Cryptanalysis of Round-Reduced LED

Ivica Nikolić, Lei Wang and Shuang Wu

NANYANG TECHNOLOGICAL UNIVERSITY

FSE 2013
Singapore
March 11, 2013

Outline

- Backgrounds
  - ➢ Specification
  - ➢ Previous Analysis
- Slidex Attack Application
- Multicollision Application
- Distinguishers
  - ➢ Differential Property
  - ➢ Random-difference Distinguisher
- Conclusion

Outline

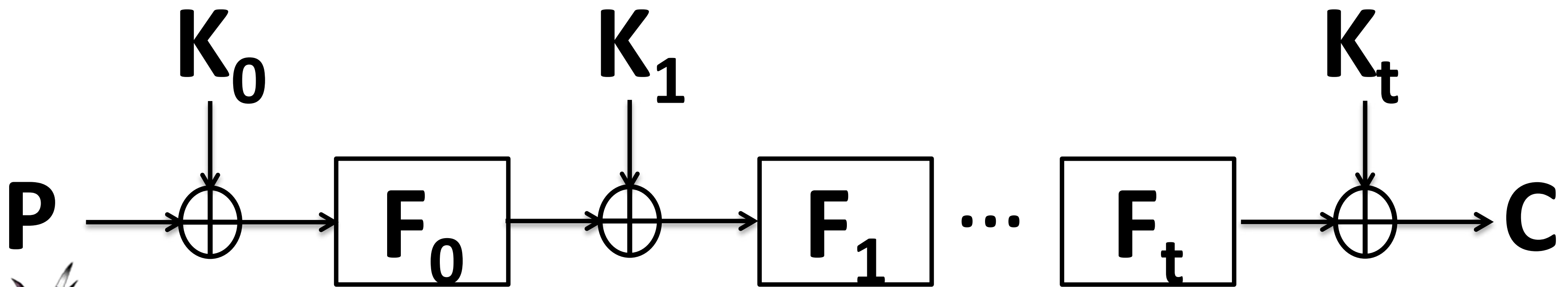
- **Backgrounds**
  - **Specification**
  - **Previous Analysis**
- Slidex Attack Application
- Multicollision Application
- Distinguishers
  - Differential Property
  - Random-difference Distinguisher
- Conclusion

LED

- Designed by Guo et al. at CHES 2011
- **L**ight **E**ncryption **D**evice
  - 64-bit block
  - 64- or 128-bit key (primarily)
- Conservative security, e.g. concerning
  - Related-key attack
  - Distinguishers in hash function setting

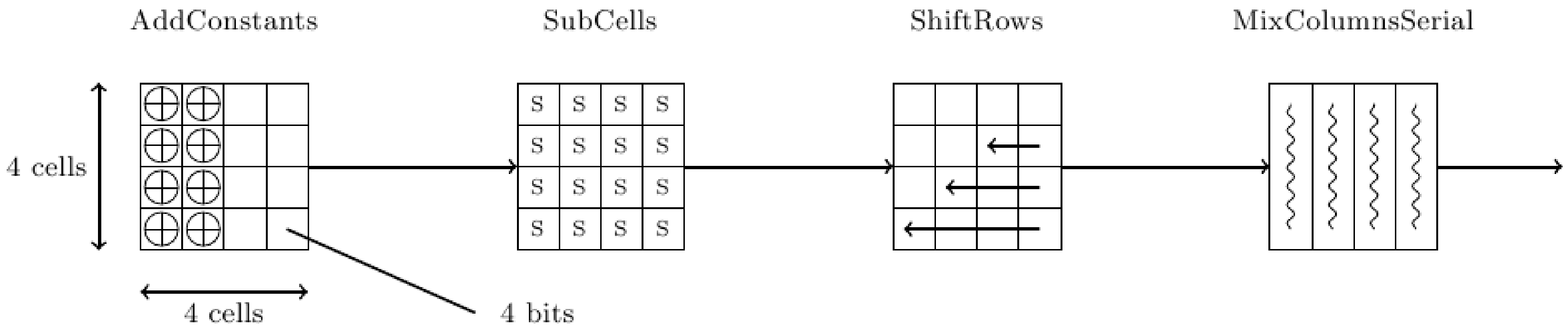
Specification (1/2)

- Extremely simple key schedule
  - Denote the secret key as K
  - LED-64: K as each round key
  - LED-128: $K = K_0 || K_1$, then K_0 and K_1 as round keys alternatively



Specification (2/2)

- LED-64: 8 steps; LED-128: 12 steps
- Step functions
  - AES like
  - 4 rounds and each round as below



  - Differ in round constants.

Timeline of Previous Analysis

- **Guo et al. at CHES 2011**
  - Distinguishers on 3.75/6.75-step LED-64/-128
  - Super-Sbox cryptanalysis
- **Isobe and Shibutani at ACISP 2012**
  - Key recovery on 2/4-step LED-64/-128
  - Meet-in-the-middle cryptanalysis
- **Mendel et al. at ASIACRYPT 2012**
  - Key recovery on 4-step LED-128
  - Related-key key recovery on 4/6-step LED-64/-128
  - Guess-then-recover, local collision, characteristics and differentials of step functions

Security State of LED

- The number of attacked steps

	Key Recovery		Distinguisher
	Single-key	Related-key	
LED-64 (8 steps)	2	4	3.75
LED-128 (12 steps)	4	6	6.75

Outline

- Backgrounds
  - Specification
  - Previous Analysis
- **Slidex Attack Application**
- Multicollision Application
- Distinguishers
  - Differential Property
  - Random-difference Distinguisher
- Conclusion

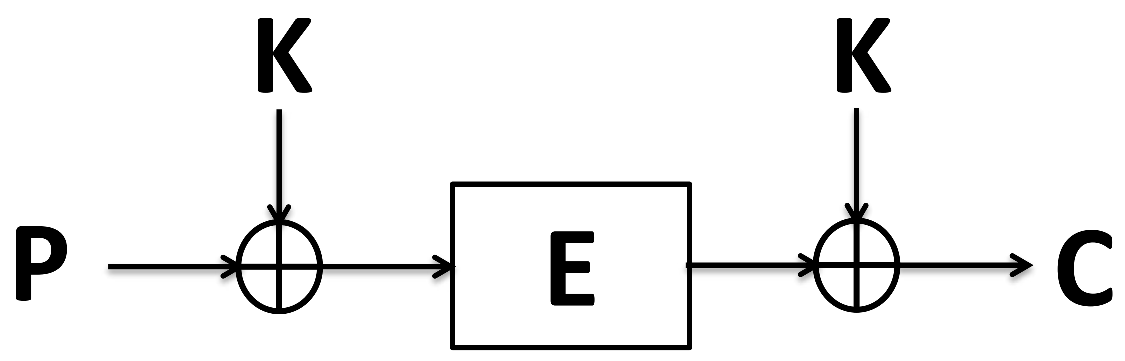
Security State of LED

- The number of attacked steps

	Key Recovery		Distinguisher
	Single-key	Related-key	
LED-64 (8 steps)	2	4	3.75
LED-128 (12 steps)	4	6	6.75

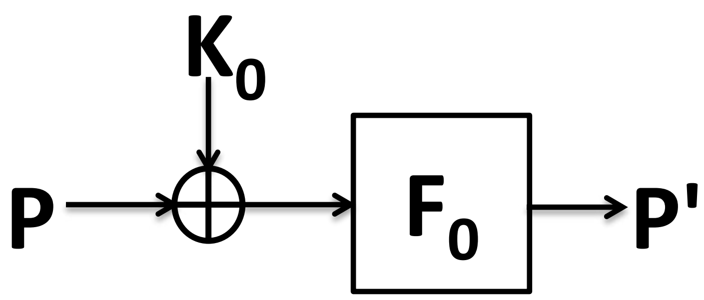
Slidex Attack

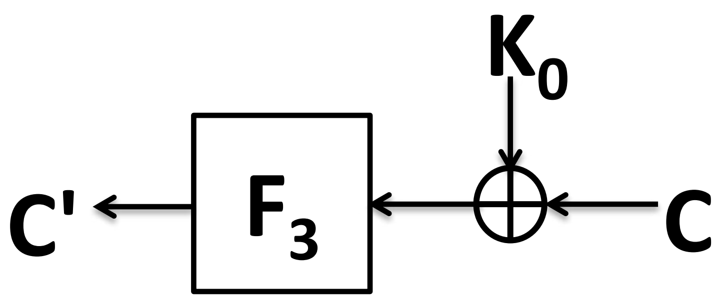
- Dunkelman et al. at EUROCRYPT 2012
- ***Known***-plaintext attack
- Wok for any public permutation E
- **Time*Data=2^n**
  - K is n bits long



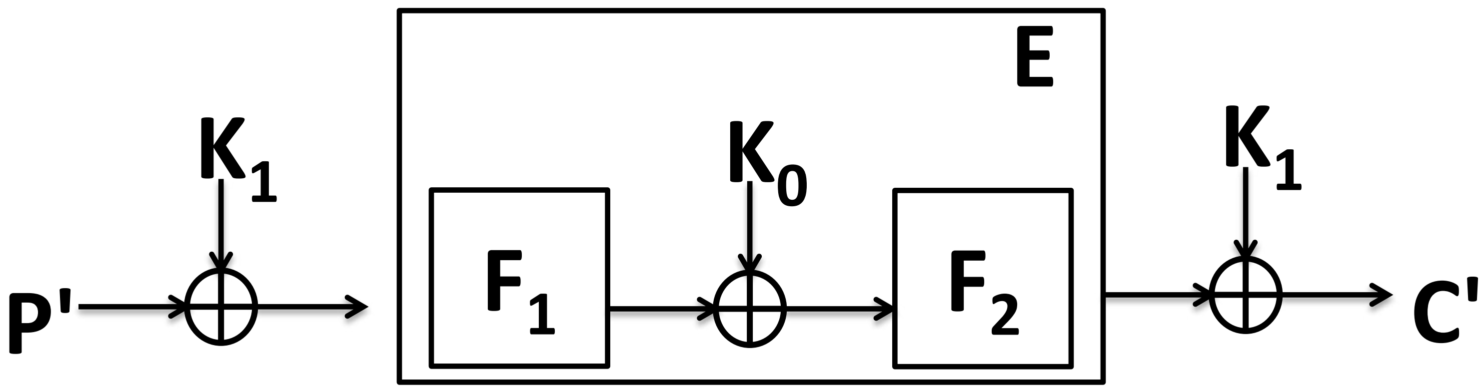
Application to 4-Step LED-128

- Guess K_0





- Recover K_1



Comparison

- Model
  - ➢ Ours: ***known***-plaintext
  - ➢ Previous: ***chosen***-plaintext
- Complexity

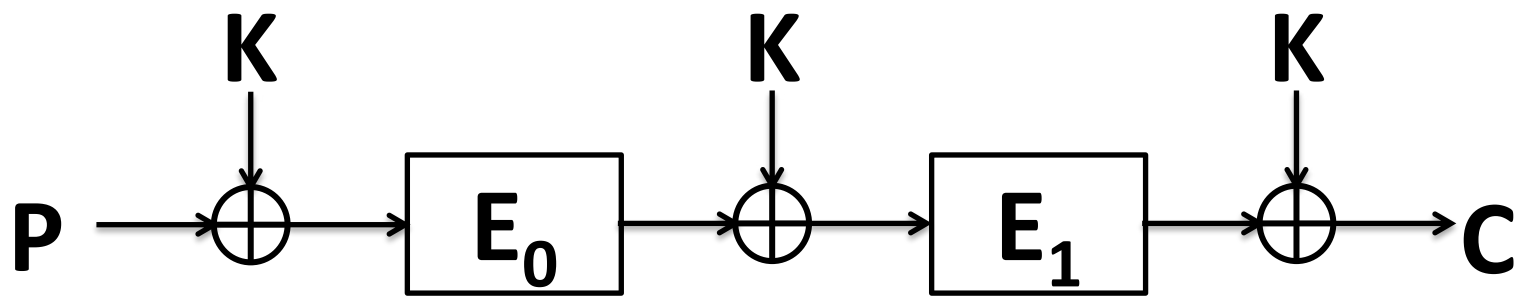
	Data	Time
IS12	2^{16}	2^{112}
MRT+12	2^{64}	2^{96}
Ours	2^{32}	2^{96}

Outline

- Backgrounds
  - Specification
  - Previous Analysis
- Slidex Attack Application
- **Multicollision Application**
- Distinguishers
  - Differential Property
  - Random-difference Distinguisher
- Conclusion

A 2-Step Even-Mansour

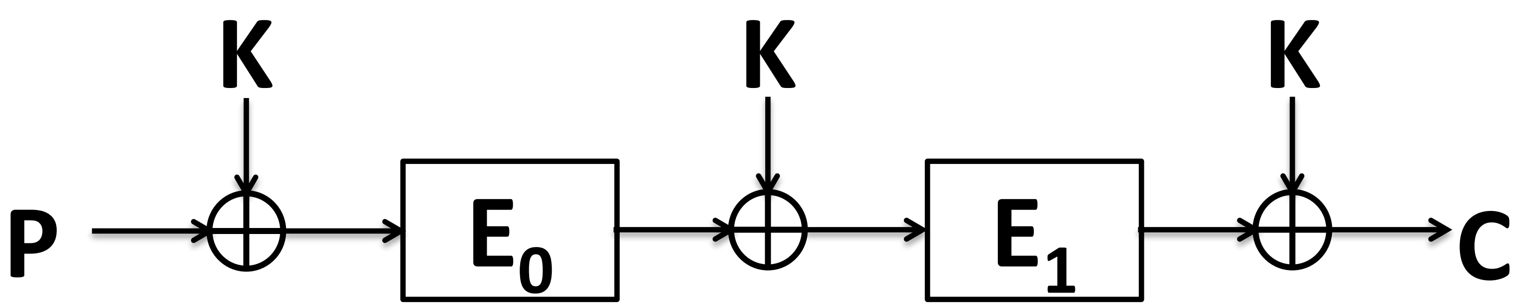
- K is n bits long
- E_0 and E_1 are public permutations



A 2-Step Even-Mansour

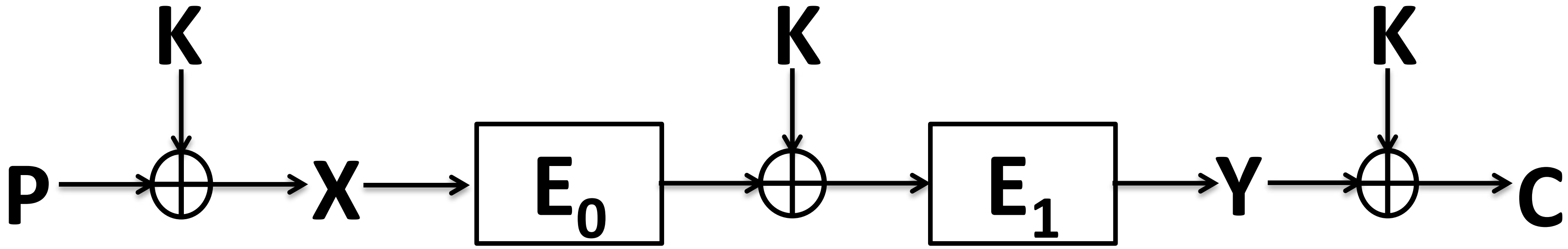
- K is n bits long
- E_0 and E_1 are public permutations

Can we recover K with a complexity less than 2^n?



An Observation (1/7)

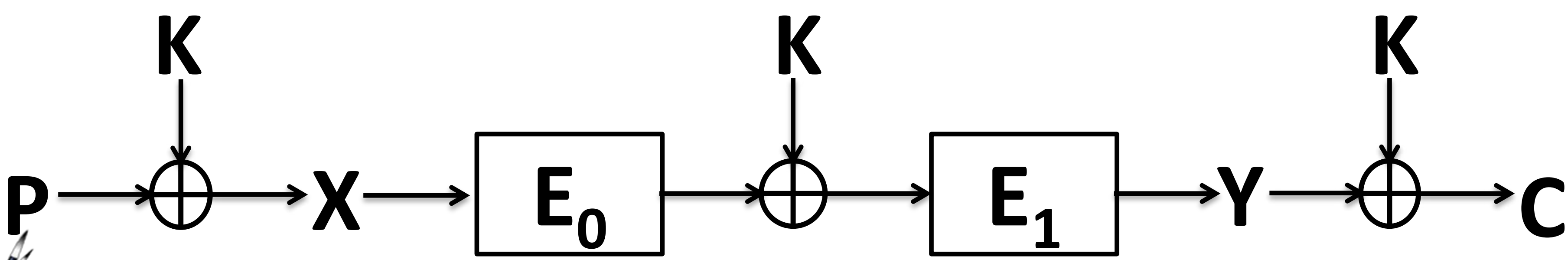
- $K = P \oplus X$
- $K = E_0(X) \oplus E_1^{-1}(Y)$
- $K = Y \oplus C$



An Observation (2/7)

- $K = P \oplus X$
- $K = E_0(X) \oplus E_1^{-1}(Y)$
- $K = Y \oplus C$

We recover X for some P, which gives us K immediately.



An Observation (3/7)

- $K = P \oplus X$
- $K = E_0(X) \oplus E_1^{-1}(Y)$
- $K = Y \oplus C$

$$\Downarrow$$

$$P = X \oplus E_0(X) \oplus E_1^{-1}(P \oplus C \oplus X)$$

An Observation (4/7)

- $K = P \oplus X$
- $K = E_0(X) \oplus E_1^{-1}(Y)$
- $K = Y \oplus C$

$$P = X \oplus E_0(X) \oplus E_1^{-1}(\boxed{P \oplus C} \oplus X)$$

An Observation (5/7)

- For a t-multicollision on $P \oplus C$, namely

$$P_1 \oplus C_1 = \dots = P_t \oplus C_t = \text{const}$$

we get

$$P_i = X_i \oplus E_0(X_i) \oplus E_1^{-1}(\text{const} \oplus X_i)$$

An Observation (6/7)

- For a t-multicollision on $P \oplus C$, namely

$$P_1 \oplus C_1 = \dots = P_t \oplus C_t = const$$

we get

$$P_i = X_i \oplus E_0(X_i) \oplus E_1^{-1}(const \oplus X_i)$$

denoted as

$$P_i = G(X_i)$$

An Observation (7/7)

- For a t-multicollision on $P \oplus C$, namely

$$P_1 \oplus C_1 = \dots = P_t \oplus C_t = \text{const}$$

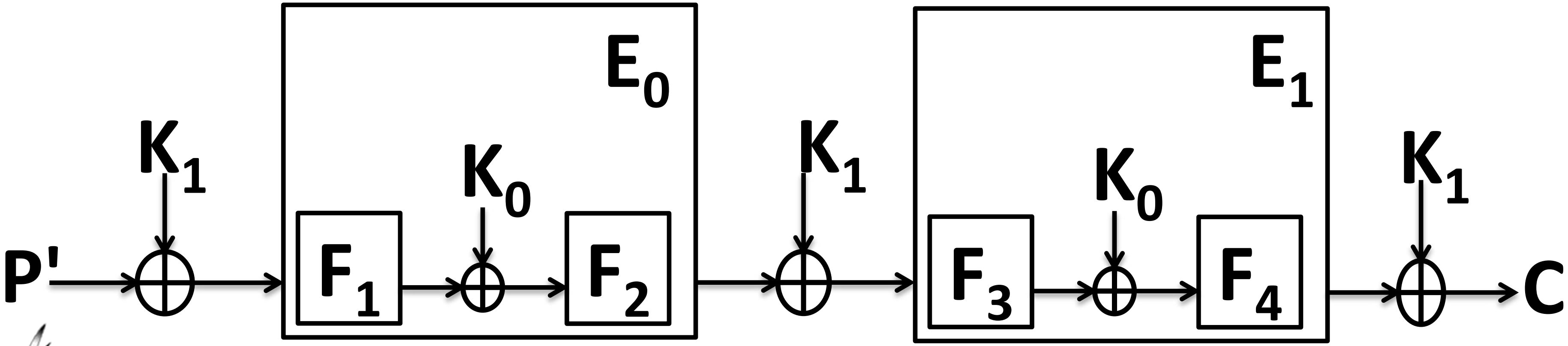
we recover a X_i with a complexity $2^n/t$

➢ try $2^n/t$ random values as X, and match G(X) to $\{P_1, P_2, \dots, P_t\}$.

Application to 6-Step LED-128

- Guess K_0

- Recover K_1

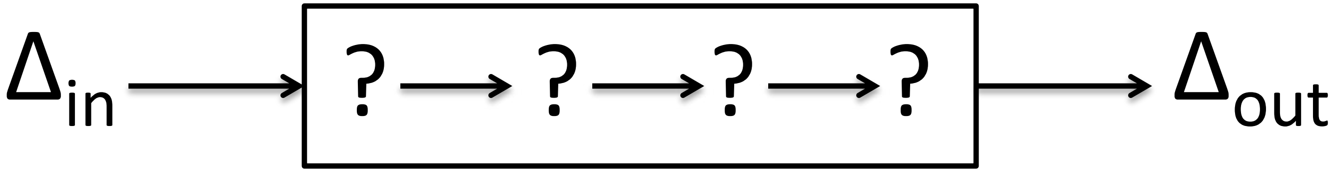


Outline

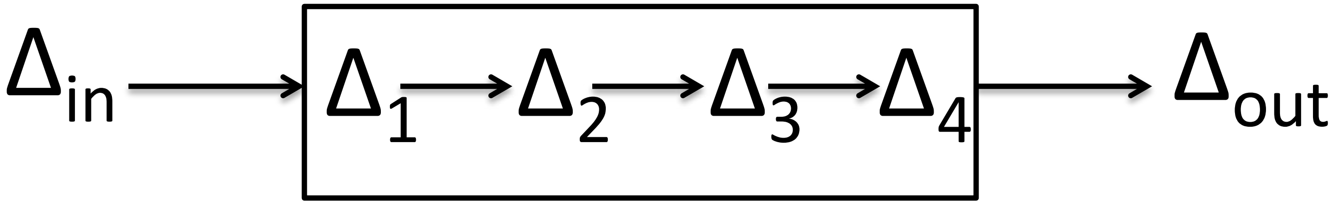
- Backgrounds
  - ➢ Specification
  - ➢ Previous Analysis
- Slidex Attack Application
- Multicollision Application
- **Distinguishers**
  - ➢ **Differential Property**
  - ➢ **Random-difference Distinguisher**
- Conclusion

Differential vs Characteristic

- Differential



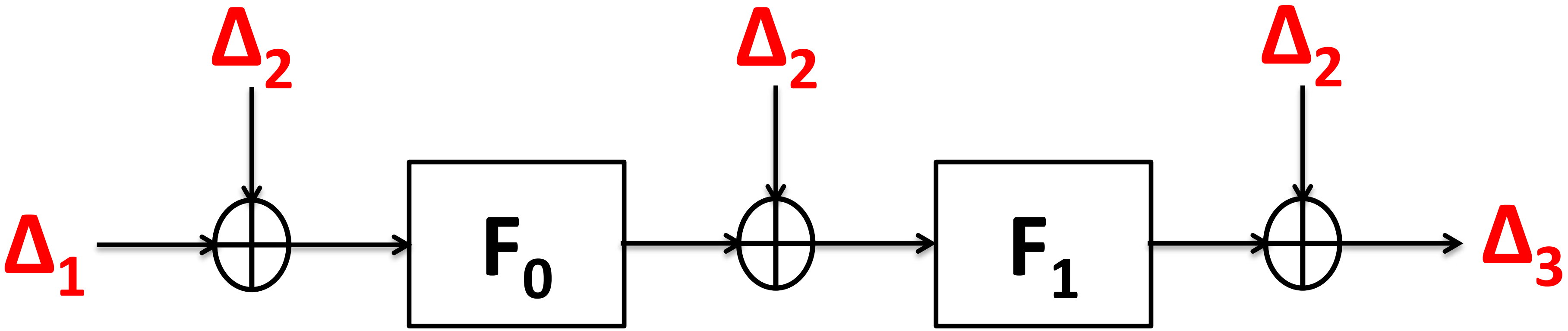
- Characteristic



  - ➢ The characteristic probability on **an active step function** is upper bounded by $\mathbf{2^{-50}}$.

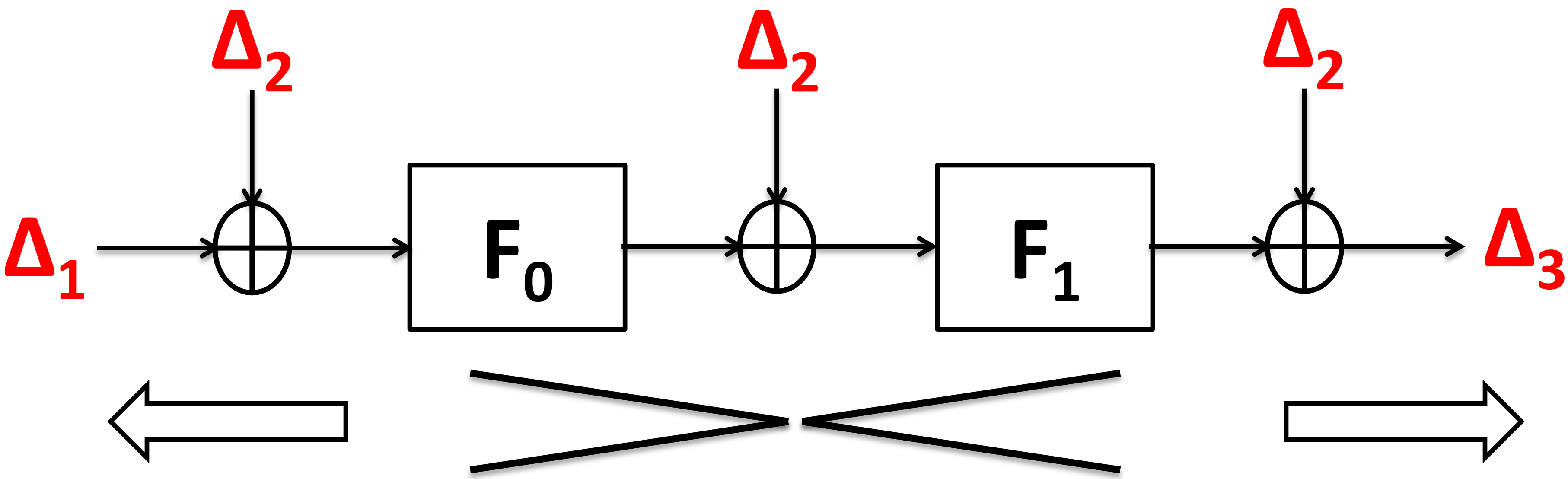
Differential on 2-step LED-64

- For a differential $(\Delta_1, \Delta_2) \longrightarrow \Delta_3$
  - what is the complexity of finding a solution (P, K)?



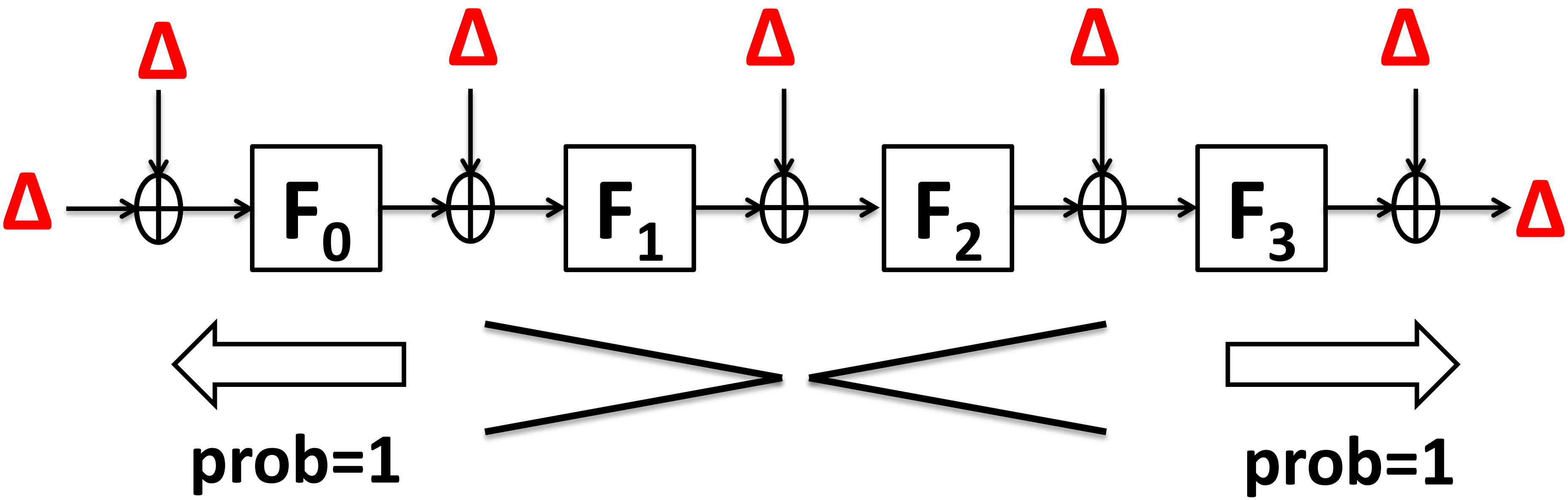
Differential on 2-step LED-64

- Meet-in-the-middle approach
  - One solution with a **birthday** complexity
- Differential multicollision distinguisher



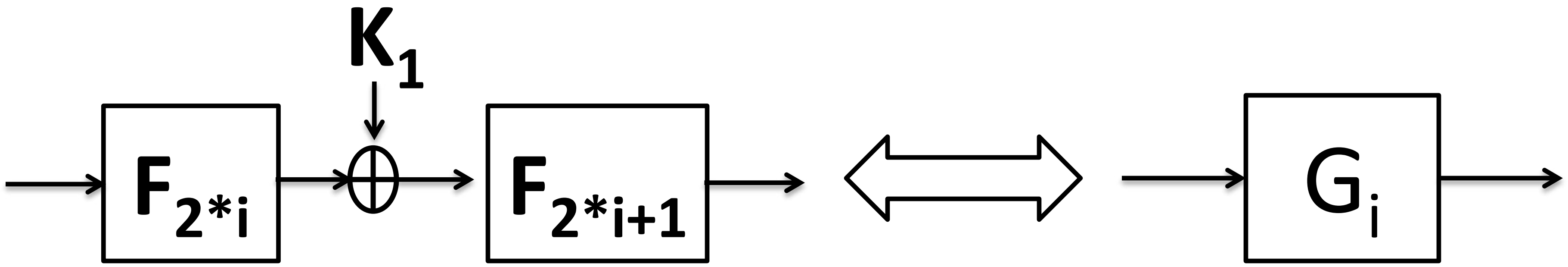
Extend to 4-Step LED-64

- **Chosen** differentials (Δ, Δ)⟶Δ
  - Complexity of **birthday bound** to find a solution (P, K).

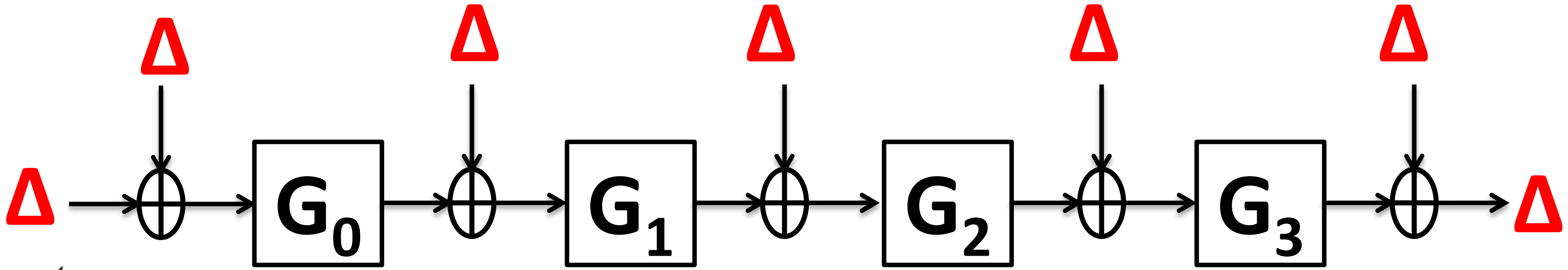


Application to 8-Step LED-128

- Set a random value to K_1 and $\Delta K_1=0$



- Set $\Delta P=\Delta K_0=\Delta$, and find a solution (P, K_0)

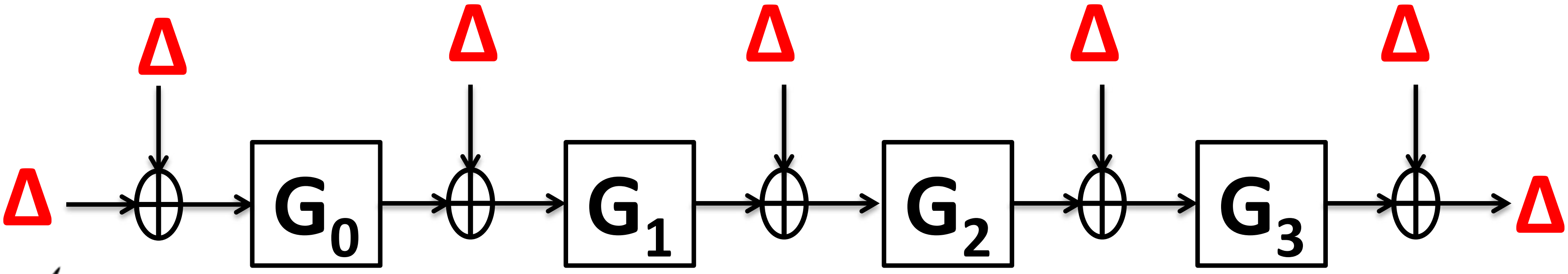


Application to 8-Step LED-128

- Set a random value to K_1 and $\Delta K_1=0$

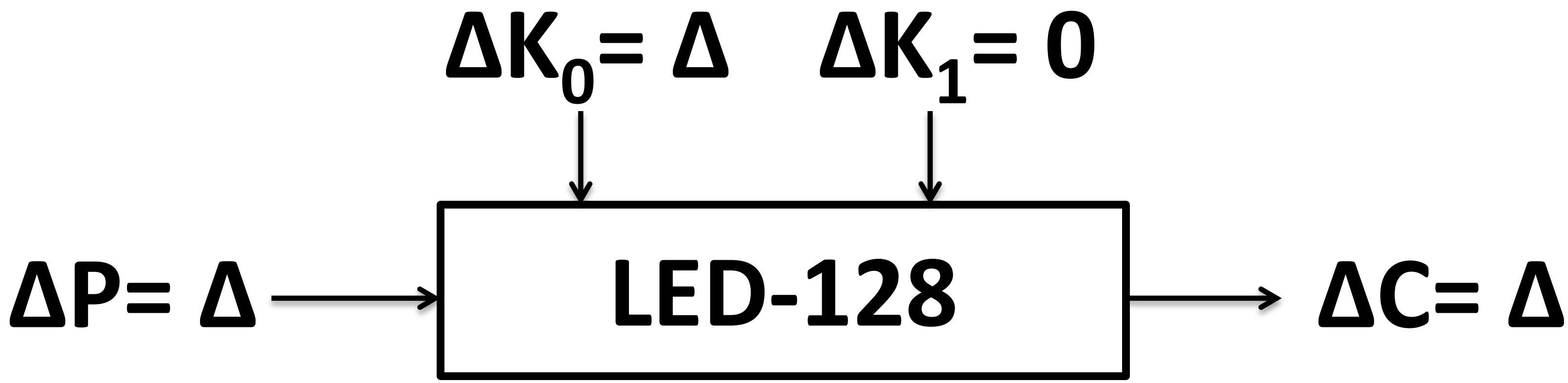
Exploit the freedom of both K_0 and K_1

- Set $\Delta P=\Delta K_0=\Delta$, and find a solution (P, K_0)



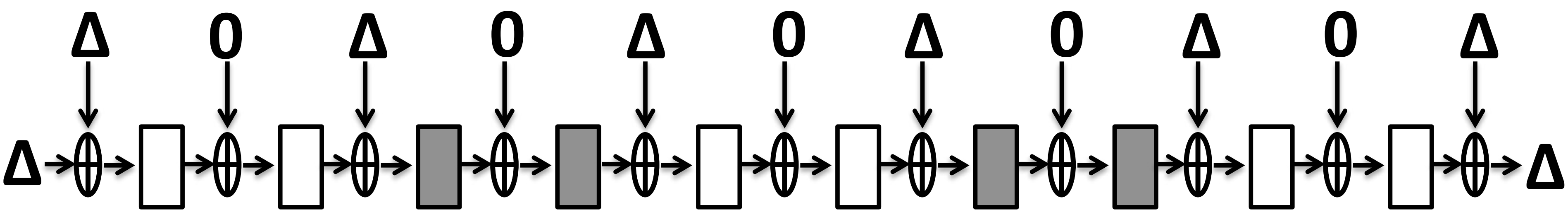
Random-Difference Distinguisher

- On a **random** difference Δ
  - Set $\Delta K_0=\Delta$, $\Delta K_1=0$, $\Delta P=\Delta$ and $\Delta C=\Delta$
  - The complexity of finding a solution?
  - Ideal case: 2^n ($n=64$)



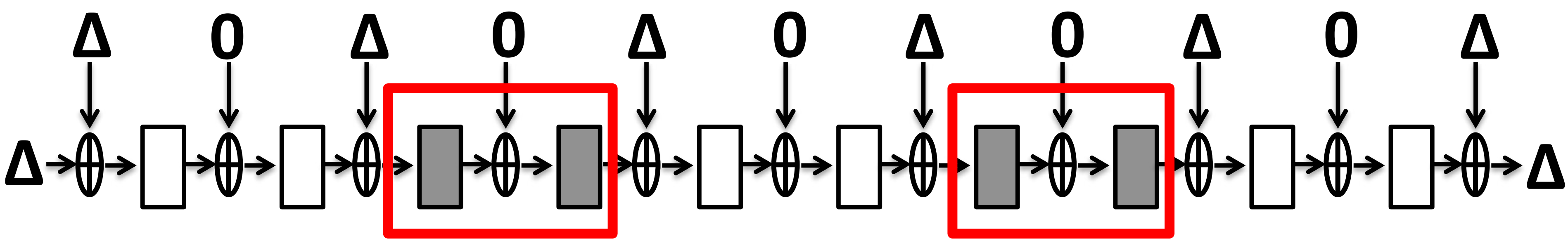
Distinguisher on 10 Steps

- Difference propagation
  - Passive step function
  - Active step function



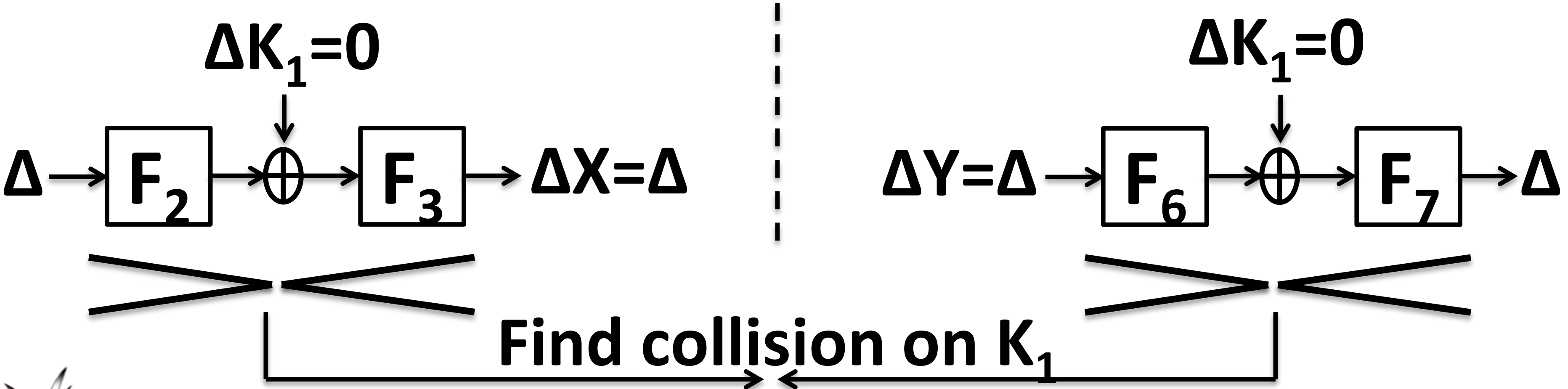
Attack Procedure (1/3)

- **Phase 1**: find solutions for differentials on F_2 and F_3, and on F_6 and F_7.
  - ➢ Exploit the freedom of K_1
  - ➢ At Phase 1, the value of K_1 is chosen.



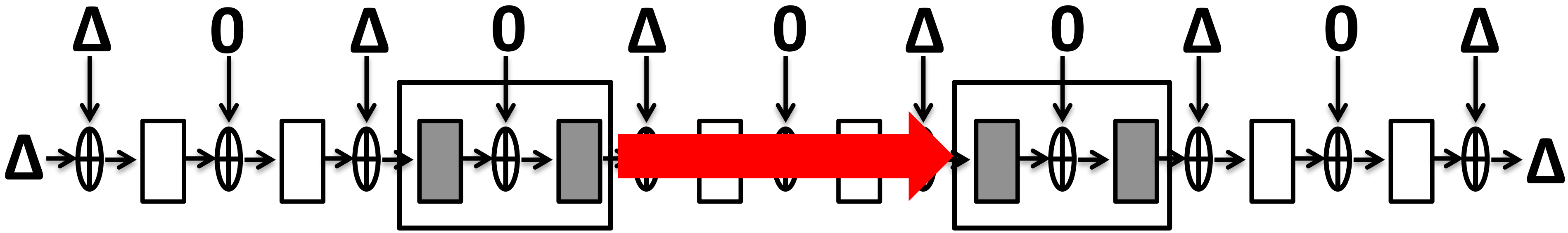
Phase 1

- Find a set of (K_1, X_i, Y_i)s such that
  - all K_1s are equal
  - (K_1, X_i)s follows differential on F_2 and F_3
  - (K_1, Y_i)s follows differential on F_6 and F_7



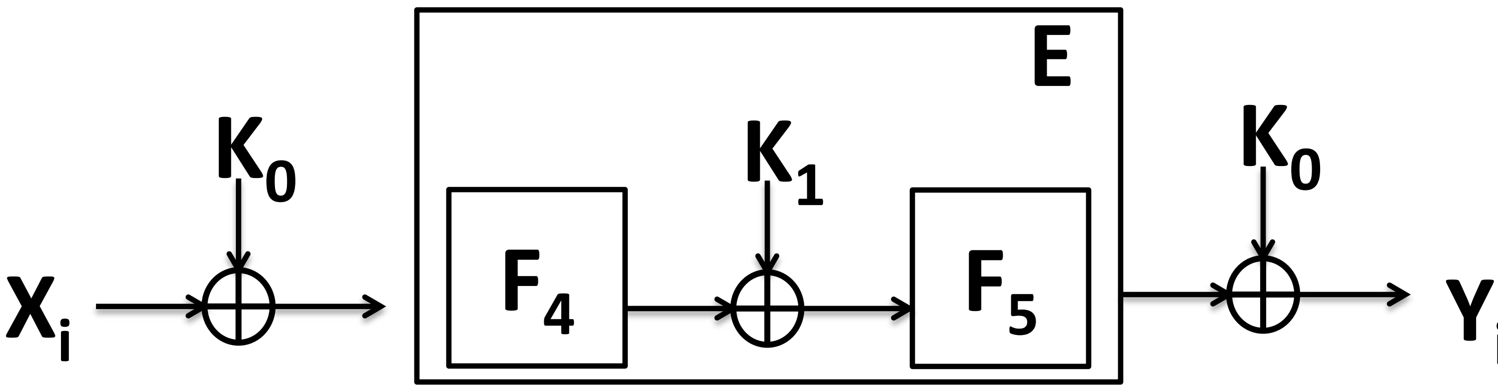
Attack Procedure (2/3)

- **Phase 2**: match a solution on F_2 and F_3 to a solution on F_6 and F_7
  - ➢ Exploit the freedom of K_0
  - ➢ At Phase 2, the value of K_0 is chosen.



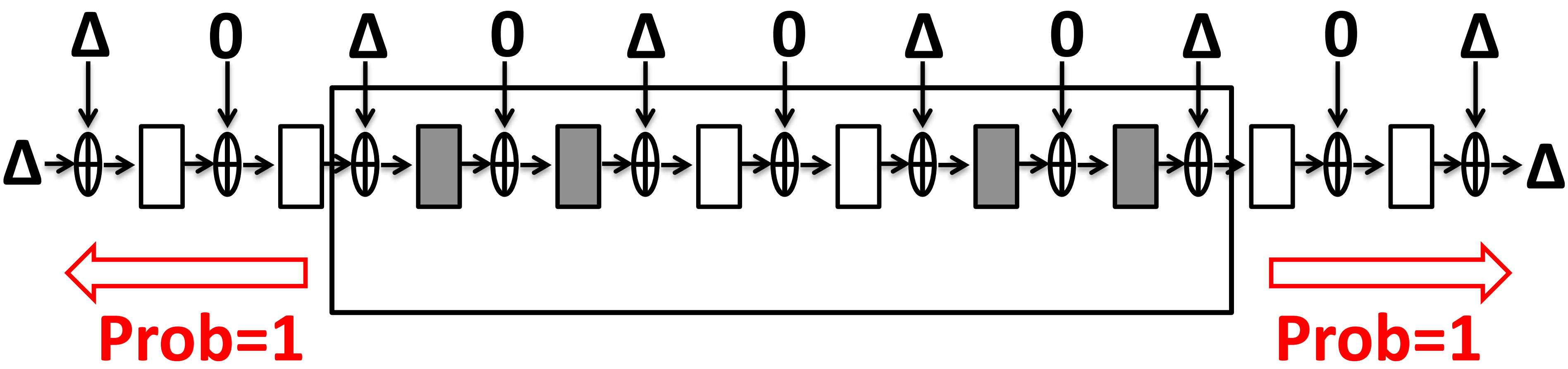
Phase 2

- Similar with the key-recovery attack on single-key 1-step Even-Mansour
  - Utilize the set $\{(K_1, X_i, Y_i)\}$ from Phase 1.



Attack Procedure (3/3)

- **Phase 3**: compute P to obtain a solution (P, K_0, K_1).



Distinguisher

- The complexity of our attack is $2^{60.3}$, which is smaller than 2^{64}
  - 10-step LED-128 is ***"non-ideal"***
- Irrespective to the specification of step function.

Outline

- Backgrounds
  - Specification
  - Previous Analysis
- Slidex Attack Application
- Multicollision Application
- Distinguishers
  - Differential Property
  - Random-difference Distinguisher
- **Conclusion**

Updated State of LED

- The number of attacked steps

	Key Recovery		Distinguisher
	Single-key	Related-key	
LED-64 (8 steps)	2	4	**3.75 → 5**
LED-128 (12 steps)	**4 → 6**	6	**6.75 → 10**

Thank you for your attention!