The Phantom of Differential Characteristics

Yunwen Liu

joint work with Bing Sun, Guoqiang Liu, Chao Li and Shaojing Fu

ESAT/COSIC, KU Leuven, and imec, Belgium
National University of Defense Technology, China

ASK, December 2017
Motivation

For various application scenarios, we often assume the ability of an attacker to control the keys:

- Single-key model
- Open-key model
- Related-key attack
- Weak-key attack
- Known-key attack
Motivation

**Distinguisher**  +
Motivation

Distinguisher + Attack
For various application scenarios, we often assume the ability of an attacker to control the keys:
Motivation

**Distinguisher** + **Attack**

For various application scenarios, we often assume the ability of an attacker to control the keys:

- Single-key model
Motivation

\[ \textbf{Distinguisher} \quad + \quad \textbf{Attack} \]

For various application scenarios, we often assume the ability of an attacker to control the keys:

- Single-key model
- Open-key model
Motivation

**Distinguisher** + **Attack**

For various application scenarios, we often assume the ability of an attacker to control the keys:

- Single-key model
- Open-key model
  - related-key attack
  - weak-key attack
  - known-key attack
Motivation

Differential cryptanalysis
Motivation

Differential cryptanalysis

- One of the most extensively studied cryptanalytic techniques

\[
x \oplus \delta \\
E_k \\
y \\
y \oplus \Delta
\]
Motivation

Differential cryptanalysis

- One of the most extensively studied cryptanalytic techniques
- Track probabilistic difference propagation

\[
x \oplus \delta \quad \quad E_k \quad \quad y \oplus \Delta
\]
Motivation

Differential cryptanalysis

- One of the most extensively studied cryptanalytic techniques
- Track probabilistic difference propagation
- Differential characteristics and differentials
Motivation

Differential cryptanalysis

- One of the most extensively studied cryptanalytic techniques
- Track probabilistic difference propagation
- Differential characteristics and differentials
- Distinguish from random and key recovery
Motivation

An attacker wants to know

- probability of a differential \((\delta, \Delta)\) under a secret key \(k\)
Motivation

An attacker wants to know

- probability of a differential \( (\delta, \Delta) \) under a secret key \( k \)
Motivation

An attacker wants to know

- probability of a differential \((\delta, \Delta)\) under a secret key \(k\)
- expected probabilities of a differential \((\delta, \Delta)\) over all master keys
Motivation

An attacker wants to know

- probability of a differential \((\delta, \Delta)\) under a secret key \(k\)
- expected probabilities of a differential \((\delta, \Delta)\) over all master keys
Motivation

An attacker wants to know

- probability of a differential \((\delta, \Delta)\) under a secret key \(k\)
- expected probabilities of a differential \((\delta, \Delta)\) over all master keys
- sum on the expected probabilities of all or some characteristics in a differential \((\delta, \Delta)\) over all random round keys

Assumptions

- Markov cipher
- Independently random round keys
- Hypothesis of stochastic equivalence
Motivation

An attacker wants to know

- probability of a differential \((\delta, \Delta)\) under a secret key \(k\)
- expected probabilities of a differential \((\delta, \Delta)\) over all master keys
- sum on the expected probabilities of all or some characteristics in a differential \((\delta, \Delta)\) over all random round keys

Assumptions

- Markov cipher
- Independently random round keys
- Hypothesis of stochastic equivalence
Motivation

With the assumptions, it allows to
Motivation

With the assumptions, it allows to

- estimate the averaged strength of a distinguisher
Motivation

With the assumptions, it allows to

- estimate the averaged strength of a distinguisher
- provable resistance against differential cryptanalysis
Motivation

With the assumptions, it allows to

- estimate the averaged strength of a distinguisher
- provable resistance against differential cryptanalysis
- guideline for designs
Motivation

With the assumptions, it allows to

- estimate the averaged strength of a distinguisher
- provable resistance against differential cryptanalysis
- guideline for designs

However, an attacker targets on one secret key.
Motivation

With the assumptions, it allows to

- estimate the averaged strength of a distinguisher
- provable resistance against differential cryptanalysis
- guideline for designs

However, an attacker targets on one secret key.

- The probability of a differential distinguisher determines the attack complexity
Motivation

With the assumptions, it allows to

- estimate the averaged strength of a distinguisher
- provable resistance against differential cryptanalysis
- guideline for designs

However, an attacker targets on one secret key.

- The probability of a differential distinguisher determines the attack complexity
- Differential or impossible differential?
Motivation

Discrepancy observed in previous works:


Motivation

Discrepancy observed in previous works:

- ARX ciphers:

Motivation

Discrepancy observed in previous works:

- ARX ciphers:
  - Differential cryptanalysis on ARX-based hash functions, see for instance [Leu12]


Motivation

Discrepancy observed in previous works:

- **ARX ciphers:**
  - Differential cryptanalysis on ARX-based hash functions, see for instance [Leu12]
  - Rotational cryptanalysis [KNP+15]
Motivation

Discrepancy observed in previous works:

- ARX ciphers:
  - Differential cryptanalysis on ARX-based hash functions, see for instance [Leu12]
  - Rotational cryptanalysis [KNP+15]

- Plateau characteristics [DR07]
Motivation

Discrepancy observed in previous works:

- **ARX ciphers:**
  - Differential cryptanalysis on ARX-based hash functions, see for instance [Leu12]
  - Rotational cryptanalysis [KNP+15]

- Plateau characteristics [DR07]

- Refined differential probability with key being zero [CLN+17]
Motivation

Discrepancy observed in previous works:

- **ARX ciphers:**
  - Differential cryptanalysis on ARX-based hash functions, see for instance [Leu12]
  - Rotational cryptanalysis [KNP+15]
- **Plateau characteristics** [DR07]
- **Refined differential probability with key being zero** [CLN+17]
- ...
Motivation

Independently random keys

To what extent can we rely on the Assumptions?
Motivation

Independently random keys

To what extent can we rely on the Assumptions?
Enumerate characteristics under the Assumptions:
Motivation

Enumerate characteristics under the Assumptions:

For a fixed key, $# \text{ characteristics} = 2^{15}$

Under the Assumptions, $# \text{ characteristics} = 2^8 \times 2^7 \times \cdots \times 2^7 = 2^{7r + 8}$

A characteristic generated under the Assumptions is "almost" impossible in reality.
Motivation

Enumerate characteristics under the Assumptions:

For a fixed key, \# characteristics = $2^{15}$

- For a fixed key, \# characteristics = $2^{15}$
Enumerate characteristics under the Assumptions:

- For a fixed key, \# characteristics = $2^{15}$
- Under the Assumptions, \# characteristics = $2^8 \times 2^7 \times \cdots \times 2^7 = 2^{7r+8}$
Motivation

Enumerate characteristics under the Assumptions:

- For a fixed key, \( \# \) characteristics = \( 2^{15} \)
- Under the Assumptions, \( \# \) characteristics = \( 2^8 \times 2^7 \times \cdots \times 2^7 = 2^{7r+8} \)
- A characteristic generated under the Assumptions is “almost” impossible in reality.
Motivation

To study differential probability in fixed-key block ciphers and permutations
It is crucial to ask:
Motivation

To study differential probability in fixed-key block ciphers and permutations
It is crucial to ask:
- EDP ≠ 0 while DP = 0 for all keys?
Motivation

To study differential probability in fixed-key block ciphers and permutations

It is crucial to ask:

- $\text{EDP} \neq 0$ while $\text{DP} = 0$ for all keys?
- Differential characteristics enumeration?
Motivation

To study differential probability in fixed-key block ciphers and permutations.
It is crucial to ask:

- $\text{EDP} \neq 0$ while $\text{DP} = 0$ for all keys?
- Differential characteristics enumeration?
- Characteristics-based attacks?
Motivation

To study differential probability in fixed-key block ciphers and permutations
It is crucial to ask:

- $\text{EDP} \neq 0$ while $\text{DP} = 0$ for all keys?
- Differential characteristics enumeration?
- Characteristics-based attacks?
- Compute $\text{DP}$ under any given key?
To study differential probability in fixed-key block ciphers and permutations
It is crucial to ask:

■ $\text{EDP} \neq 0$ while $\text{DP} = 0$ for all keys?
■ Differential characteristics enumeration?
■ Characteristics-based attacks?
■ Compute $\text{DP}$ under any given key?
■ Design better key schedules and/or constants?
Effective Keys and Singular Characteristics

Differential probability is dependent on the key. Characteristics with zero or nonzero probability are considered effective keys. A key is effective for a characteristic if the characteristic is of nonzero probability under the key. If no effective key exists, it is called a singular characteristic.
Effective Keys and Singular Characteristics

- Differential probability is dependent on the key.
Effective Keys and Singular Characteristics

- Differential probability is dependent on the key
- Characteristics with zero or nonzero probability
Effective Keys and Singular Characteristics

- Differential probability is dependent on the key
- Characteristics with zero or nonzero probability

Effective keys

A key is effective for a characteristic if the characteristic is of nonzero probability under the key.
Effective Keys and Singular Characteristics

- Differential probability is dependent on the key
- Characteristics with zero or nonzero probability

**Effective keys**

A key is effective for a characteristic if the characteristic is of nonzero probability under the key.

If no effective key exists, it is called a *singular characteristic*.
Effective Keys

- SPN cipher with keys XORed after the linear layer

\[ k = P_x \oplus y \]
Effective Keys

- SPN cipher with keys XORed after the linear layer
- Right output and right input of the Sboxes
Effective Keys

- SPN cipher with keys XORed after the linear layer
- Right output and right input of the Sboxes
- Effective key candidates: $k = Px \oplus y$
Singular Characteristics

When the difference propagation is legal, the effective key set of a 2-round characteristic is non-empty. Effective keys derived from two consecutive rounds may not be compatible with the key schedule.
Singular Characteristics

\[
\begin{align*}
\alpha_0 & \xrightarrow{S} \beta_0 \xrightarrow{P} \alpha_1 \xrightarrow{S} \beta_1 \xrightarrow{P} \alpha_2 \xrightarrow{S} \beta_2 \xrightarrow{P} \alpha_3 \xrightarrow{S} \beta_3 \xrightarrow{P} \alpha_4 \\
\end{align*}
\]

When the difference propagation is legal, the effective key set of a 2-round characteristic is non-empty. Effective keys derived from two consecutive rounds may not be compatible with the key schedule.
Singular Characteristics

When the difference propagation is legal, the effective key set of a 2-round characteristic is non-empty. Effective keys derived from two consecutive rounds may not be compatible with the key schedule.
Singular Characteristics

When the difference propagation is legal, the effective key set of a 2-round characteristic is non-empty. Effective keys derived from two consecutive rounds may not be compatible with the key schedule.
When the difference propagation is legal, the effective key set of a 2-round characteristic is non-empty.
When the difference propagation is legal, the effective key set of a 2-round characteristic is non-empty.

Effective keys derived from two consecutive rounds may not be compatible with the key schedule.
Singular Characteristics

\[ \alpha_0 \xrightarrow{S} \beta_0 \xrightarrow{P} \alpha_1 \xrightarrow{S} \beta_1 \xrightarrow{P} \alpha_2 \xrightarrow{S} \beta_2 \xrightarrow{P} \alpha_3 \xrightarrow{S} \beta_3 \xrightarrow{P} \alpha_4 \]

Key Schedule

Procedure:

1. Conditions on \( K_i \) to be effective
2. Conditions based on a specific key schedule
3. Key schedule details
4. Linear equation systems

▶ No solution found

→ Further filter by nonlinear constraints
Singular Characteristics

\[ \begin{align*}
\alpha_0 & \xrightarrow{S} \beta_0 \xrightarrow{P} \alpha_1 \xrightarrow{S} \beta_1 \xrightarrow{P} \alpha_2 \xrightarrow{S} \beta_2 \xrightarrow{P} \alpha_3 \xrightarrow{S} \beta_3 \xrightarrow{P} \alpha_4 \\
K_1 \quad & \quad K_2 \quad & \quad K_3 \\
\uparrow \quad & \quad \uparrow \quad & \quad \uparrow \\
k & \rightarrow & \text{Key Schedule}
\end{align*} \]

Procedure:

1. Conditions on \( K_i \) to be effective
Singular Characteristics

\[ \alpha_0 \xrightarrow{S} \beta_0 \xrightarrow{P} \alpha_1 \xrightarrow{S} \beta_1 \xrightarrow{P} \alpha_2 \xrightarrow{S} \beta_2 \xrightarrow{P} \alpha_3 \xrightarrow{S} \beta_3 \xrightarrow{P} \alpha_4 \]

Key Schedule

\[ k \rightarrow \text{Key Schedule} \]

Procedure:
1. Conditions on \( K_i \) to be effective
2. Conditions based on a specific key schedule
Singular Characteristics

\[
\begin{align*}
\alpha_0 & \xrightarrow{S} \beta_0 \xrightarrow{P} \alpha_1 \xrightarrow{S} \beta_1 \xrightarrow{P} \alpha_2 \xrightarrow{S} \beta_2 \xrightarrow{P} \alpha_3 \xrightarrow{S} \beta_3 \xrightarrow{P} \alpha_4 \\
K_1 & \quad K_2 \quad K_3
\end{align*}
\]

Procedure:
1. Conditions on \( K_i \) to be effective
2. Conditions based on a specific key schedule
3. Key schedule details
Singular Characteristics

\[ \alpha_0 \xrightarrow{S} \beta_0 \xrightarrow{P} \alpha_1 \xrightarrow{S} \beta_1 \xrightarrow{P} \alpha_2 \xrightarrow{S} \beta_2 \xrightarrow{P} \alpha_3 \xrightarrow{S} \beta_3 \xrightarrow{P} \alpha_4 \]

**Key Schedule**

\[ k \rightarrow \text{Key Schedule} \]

**Procedure:**

1. Conditions on \( K_i \) to be effective
2. Conditions based on a specific key schedule
3. Key schedule details
4. Linear equation systems
Singular Characteristics

\[ \alpha_0 \xrightarrow{S} \beta_0 \xrightarrow{P} \alpha_1 \xrightarrow{S} \beta_1 \xrightarrow{P} \alpha_2 \xrightarrow{S} \beta_2 \xrightarrow{P} \alpha_3 \xrightarrow{S} \beta_3 \xrightarrow{P} \alpha_4 \]

Key Schedule

Procedure:

1. Conditions on \( K_i \) to be effective
2. Conditions based on a specific key schedule
3. Key schedule details
4. Linear equation systems
   - No solution found \( \rightarrow \) singular
Singular Characteristics

\[ \alpha_0 \xrightarrow{S} \beta_0 \xrightarrow{P} \alpha_1 \xrightarrow{S} \beta_1 \xrightarrow{P} \alpha_2 \xrightarrow{S} \beta_2 \xrightarrow{P} \alpha_3 \xrightarrow{S} \beta_3 \xrightarrow{P} \alpha_4 \]

Key Schedule

\[ k \rightarrow \text{Key Schedule} \]

Procedure:

1. Conditions on \( K_i \) to be effective
2. Conditions based on a specific key schedule
3. Key schedule details
4. Linear equation systems
   - No solution found \( \rightarrow \) singular
   - Key candidates found \( \rightarrow \) Further filter by nonlinear constraints
Singular Characteristics in the AES

Find singular characteristics in AES-128:

Picture credit: TikZ for Cryptographers
Find singular characteristics in AES-128:

- Subspaces of effective keys in every two consecutive rounds

Picture credit: TikZ for Cryptographers
Singular Characteristics in the AES

Find singular characteristics in AES-128:

- Subspaces of effective keys in every two consecutive rounds
- Build equation systems with key schedule

Picture credit:
TikZ for Cryptographers
Find singular characteristics in AES-128:

- Subspaces of effective keys in every two consecutive rounds
- Build equation systems with key schedule
- 3 out of 4 columns in AES-128 key schedule are linear relations
Find singular characteristics in AES-128:

- Subspaces of effective keys in every two consecutive rounds
- Build equation systems with key schedule
- 3 out of 4 columns in AES-128 key schedule are linear relations
- Simplify and solve the equation system
Singular Characteristics in the AES

Examples of 5-round singular characteristics can be found in the AES-128.

\[
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
\end{pmatrix}
\rightarrow
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
\end{pmatrix}
\rightarrow
\begin{pmatrix}
2 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 \\
3 & 0 & 0 & 0 \\
\end{pmatrix}
\rightarrow
\begin{pmatrix}
3 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 \\
\end{pmatrix}
\rightarrow
\begin{pmatrix}
6 & 2 & 1 & 3 \\
3 & 2 & 3 & 2 \\
3 & 6 & 2 & 1 \\
5 & 4 & 1 & 1 \\
\end{pmatrix}
\rightarrow
\begin{pmatrix}
24 & 27 & 39 & 9d \\
45 & 36 & 36 & 27 \\
36 & f1 & 2e & 2d \\
39 & 2d & 1f & 3a \\
\end{pmatrix}
\rightarrow
\begin{pmatrix}
6 & 0 & 0 & 0 \\
0 & 5 & 0 & 0 \\
0 & 0 & 5 & 0 \\
0 & 0 & 0 & 36 \\
\end{pmatrix}
\rightarrow
\begin{pmatrix}
e & 0 & 0 & 0 \\
0 & 9 & 0 & 0 \\
0 & 0 & d & 0 \\
0 & 0 & 0 & b \\
\end{pmatrix}
\rightarrow
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
\end{pmatrix}
\rightarrow
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
\end{pmatrix}
\rightarrow
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
\end{pmatrix}.
\]
Singular Characteristics in the AES

Examples of 5-round singular characteristics can be found in the AES-128.

MITM attack
Singular Characteristics in the AES

Density of singular characteristics:
Density of singular characteristics:

\[
\begin{pmatrix}
* & 0 & 0 & 0 \\
* & 0 & 0 & 0 \\
* & 0 & 0 & 0 \\
* & 0 & 0 & 0 \\
\end{pmatrix}
\rightarrow
\begin{pmatrix}
* & 0 & 0 & 0 \\
* & 0 & 0 & 0 \\
* & 0 & 0 & 0 \\
* & 0 & 0 & 0 \\
\end{pmatrix}
\rightarrow
\begin{pmatrix}
* & * & * & * \\
* & * & * & * \\
* & * & * & * \\
* & * & * & * \\
\end{pmatrix}
\rightarrow
\begin{pmatrix}
* & * & * & * \\
* & * & * & * \\
* & * & * & * \\
* & * & * & * \\
\end{pmatrix}
\rightarrow
\begin{pmatrix}
* & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
\end{pmatrix}
\rightarrow
\begin{pmatrix}
* & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
\end{pmatrix}
\]
Density of singular characteristics:

\[
\begin{pmatrix}
* & 0 & 0 & 0 \\
* & 0 & 0 & 0 \\
* & 0 & 0 & 0 \\
* & 0 & 0 & 0 \\
\end{pmatrix}
\xrightarrow{S}
\begin{pmatrix}
* & 0 & 0 & 0 \\
* & 0 & 0 & 0 \\
* & 0 & 0 & 0 \\
* & 0 & 0 & 0 \\
\end{pmatrix}
\xrightarrow{P}
\begin{pmatrix}
**** \\
**** \\
**** \\
**** \\
\end{pmatrix}
\xrightarrow{S}
\begin{pmatrix}
**** \\
**** \\
**** \\
**** \\
\end{pmatrix}
\xrightarrow{P}
\begin{pmatrix}
* & 0 & 0 & 0 \\
0 & * & 0 & 0 \\
0 & 0 & * & 0 \\
0 & 0 & 0 & * \\
\end{pmatrix}
\xrightarrow{S}
\begin{pmatrix}
* & 0 & 0 & 0 \\
0 & * & 0 & 0 \\
0 & 0 & * & 0 \\
0 & 0 & 0 & * \\
\end{pmatrix}
\]

- Enumerate all characteristics given a 3-round differential
Singular Characteristics in the AES

Density of singular characteristics:

\[
\begin{pmatrix}
*000 \\
000 \\
000 \\
000 \\
000
\end{pmatrix}
\rightarrow
\begin{pmatrix}
*000 \\
000 \\
000 \\
000 \\
000
\end{pmatrix}
\rightarrow
\begin{pmatrix}
***** \\
***** \\
***** \\
***** \\
*****
\end{pmatrix}
\rightarrow
\begin{pmatrix}
**** \\
**** \\
**** \\
**** \\
****
\end{pmatrix}
\rightarrow
\begin{pmatrix}
0000 \\
0000 \\
0000 \\
0000 \\
*000
\end{pmatrix}
\rightarrow
\begin{pmatrix}
000 \\
000 \\
000 \\
000 \\
000
\end{pmatrix}
\rightarrow
\begin{pmatrix}
0000 \\
0000 \\
0000 \\
0000 \\
*000
\end{pmatrix}
\rightarrow
\begin{pmatrix}
0000 \\
0000 \\
0000 \\
0000 \\
0000
\end{pmatrix}
\]

- Enumerate all characteristics given a 3-round differential
- More than 98.47% of all the characteristics are singular
Density of singular characteristics:

\[
\begin{bmatrix}
\ast & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
\end{bmatrix}
\]

\[
\rightarrow
\begin{bmatrix}
\ast & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
\end{bmatrix}
\]

\[
\rightarrow
\begin{bmatrix}
\ast & \ast & \ast & \ast \\
\ast & \ast & \ast & \ast \\
\ast & \ast & \ast & \ast \\
\ast & \ast & \ast & \ast \\
\end{bmatrix}
\]

\[
\rightarrow
\begin{bmatrix}
\ast & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
\end{bmatrix}
\]

\[
\rightarrow
\begin{bmatrix}
\ast & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
\end{bmatrix}
\]

- Enumerate all characteristics given a 3-round differential
- More than 98.47% of all the characteristics are singular
- For the remaining characteristics, we consider the nonlinear constraints from the key schedule and get their effective keys
Singular Characteristics in the AES

Density of singular characteristics:

$$\begin{pmatrix} *000 \\ *000 \\ *000 \\ *000 \end{pmatrix} \xrightarrow{S} \begin{pmatrix} *000 \\ *000 \\ *000 \\ *000 \end{pmatrix} \xrightarrow{P} \begin{pmatrix} **** \\ **** \\ **** \\ **** \end{pmatrix} \xrightarrow{S} \begin{pmatrix} **** \\ **** \\ **** \\ **** \end{pmatrix} \xrightarrow{P} \begin{pmatrix} *000 \\ 0*00 \\ 00*0 \\ 00*0 \end{pmatrix} \xrightarrow{S} \begin{pmatrix} *000 \\ 0*00 \\ 00*0 \\ 00*0 \end{pmatrix}$$

- Enumerate all characteristics given a 3-round differential
- More than 98.47% of all the characteristics are singular
- For the remaining characteristics, we consider the nonlinear constraints from the key schedule and get their effective keys
  - some of them may also be singular
  - the number of effective keys is around $2^7$ to $2^{10}$
Different key schedules affect the singularity of a characteristic.
Different key schedules affect the singularity of a characteristic

- Encrypt a pair of plaintexts under some key with AES-128, track the characteristic
Singular Characteristics in the AES

- Different key schedules affect the singularity of a characteristic
  - Encrypt a pair of plaintexts under some key with AES-128, track the characteristic
  - Change the key schedule into AES-192
Different key schedules affect the singularity of a characteristic

- Encrypt a pair of plaintexts under some key with AES-128, track the characteristic
- Change the key schedule into AES-192
- A valid characteristic in AES-128 is highly probable to be singular in AES-192
Singular Characteristics in the AES

- Different key schedules affect the singularity of a characteristic
  - Encrypt a pair of plaintexts under some key with AES-128, track the characteristic
  - Change the key schedule into AES-192
  - A valid characteristic in AES-128 is highly probable to be singular in AES-192
- Differential enumeration + key schedule constraints
Different key schedules affect the singularity of a characteristic

- Encrypt a pair of plaintexts under some key with AES-128, track the characteristic
- Change the key schedule into AES-192
- A valid characteristic in AES-128 is highly probable to be singular in AES-192

Differential enumeration + key schedule constraints

Extension to AES-like, Feistel-SP, Feistel
Singular Characteristics in Prince
Singular Characteristics in Prince

\[
\begin{pmatrix}
8 & 0 & 4 & 0 \\
0 & 0 & 0 & 0 \\
4 & 0 & 8 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix}
\xrightarrow{S}
\begin{pmatrix}
8 & 0 & 4 & 0 \\
0 & 0 & 0 & 0 \\
8 & 0 & 4 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix}
\xrightarrow{M'}
\begin{pmatrix}
8 & 0 & 4 & 0 \\
0 & 0 & 0 & 0 \\
8 & 0 & 4 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix}
\xrightarrow{SR}
\begin{pmatrix}
8 & 0 & 4 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix}
\xrightarrow{S}
\begin{pmatrix}
8 & 0 & 5 & 0 \\
0 & 0 & 0 & 0 \\
8 & 0 & 5 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix}
\xrightarrow{M'}
\begin{pmatrix}
8 & 0 & 5 & 0 \\
0 & 0 & 0 & 0 \\
8 & 0 & 5 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix}
\xrightarrow{SR}
\begin{pmatrix}
8 & 0 & 5 & 0 \\
0 & 0 & 0 & 0 \\
5 & 0 & 8 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix}
\xrightarrow{S}
\begin{pmatrix}
2 & 0 & 5 & 0 \\
0 & 0 & 0 & 0 \\
2 & 0 & 5 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix}
\]
A 3-round singular characteristic with EDP $= 2^{-35}$
Singular Cluster

If no effective key in common \(\rightarrow\) singular cluster.

Differentials/truncated differentials/multiple differentials
Singular Cluster

If no effective key in common → singular cluster.

Differentials/truncated differentials/multiple differentials

\[
\begin{align*}
\alpha_0 & \xrightarrow{S} \beta_0 \xrightarrow{P} \alpha_1 \xrightarrow{S} \beta_1 \xrightarrow{P} \alpha_2 \xrightarrow{S} \beta_2 \xrightarrow{P} \alpha_3 \xrightarrow{S} \beta_3 \xrightarrow{P} \alpha_4 \\
\alpha'_0 & \xrightarrow{S} \beta'_0 \xrightarrow{P} \alpha'_1 \xrightarrow{S} \beta'_1 \xrightarrow{P} \alpha'_2 \xrightarrow{S} \beta'_2 \xrightarrow{P} \alpha'_3 \xrightarrow{S} \beta'_3 \xrightarrow{P} \alpha'_4
\end{align*}
\]
If no effective key in common → *singular cluster*. 

---

*Singular Cluster*

\[
\begin{align*}
\alpha_0 & \xrightarrow{S} \beta_0 \xrightarrow{P} \alpha_1 \xrightarrow{S} \beta_1 \xrightarrow{P} \alpha_2 \xrightarrow{S} \beta_2 \xrightarrow{P} \alpha_3 \xrightarrow{S} \beta_3 \xrightarrow{P} \alpha_4 \\
\alpha'_0 & \xrightarrow{S} \beta'_0 \xrightarrow{P} \alpha'_1 \xrightarrow{S} \beta'_1 \xrightarrow{P} \alpha'_2 \xrightarrow{S} \beta'_2 \xrightarrow{P} \alpha'_3 \xrightarrow{S} \beta'_3 \xrightarrow{P} \alpha'_4
\end{align*}
\]
If no effective key in common $\rightarrow$ singular cluster.
Differentials/truncated differentials/multiple differentials
**Observation**: If a differential contains only singular characteristics, it is an impossible differential.
Observation: If a differential contains only singular characteristics, it is an impossible differential.

- Provable security against impossible differential on structures [SLG+16]
Observation: If a differential contains only singular characteristics, it is an impossible differential.

- Provable security against impossible differential on structures [SLG+16]
- Focus on the Sbox and the key schedule
Further Applications

Observation: If a differential contains only singular characteristics, it is an impossible differential.

- Provable security against impossible differential on structures [SLG+16]
- Focus on the Sbox and the key schedule
- Impossible differential by singular characteristics
Further Applications

Observation: If a differential contains only singular characteristics, it is an impossible differential.

- Provable security against impossible differential on structures [SLG+16]
- Focus on the Sbox and the key schedule
- Impossible differential by singular characteristics
- An impossible differential is found in a toy cipher
Further Applications

Observation: If a differential contains only singular characteristics, it is an impossible differential.

- Provable security against impossible differential on structures [SLG+16]
- Focus on the Sbox and the key schedule
- Impossible differential by singular characteristics
- An impossible differential is found in a toy cipher
- Improve distinguishers?
Consider a 5-round differential $D$ of the AES with active pattern 1-4-16-4-1. The effective keys of each characteristic can be precomputed. By assuming the knowledge on the effective keys of the differential:
Further Applications

Consider a 5-round differential $\mathcal{D}$ of the AES with active pattern 1-4-16-4-1. The effective keys of each characteristic can be precomputed.

By assuming the knowledge on the effective keys of the differential:

- $\Omega_\mathcal{D} = \emptyset \rightarrow \text{singular}$
Further Applications

Consider a 5-round differential $D$ of the AES with active pattern 1-4-16-4-1. The effective keys of each characteristic can be precomputed.

By assuming the knowledge on the effective keys of the differential:

- $\Omega_D = \emptyset \rightarrow$ singular
- $|\Omega_D| \neq \emptyset$
Further Applications

Consider a 5-round differential $D$ of the AES with active pattern 1-4-16-4-1. The effective keys of each characteristic can be precomputed. By assuming the knowledge on the effective keys of the differential:

- $\Omega_D = \emptyset \rightarrow$ singular
- $|\Omega_D| \neq \emptyset$
  - Information leaked about the secret key
Further Applications

Consider a 5-round differential $D$ of the AES with active pattern 1-4-16-4-1. The effective keys of each characteristic can be precomputed.

By assuming the knowledge on the effective keys of the differential:

- $\Omega_D = \emptyset \rightarrow$ singular
- $|\Omega_D| \neq \emptyset$
  - Information leaked about the secret key
  - The total number of characteristics is around $2^{70}$, $|\Omega_D| < 2^{128}$
Further Applications

Consider a 5-round differential $\mathcal{D}$ of the AES with active pattern 1-4-16-4-1. The effective keys of each characteristic can be precomputed.

By assuming the knowledge on the effective keys of the differential:

- $\Omega_{\mathcal{D}} = \emptyset \rightarrow$ singular
- $|\Omega_{\mathcal{D}}| \neq \emptyset$
  - Information leaked about the secret key
  - The total number of characteristics is around $2^{70}$, $|\Omega_{\mathcal{D}}| < 2^{128}$
  - Exhaustive search space reduced?
Summary

- Differential cryptanalysis in fixed-key block ciphers and permutations
Summary

- Differential cryptanalysis in fixed-key block ciphers and permutations
- Effective keys and singular characteristics are proposed based on fixed-key DP
Summary

- Differential cryptanalysis in fixed-key block ciphers and permutations
- Effective keys and singular characteristics are proposed based on fixed-key DP
- Concrete examples are found for AES-like ciphers with efficient algorithms
Summary

- Differential cryptanalysis in fixed-key block ciphers and permutations
- Effective keys and singular characteristics are proposed based on fixed-key DP
- Concrete examples are found for AES-like ciphers with efficient algorithms
- Pay extra attention to characteristics generated from enumeration techniques when they are applied in attacks
Summary

- Differential cryptanalysis in fixed-key block ciphers and permutations
- Effective keys and singular characteristics are proposed based on fixed-key DP
- Concrete examples are found for AES-like ciphers with efficient algorithms
- Pay extra attention to characteristics generated from enumeration techniques when they are applied in attacks
- New approach towards improved distinguisher or key recovery technique
Summary

- Differential cryptanalysis in fixed-key block ciphers and permutations
- Effective keys and singular characteristics are proposed based on fixed-key DP
- Concrete examples are found for AES-like ciphers with efficient algorithms
- Pay extra attention to characteristics generated from enumeration techniques when they are applied in attacks
- New approach towards improved distinguisher or key recovery technique

Thank you for your attention!