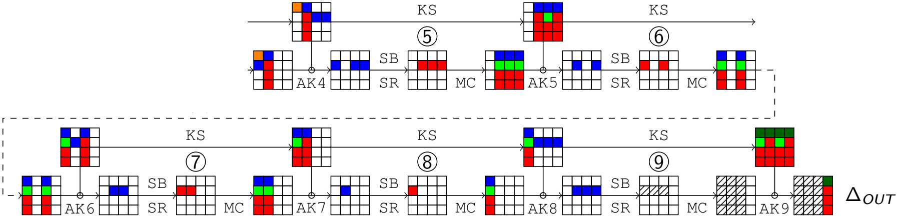
$$m \oplus m' \in \Delta_{IN}$$

$$\text{and : } \mathcal{E}_k(m) \oplus \mathcal{E}_{k \oplus \delta}(m') \in \Delta_{OUT}.$$

9-Round characteristic for AES−128

Construction of the characteristic

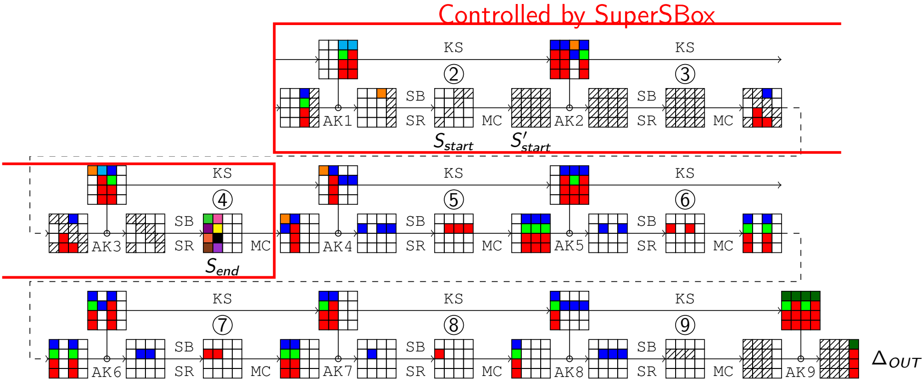
Take the best 5-round characteristic for AES−128 we have found.



9-Round characteristic for AES−128

Construction of the characteristic

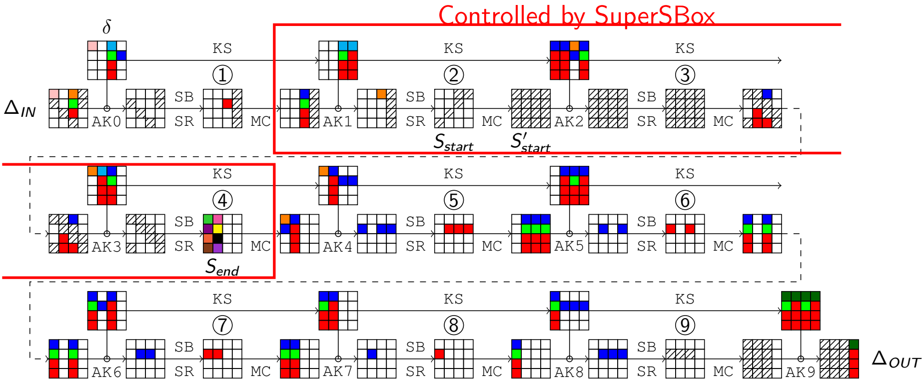
Prepend three rounds to be controlled by the SuperSBox technique.



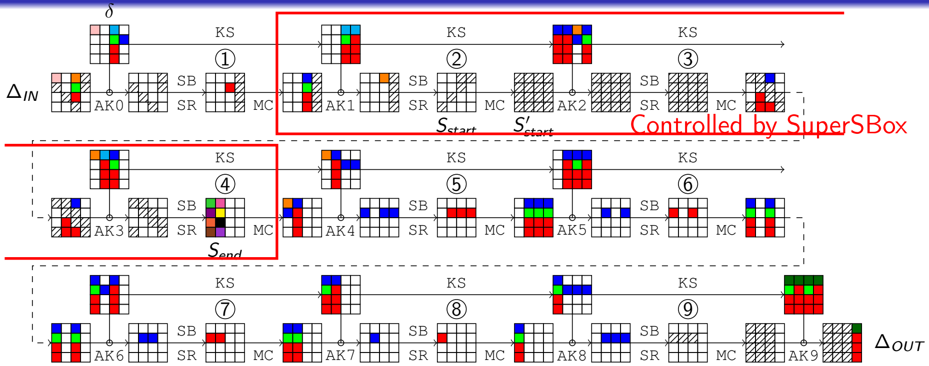
9-Round characteristic for AES−128

Construction of the characteristic

Prepend one other round, as inactive as possible.



9-Round CK Distinguisher for AES−128



Distinguishing algorithm

- Generate a valid pair of keys (about 2^{27} of them, since $\mathbb{P}_{KS} = 2^{-101}$)
  - Store the ith SuperSBox from S'_{start} to S_{end} in T_i
  - For all 5 differences at S_{start}, check the tables and :
    - Check backward direction : $p = 2^{-7}$ (a single S-Box)
    - Check forward direction : $p = 2^{-6\times 8} = 2^{-48}$ (6 S-Boxes)

Time complexity

Complexity of the distinguishing algorithm

- Check probability : $2^{-7-48} = 2^{-55}$
- Time complexity :

$$2^{15} \times (2^{32} + 2^{40}) \approx 2^{55} \text{ computations}$$

- For 2^{15} different pairs of keys :
  - Construct the SuperSBoxes in 2^{32} operations
  - Try all values for the 5 byte-differences in 2^{40} operations

Generic time complexity

- Limited-Birthday Problem [GP-FSE10]
- Input space (Δ_{IN}) of size $4 \times 8 + 7 = 39$ bits
- Output space (Δ_{OUT}) of size $3 \times 7 = 21$ bits
- Time complexity : 2^{68} encryptions

Conclusion

- New algorithm for SPN ciphers
  - Graph-based approach : Dijkstra and A^* optimization
  - Search the best truncated differential characteristics
  - Instantiation $\Longrightarrow$ best differential characteristics
  - Time complexity linear in the number of rounds considered
- Applications to the structure of AES−128 :
  - Impossibility results for related-key attacks
  - Impossibility results for the hash function setting
- Chosen-key distinguisher for 9-rounds AES−128
  - Solve open problem
  - Time Complexity : 2^{55} encryptions
  - Generic Complexity : 2^{68} encryptions
- More details in the paper and its extended version (ePrint/2013/366)

Conclusion

- New algorithm for SPN ciphers
  - Graph-based approach : Dijkstra and A^* optimization
  - Search the best truncated differential characteristics
  - Instantiation $\Longrightarrow$ best differential characteristics
  - Time complexity linear in the number of rounds considered
- Applications to the structure of AES−128 :
  - Impossibility results for related-key attacks
  - Impossibility results for the hash function setting
- Chosen-key distinguisher for 9-rounds AES−128
  - Solve open problem
  - Time Complexity : 2^{55} encryptions
  - Generic Complexity : 2^{68} encryptions
- More details in the paper and its extended version (ePrint/2013/366)

Thank you !

Thanks to the organizing committee and sponsors for waiving my registration fee.