Probabilistic Slide Cryptanalysis and Its Applications to LED-64 and Zorro

Hadi Soleimany

Department of Information and Computer Science,
Aalto University School of Science, Finland

FSE 2014

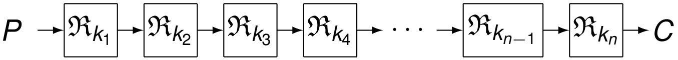
Outline

Iterated Block Cipher

Block cipher:

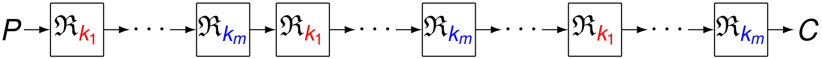
$$E_K(P) : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$$

Iterated block cipher:

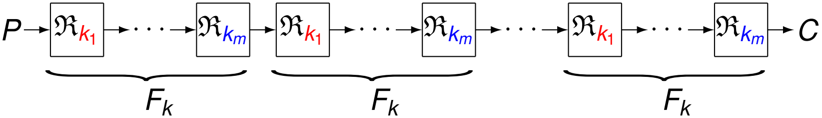


$$C = \mathfrak{R}_{k_n} \circ \cdots \circ \mathfrak{R}_{k_2} \circ \mathfrak{R}_{k_1}(P)$$

Iterated Block Cipher with Periodic Subkeys

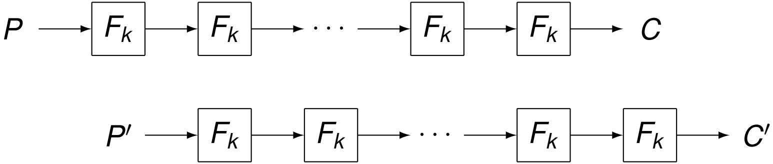


Iterated Block Cipher with Periodic Subkeys

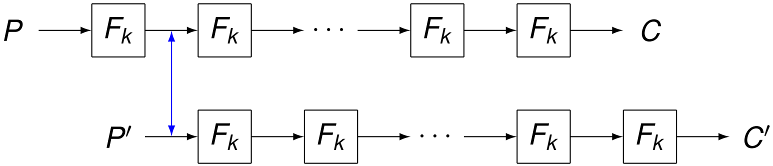


- The cipher can be presented as a cascade of identical functions F_k.

Slide Cryptanalysis [Biryukov Wagner 99]

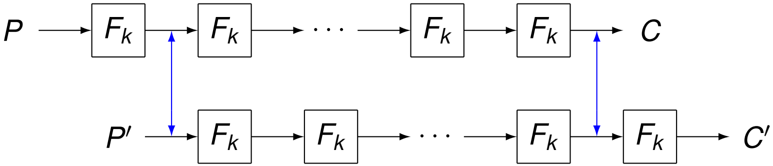


Slide Cryptanalysis [Biryukov Wagner 99]



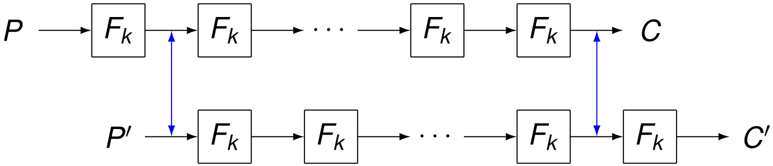
$P' = F_k(P)$

Slide Cryptanalysis [Biryukov Wagner 99]



$P' = F_k(P) \implies C' = F_k(C)$ (Slid pair)

Slide Cryptanalysis [Biryukov Wagner 99]

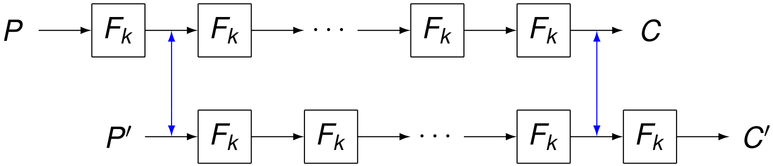


$P' = F_k(P) \quad \Longrightarrow \quad C' = F_k(C)$ (Slid pair)

$\Pr[P' = F_k(P)] = 2^{-n} \qquad \Pr[C = F_k^{-1}(C'), P' = F_k(P)] = 2^{-n} > 2^{-2n}$

$\Longrightarrow$ 2^n pairs $((P, C), (P', C'))$ are expected to find a slid pair.

Slide Cryptanalysis [Biryukov Wagner 99]



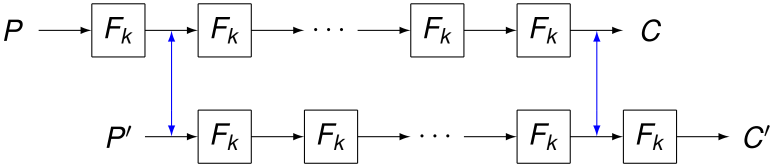
$P' = F_k(P)$ $\Longrightarrow$ $C' = F_k(C)$ (Slid pair)

$\Pr[P' = F_k(P)] = 2^{-n}$ $\quad \Pr[C = F_k^{-1}(C'), P' = F_k(P)] = 2^{-n} > 2^{-2n}$

$\Longrightarrow 2^n$ pairs $((P, C), (P', C'))$ are expected to find a slid pair.

Typical countermeasures: Key-schedule or round constants.

Slide Cryptanalysis [Biryukov Wagner 99]



$P' = F_k(P) \quad \Longrightarrow \quad C' = F_k(C)$ (Slid pair)

$\Pr[P' = F_k(P)] = 2^{-n} \qquad \Pr[C = F_k^{-1}(C'), P' = F_k(P)] = 2^{-n} > 2^{-2n}$

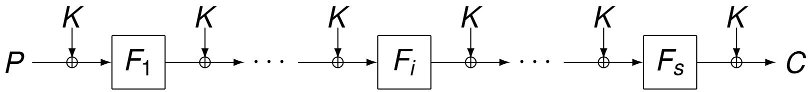
$\Longrightarrow$ 2^n pairs $((P, C), (P', C'))$ are expected to find a slid pair.

Typical countermeasures: Key-schedule or round constants.

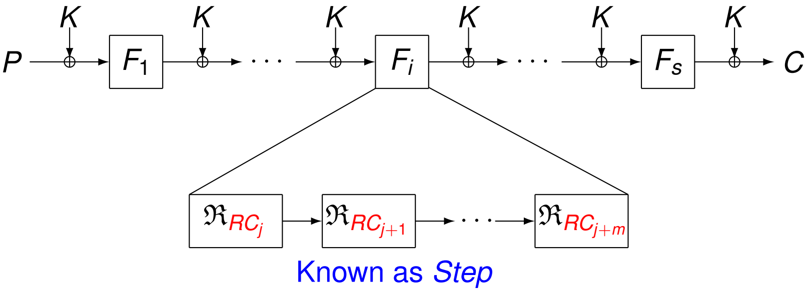
This Work:

Probabilistic technique to overcome round constants in block ciphers based on the Even-Mansour scheme with a single key.

Even-Mansour Scheme with a Single Key

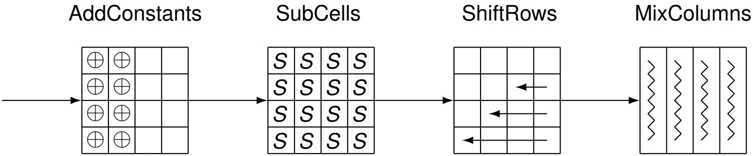


Even-Mansour Scheme with a Single Key



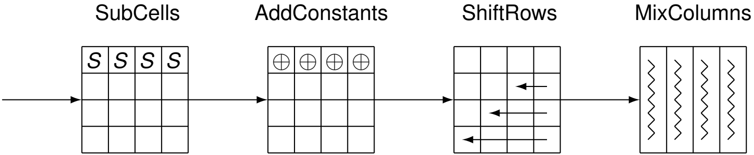
- Block ciphers like LED-64, PRINCE_{core}, Zorro and PRINTcipher.

LED-64



- Presented at CHES 2011 [Guo et al 11]
- 64-bit block cipher and supports 64-bit key
- 6 steps
- Each step consists of four rounds.

Zorro



- Presented at CHES 2013 [Gérard et al 13]
- 128-bit block cipher and supports 128-bit key
- 6 steps
- Each step consists of four rounds

Overview of Previous Attacks

- Slide cryptanalysis requires known plaintexts.

Overview of Previous Attacks

- Slide cryptanalysis requires known plaintexts.
  - But it is limited to the ciphers with identical rounds.

Overview of Previous Attacks

- Slide cryptanalysis requires known plaintexts.
  - But it is limited to the ciphers with identical rounds.
- Differential cryptanalysis is usually applicable on any round functions [Biham Shamir 90].

Overview of Previous Attacks

- Slide cryptanalysis requires known plaintexts.
  - But it is limited to the ciphers with identical rounds.
- Differential cryptanalysis is usually applicable on any round functions [Biham Shamir 90].
  - But there exists a lower bound for active S-boxes and it usually requires chosen plaintexts.

Overview of Previous Attacks

- Slide cryptanalysis requires known plaintexts.
  - But it is limited to the ciphers with identical rounds.
- Differential cryptanalysis is usually applicable on any round functions [Biham Shamir 90].
  - But there exists a lower bound for active S-boxes and it usually requires chosen plaintexts.
- Related-key differential usually has less active S-boxes and applicable on more rounds [Kelsey et al 97].

Overview of Previous Attacks

- Slide cryptanalysis requires known plaintexts.
  - But it is limited to the ciphers with identical rounds.
- Differential cryptanalysis is usually applicable on any round functions [Biham Shamir 90].
  - But there exists a lower bound for active S-boxes and it usually requires chosen plaintexts.
- Related-key differential usually has less active S-boxes and applicable on more rounds [Kelsey et al 97].
  - But usually it is not a realistic model.

Overview of Previous Attacks

- Slide cryptanalysis requires known plaintexts.
  - But it is limited to the ciphers with identical rounds.
- Differential cryptanalysis is usually applicable on any round functions [Biham Shamir 90].
  - But there exists a lower bound for active S-boxes and it usually requires chosen plaintexts.
- Related-key differential usually has less active S-boxes and applicable on more rounds [Kelsey et al 97].
  - But usually it is not a realistic model.
- Probabilistic reflection attack is applicable on block ciphers with almost symmetric rounds [Soleimany et al 13].

Overview of Previous Attacks

- Slide cryptanalysis requires known plaintexts.
  - But it is limited to the ciphers with identical rounds.
- Differential cryptanalysis is usually applicable on any round functions [Biham Shamir 90].
  - But there exists a lower bound for active S-boxes and it usually requires chosen plaintexts.
- Related-key differential usually has less active S-boxes and applicable on more rounds [Kelsey et al 97].
  - But usually it is not a realistic model.
- Probabilistic reflection attack is applicable on block ciphers with almost symmetric rounds [Soleimany et al 13].
  - But its application is limited to involutional block ciphers.

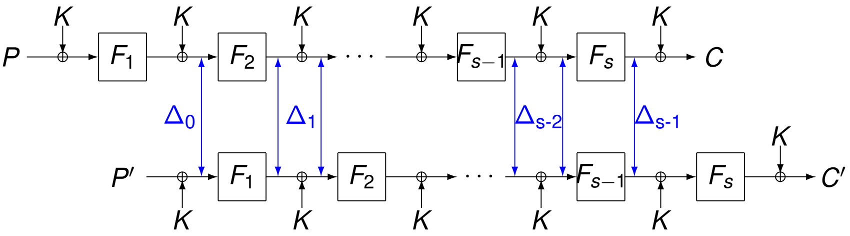
Overview of Previous Attacks

- Slide cryptanalysis requires known plaintexts.
  - But it is limited to the ciphers with identical rounds.
- Differential cryptanalysis is usually applicable on any round functions [Biham Shamir 90].
  - But there exists a lower bound for active S-boxes and it usually requires chosen plaintexts.
- Related-key differential usually has less active S-boxes and applicable on more rounds [Kelsey et al 97].
  - But usually it is not a realistic model.
- Probabilistic reflection attack is applicable on block ciphers with almost symmetric rounds [Soleimany et al 13].
  - But its application is limited to involutional block ciphers.

This Work

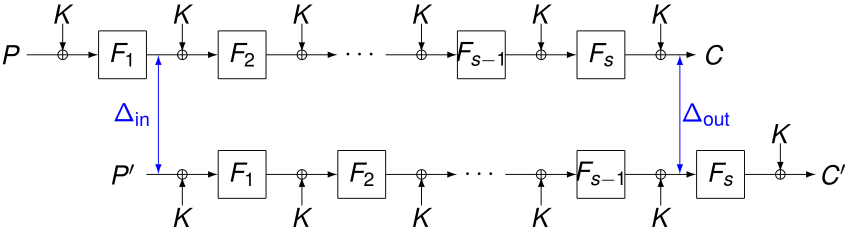
Exploit previous ideas to take advantage of the positive properties and overcome the negative aspects!

Probabilistic Slide Distinguisher



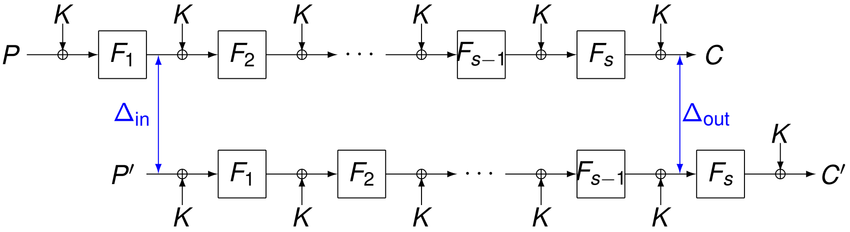
- Assume there exists a sequence of differences $\mathcal{D} = \{\Delta_0, \ldots, \Delta_{s-1}\}$ such that $\Pr[F_r(x) \oplus F_{r-1}(x \oplus \Delta_{r-2}) = \Delta_{r-1}] = 2^{-p_{r-1}}$ where $0 \leq p_r$.
- A differential-type characteristic with input difference $\Delta_{in} = \Delta_0$ and output difference $\Delta_{out} = \Delta_{s-1}$ can be obtained with probability $2^{-p} = \Pi_{r=1}^{s-1} 2^{-p_r}$.

Probabilistic Slide Distinguisher



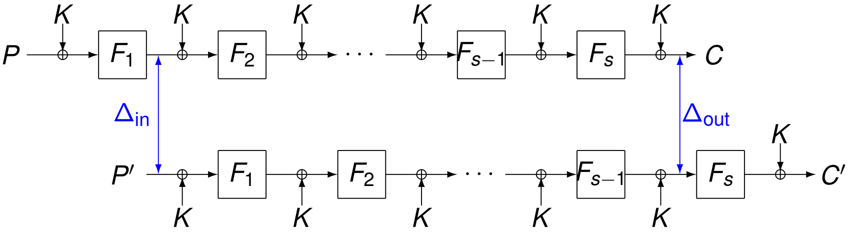
$P' \oplus F_1(P \oplus K) = \Delta_{in}$

Probabilistic Slide Distinguisher



$$P' \oplus F_1(P \oplus K) = \Delta_{in} \quad \overset{\text{probability } 2^{-p}}{\Longrightarrow} \quad C \oplus F_s^{-1}(C' \oplus K) = \Delta_{out}$$

Probabilistic Slide Distinguisher



$P' \oplus F_1(P \oplus K) = \Delta_{in}$ $\overset{\text{probability } 2^{-p}}{\Longrightarrow}$ $C \oplus F_s^{-1}(C' \oplus K) = \Delta_{out}$

$$\Pr[P' \oplus F_1(P \oplus K) = \Delta_{in}] = 2^{-n}$$

$$\Pr[C \oplus F_s^{-1}(C' \oplus K) = \Delta_{out}, P' \oplus F_1(P \oplus K) = \Delta_{in}] = 2^{-n-p}$$

$\Longrightarrow 2^{(n+p)}$ pairs $((P, C), (P', C'))$ are expected to find a right slid pair

Key Recovery

- The right slid pair satisfies the relation

$$C' \oplus F_s(C \oplus \Delta_{out}) = K = P \oplus F_1^{-1}(\Delta_{in} \oplus P',)$$

Key Recovery

- The right slid pair satisfies the relation

$$C' \oplus F_1^{-1}(\Delta_{\text{in}} \oplus P') = P \oplus F_s(C \oplus \Delta_{\text{out}}).$$

Key Recovery

- The right slid pair satisfies the relation

$$C' \oplus F_1^{-1}(\Delta_{\text{in}} \oplus P') = P \oplus F_s(C \oplus \Delta_{\text{out}}).$$

For given $2^{(n+p)/2}$ known (P, C):

Step 1 For all pairs (P, C) compute $C \oplus F_1^{-1}(P \oplus \Delta_{\text{in}})$ and store the computed value with C in the hash table T_1.

Key Recovery

- The right slid pair satisfies the relation

$$C' \oplus F_1^{-1}(\Delta_{\text{in}} \oplus P') = P \oplus F_s(C \oplus \Delta_{\text{out}}).$$

For given $2^{(n+p)/2}$ known (P, C):

Step 1 For all pairs (P, C) compute $C \oplus F_1^{-1}(P \oplus \Delta_{\text{in}})$ and store the computed value with C in the hash table T_1.

Step 2 For all pairs (P, C) compute $P \oplus F_s(\Delta_{\text{out}} \oplus C)$ and store the computed value with C in the hash table T_2.

Key Recovery

- The right slid pair satisfies the relation

$$C' \oplus F_1^{-1}(\Delta_{\text{in}} \oplus P') = P \oplus F_s(C \oplus \Delta_{\text{out}}).$$

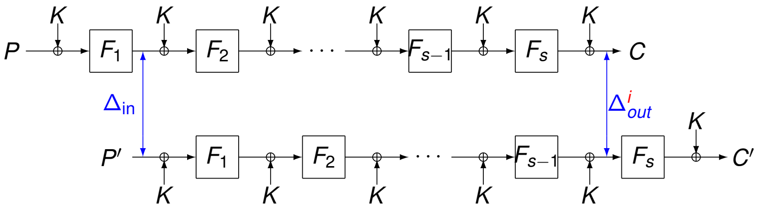
For given $2^{(n+p)/2}$ known (P, C):

Step 1 For all pairs (P, C) compute $C \oplus F_1^{-1}(P \oplus \Delta_{\text{in}})$ and store the computed value with C in the hash table T_1.

Step 2 For all pairs (P, C) compute $P \oplus F_s(\Delta_{\text{out}} \oplus C)$ and store the computed value with C in the hash table T_2.

Step 3 For each collision in T_1 and T_2 find corresponding ciphertexts C and C' then compute a key candidate $K = C' \oplus F_s(C \oplus \Delta_{\text{out}})$.

More Output Differences



$P' = F_1(P \oplus \Delta_{in})$ $\quad C' = F_s(C \oplus \Delta^i_{out}), 1 \leq i \leq L$

$\Pr[P' = F_1(P \oplus \Delta_{in})] = 2^{-n}$

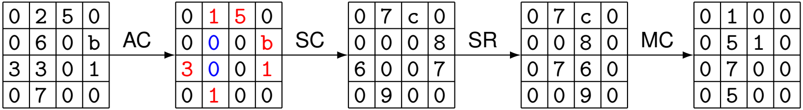
$\Pr[P' = F_1(P \oplus \Delta_{in}), C' = F_s(C \oplus \Delta^i_{out})] = 2^{-n} \sum_{i=1}^{L} 2^{-p_i}$

- Decrease the data requirement by increasing the total probability.
- This comes with the cost of repeating the attack algorithm L times.

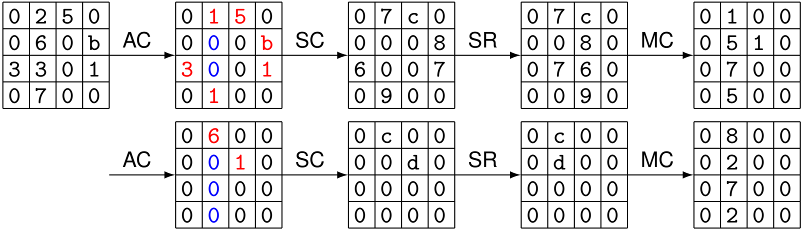
Slide Cryptanalysis of LED-64

0	2	5	0
0	6	0	b
3	3	0	1
0	7	0	0

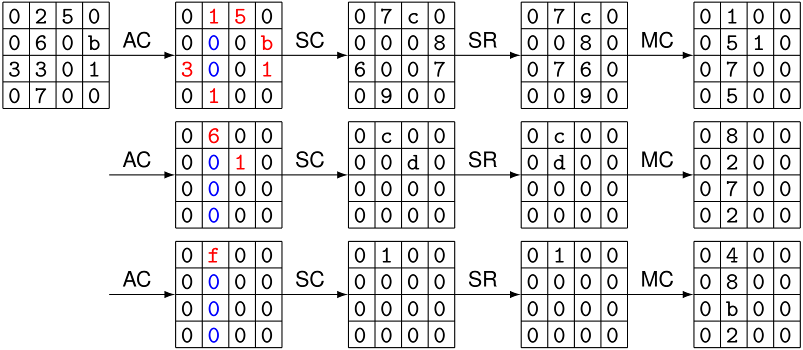
Slide Cryptanalysis of LED-64



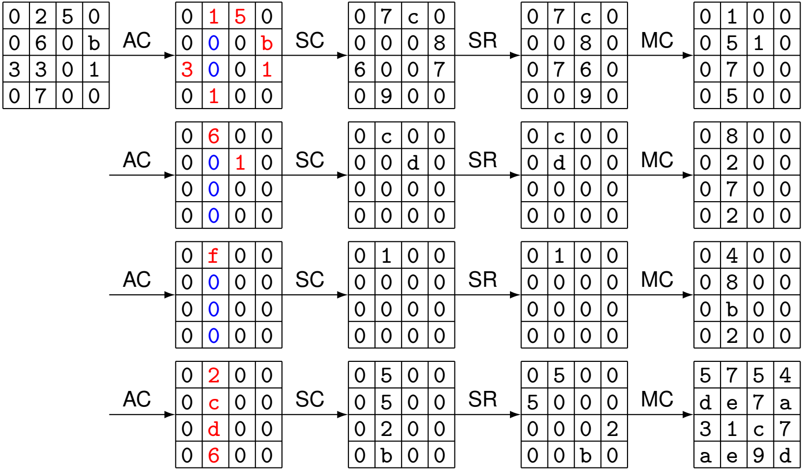
Slide Cryptanalysis of LED-64



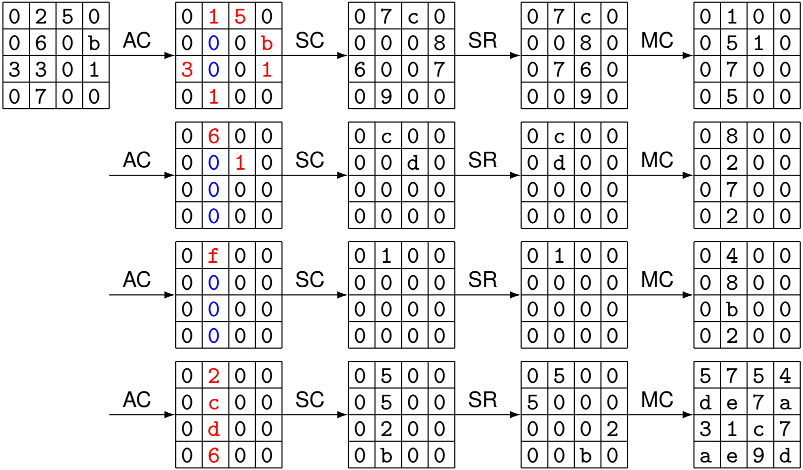
Slide Cryptanalysis of LED-64



Slide Cryptanalysis of LED-64

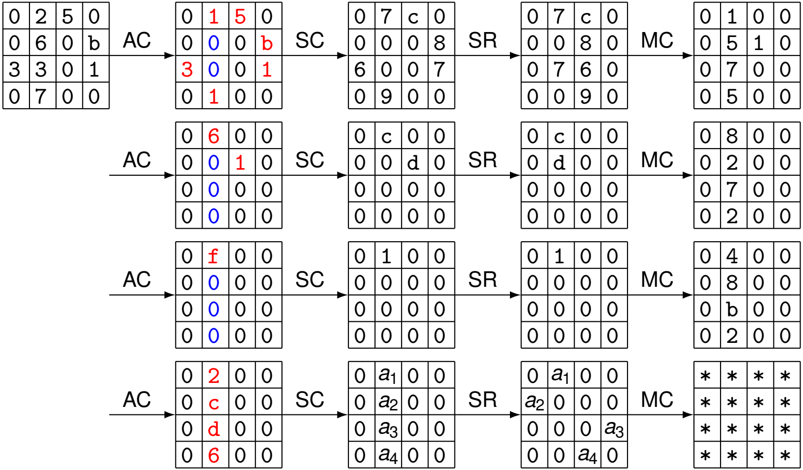


Slide Cryptanalysis of LED-64



- Thanks to cancellation, the characteristic has 13 active S-boxes while normal differential characteristic has at least 25 S-boxes.

Slide Cryptanalysis of LED-64



- $a_i \in \mathcal{A}_i$ where $\mathcal{A}_1 = \{3, 5, 6, \mathtt{a}, \mathtt{c}, \mathtt{d}, \mathtt{e}\}$, $\mathcal{A}_2 = \{2, 5, 7, 8, 9, \mathtt{a}, \mathtt{e}\}$, $\mathcal{A}_3 = \{1, 2, 3, 4, 7, \mathtt{a}, \mathtt{b}\}$ and $\mathcal{A}_4 = \{2, 6, 8, \mathtt{b}, \mathtt{c}, \mathtt{f}\}$

Slide Cryptanalysis of Zorro

State	Difference
$\Delta_{in} = X_5^I \oplus P'$	00000000d52c6f72120a92b50c8c2eee
$X_5^S \oplus X_1'^S$	00000000d52c6f72120a92b50c8c2eee
$X_5^A \oplus X_1^A$	04040420d52c6f72120a92b50c8c2eee
$X_5^R \oplus X_1'^R$	040404202c6f72d592b5120aee0c8c2e
$\vdots$	$\vdots$
$X_{16}^A \oplus X_{12}'^A$	1c17980d447ad32bfbc96dc0a06a35cc
$X_{16}^R \oplus X_{12}'^R$	1c17980d7ad32b446dc0fbc9cca06a35
$\Delta_{out} = X_{16}^M \oplus X_{12}'^M$	1720c72a9351b2f0f3a4e09fb071b7f0

- Differential characteristic for 3 steps (probability $2^{-119.24}$).
- Key-recovery cryptanalysis on 4 steps.
- This result improves the best cryptanalysis presented by the designers one step (four rounds).

Results

Cipher	Attack Type	Steps	Data	Time	Memory	Source
Zorro	Impossible differential	2.5	2^{115}CP	2^{115}	2^{115}	[Gérard et al 13]
	Meet-in-the-middle	3	2^{2}KP	2^{104}	-	[Gérard et al 13]
	Probabilistic slide	**4**	**$2^{123.62}$KP**	**$2^{123.8}$**	**$2^{123.62}$**	**This work**
	Probabilistic slide	**4**	**$2^{121.59}$KP**	**$2^{124.23}$**	**$2^{121.59}$**	**This work**
	Internal differential†	6	$2^{54.25}$CP	$2^{54.25}$	$2^{54.25}$	[Guo et al 13]
	Differential	6	$2^{112.4}$CP	2^{108}	-	[Wang et al 13]
LED-64	Meet-in-the-middle	2	2^{8}CP	2^{56}	2^{11}	[Isobe et al 12]
	Generic	2	2^{45}KP	$2^{60.1}$	2^{60}	[Dinur et al 13]
	Meet-in-the-middle	2	2^{16}CP	2^{48}	2^{17}	[Dinur et al 14]
	Meet-in-the-middle	2	2^{48}KP	2^{48}	2^{48}	[Dinur et al 14]
	Probabilistic slide	**2**	**$2^{45.5}$KP**	**$2^{46.5}$**	**$2^{46.5}$**	**This work**
	Probabilistic slide	**2**	**$2^{41.5}$KP**	**$2^{51.5}$**	**$2^{42.5}$**	**This work**
	Generic	3	2^{49}KP	$2^{60.2}$	2^{60}	[Dinur et al 13]

† – this attack is applicable just on 2^{64} keys (out of 2^{128}), CP – Chosen Plaintexts, KP – Known Plaintext.

Conclusion and Future Work

Conclusion

- Framework of probabilistic slide cryptanalysis on EMS which requires known-plaintext in the single-key model.
- The relation between round constants should be taken into account .
- Applications of the probabilistic slide cryptanalysis on LED-64 and Zorro.

Future Work

- Application on other EMS block ciphers.
- Improve the results on Zorro and LED-64 by exploiting *differential* instead of differential characteristic.

Thanks for your attention!