Differential Cryptoanalysis of the Full 16-round DES

Adi Shamir, Eli Biham

2022350222 Won Sangyun

Background

Background

: old attacks & limits

- ***Charm & Evertse*** : reduced variants of DES (6-round attack in 2^{54}) - But not applicable for 8 or more rounds DES

- ***Davies*** : Known Plaintext Attack (8-round attack in 2^{40}) - But not applicable for 16-round Full DES

- Most successful attack - **Differential Cryptoanalysis** (15-round attack faster than exhaustive search, but not in 16-round Full DES also)

Enhanced this Differential Cryptoanalysis to 16-round DES with less prob.

Differences

: New attack & Advantages

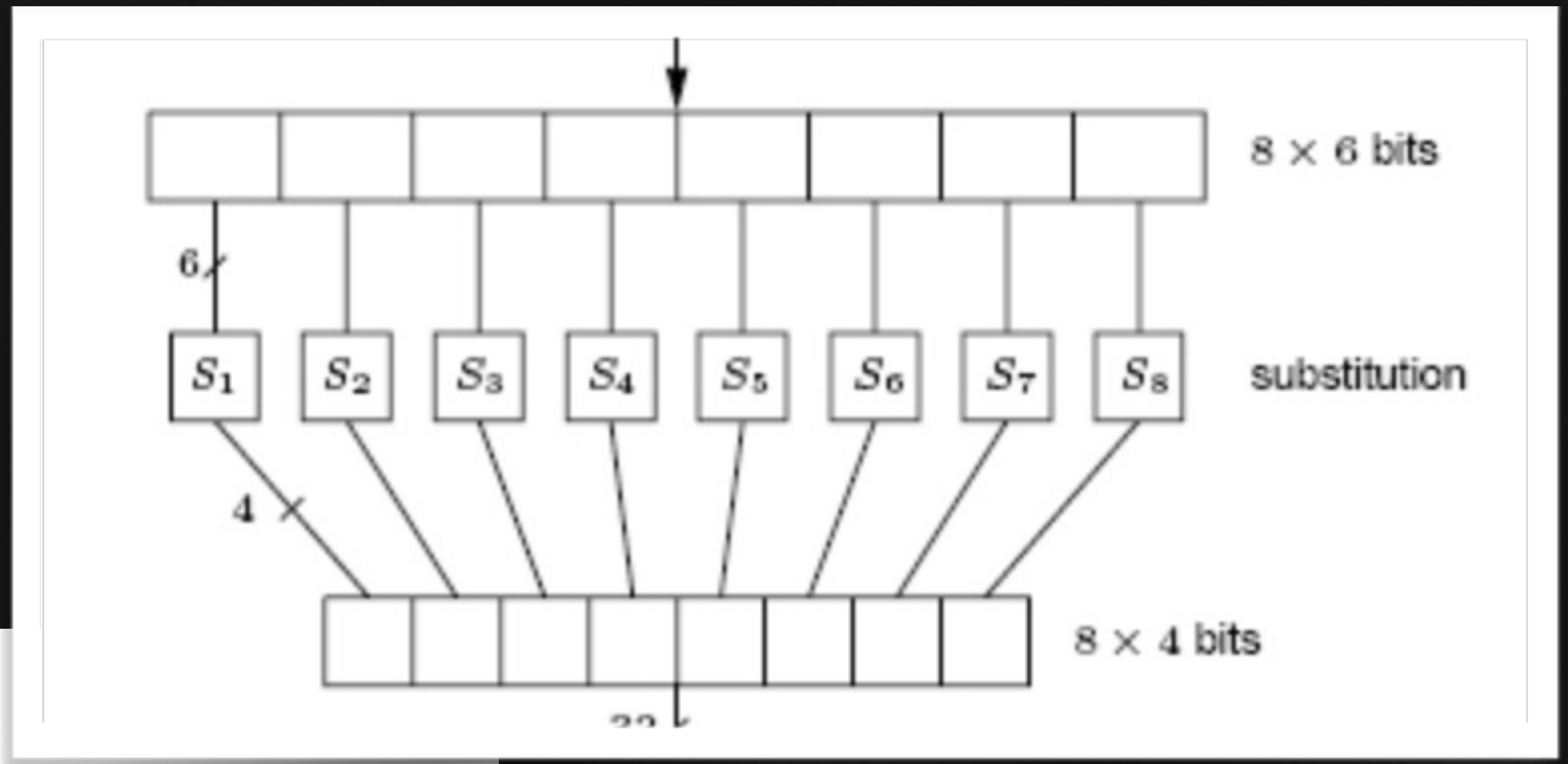
- Breaking 16-round Full DES in 2^{36} plaintext with 2^{37} time.
- Even if the key changes frequently, the attack will have same complexity. But for example, in bank authentication schemes, this attack has to act quickly before the key changes… → the (plaintext-ciphertext) pairs' pool for attack needs to be encrypted with the same keys
- Needs negligible space (memory) because it uses no counter.

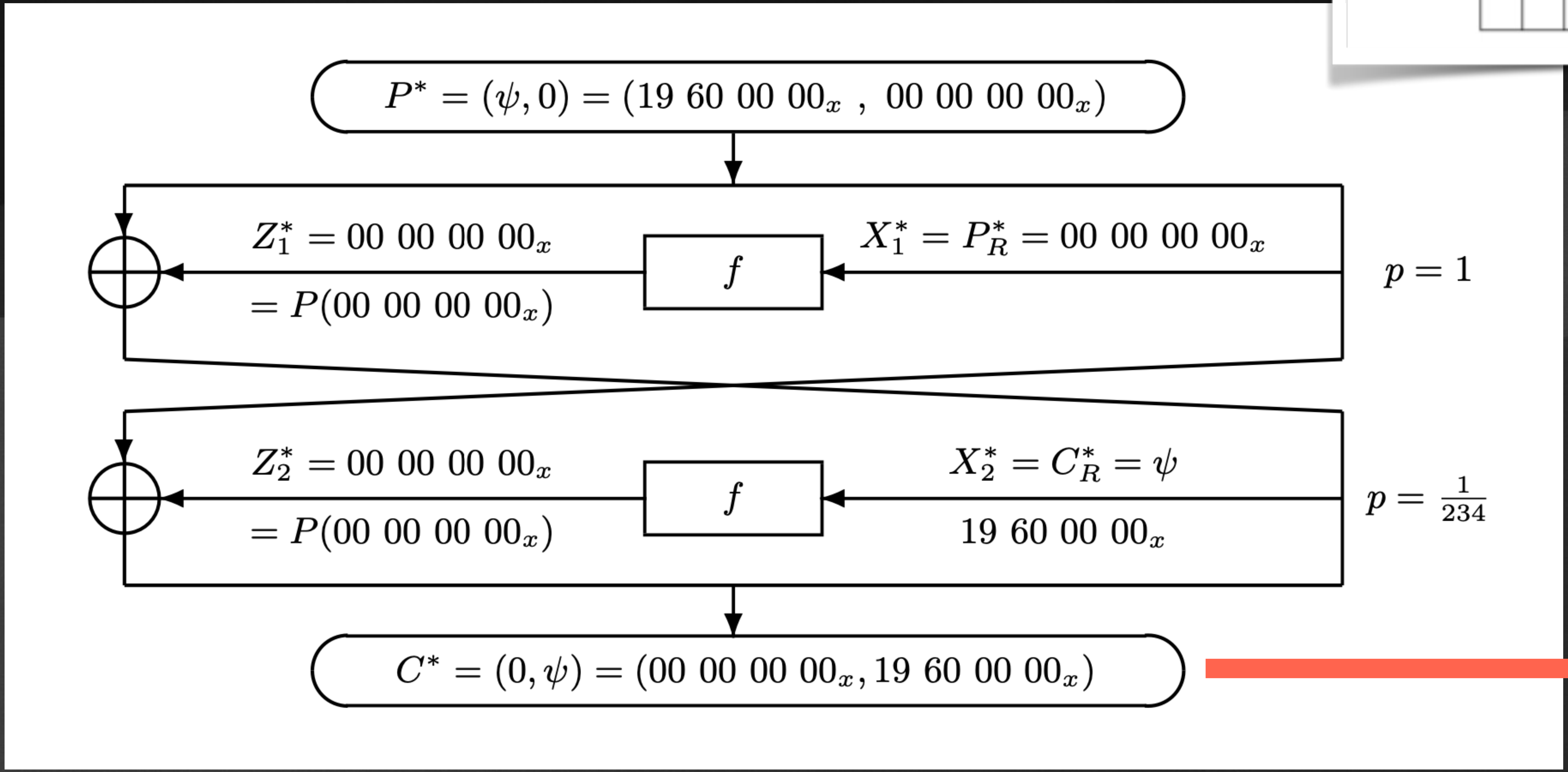
How to analyze DES?

Differential Cryptoanalysis

: First idea - DC characteristic

Function f





$$f(\psi) = 00 \cdots 00$$

$$S_1 \times S_2 \times S_3$$

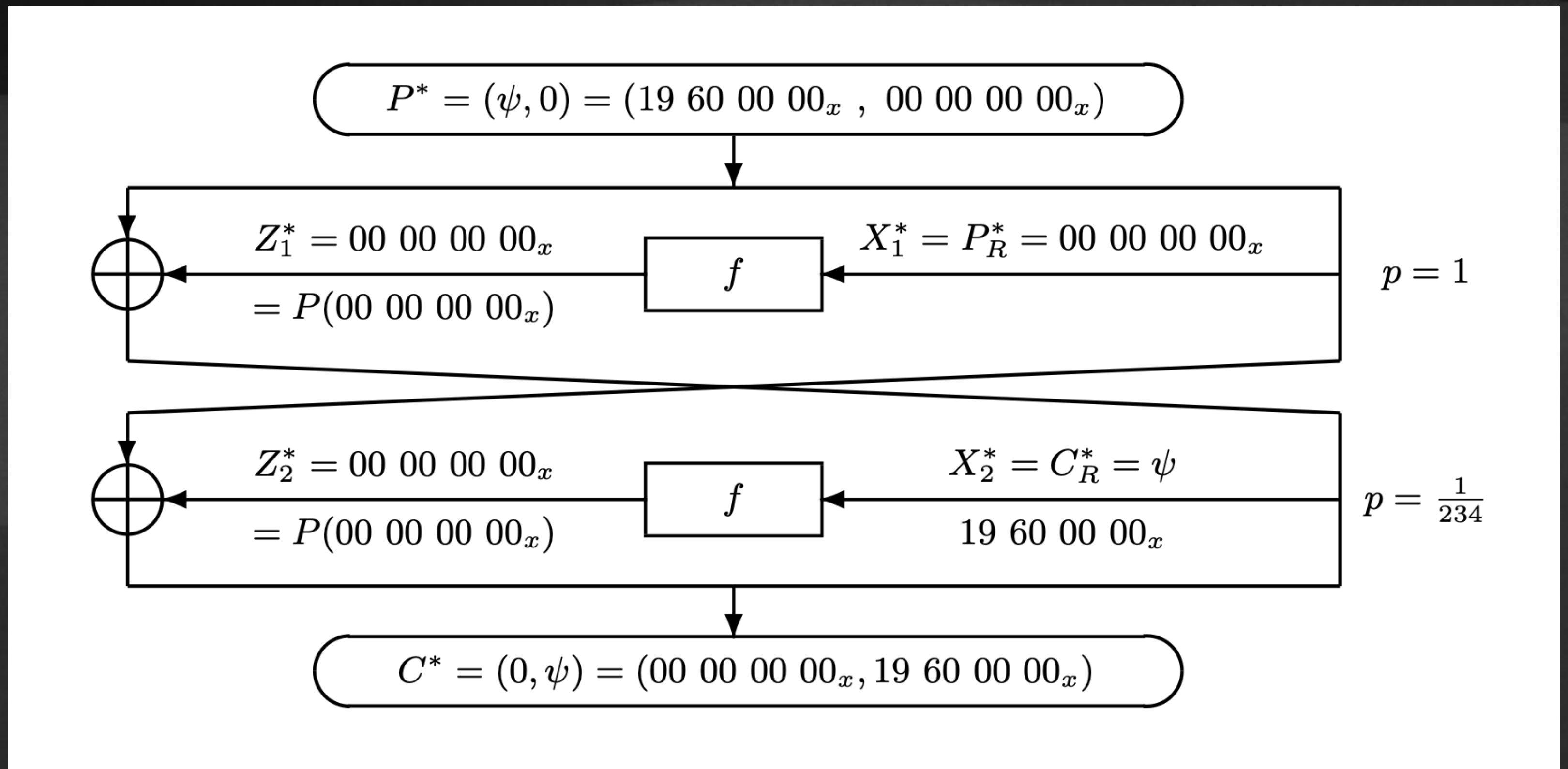
$$\frac{14}{64} \times \frac{8}{64} \times \frac{10}{64} \approx \frac{1}{234}$$

A constant plaintext is repeated continuously.

How can I use it??

: repeat 6.5 times

- If input = output, very useful DC characteristic !!
- Let's compare with exhaustive search (brute-force)

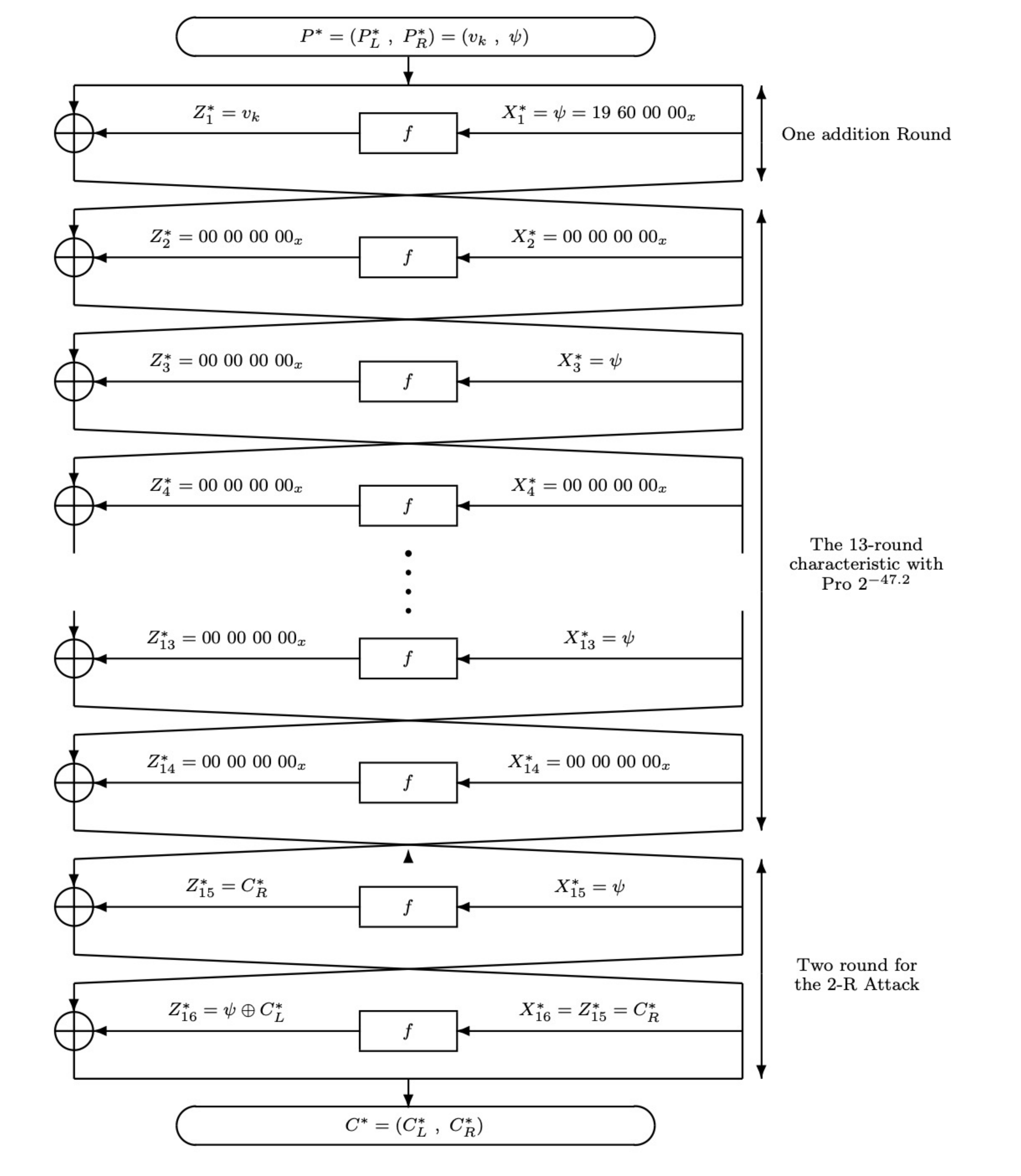


- Exhaustive search : 2^{55} complex
- How many rounds can we use it to make lower complex than exhaustive search??

$\rightarrow {\frac{1}{234}}^{6} \approx \frac{1}{2^{47.2}}$ & ${\frac{1}{234}}^{7} \approx \frac{1}{2^{55.1}}$ so just 6 times!!

Differential Cryptoanalysis

: next step - one additional round & 2-R attack



- We solved 13 rounds with $2^{-47.2}$ prob.
- In 16-round Full DES, there are 3 rounds left..
- We need to append 3 rounds without making the prob lower…

→ ***one additional round & 2-R attack***

One additional round

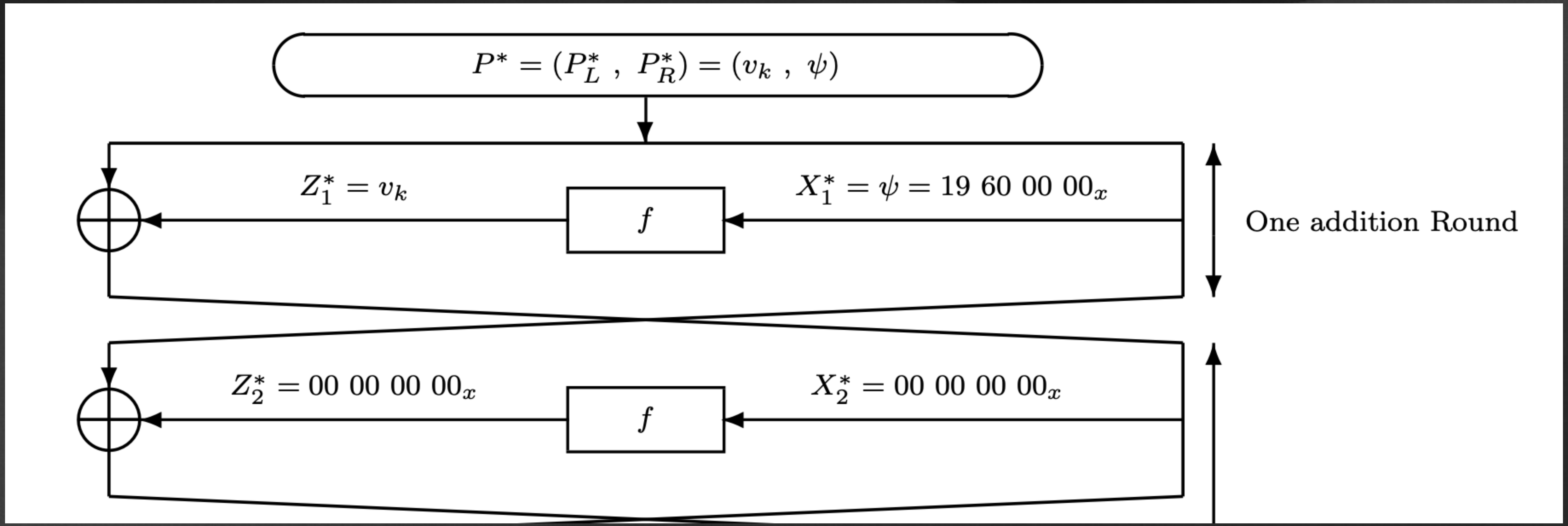
: using plaintext pairs

1. Make random plaintext : P
2. Let $P_i = P \oplus (\alpha_i, 0)$ and $\overline{P_i} = P \oplus (\alpha_i, \psi)$ for $\alpha_i = ABC00000$ format (Because of the format of α, number of α is 2^{12})
3. Let $P = P_1|P_2$ and P_2 is the right block of plaintext P.
4. Then, P_2 are all the same for P_i and $\overline{P_i}$ $\rightarrow$ **output difference is constant**
5. When I choose any P_i , there must be one j that satisfies $\alpha_j = \alpha_i \oplus \alpha_k$

One additional round

: using plaintext pairs

- With one plaintext P, we can make 2^{12} pairs which matches the condition



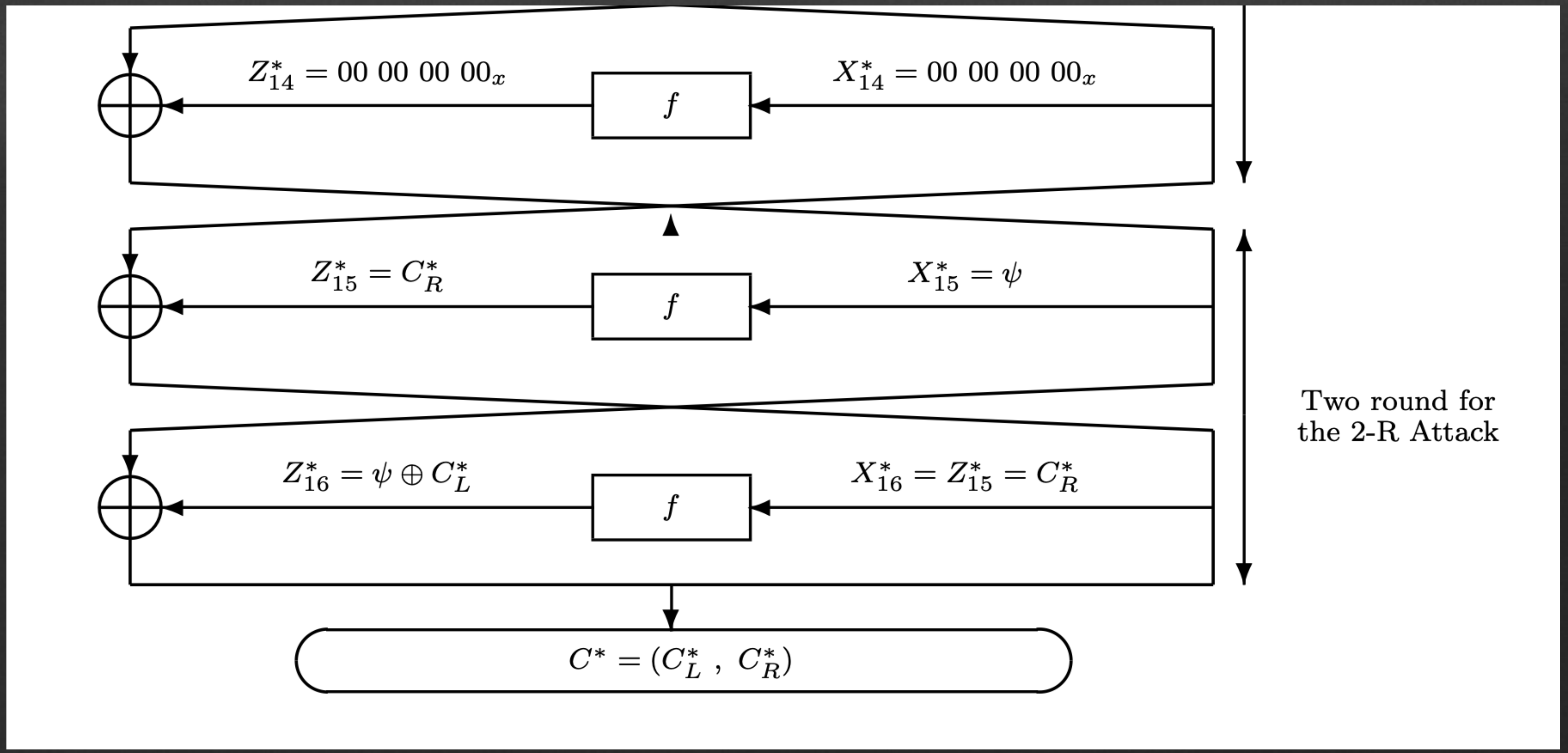
- With one P, we can have $2^{12} \times 2^{-47.2} = 2^{-35.2}$ prob that satisfies the whole Differential Cryptoanalysis !!

But..

: can’t know intermediate value of crypto system

- We should catch the right pair that satisfies our characteristic.
- So we need to brute force it !! → 2^{24} (whole pairs)

- right block of the ciphertext = $f(\psi)$
- Needs to be $ABC00000$ format
- $2^{24} \times 2^{-20} = 2^4$ candidates



Probability calculating

: how many plaintext will be..??

- We must consider 1, 15 rounds.
- 1, 15 round → S_1, S_2, S_3 possible outputs' prob → $\frac{14}{16} \times \frac{13}{16} \times \frac{15}{16}$
- In addition, when we analyze the S-Box, the average of probability of the valid input - output pair is about $\frac{8}{10}$!!
- So in result, number of possible plaintext : $2^4 \times (\frac{14}{16} \times \frac{13}{16} \times \frac{15}{16})^2 \times (\frac{8}{10})^8 \approx 1.19$

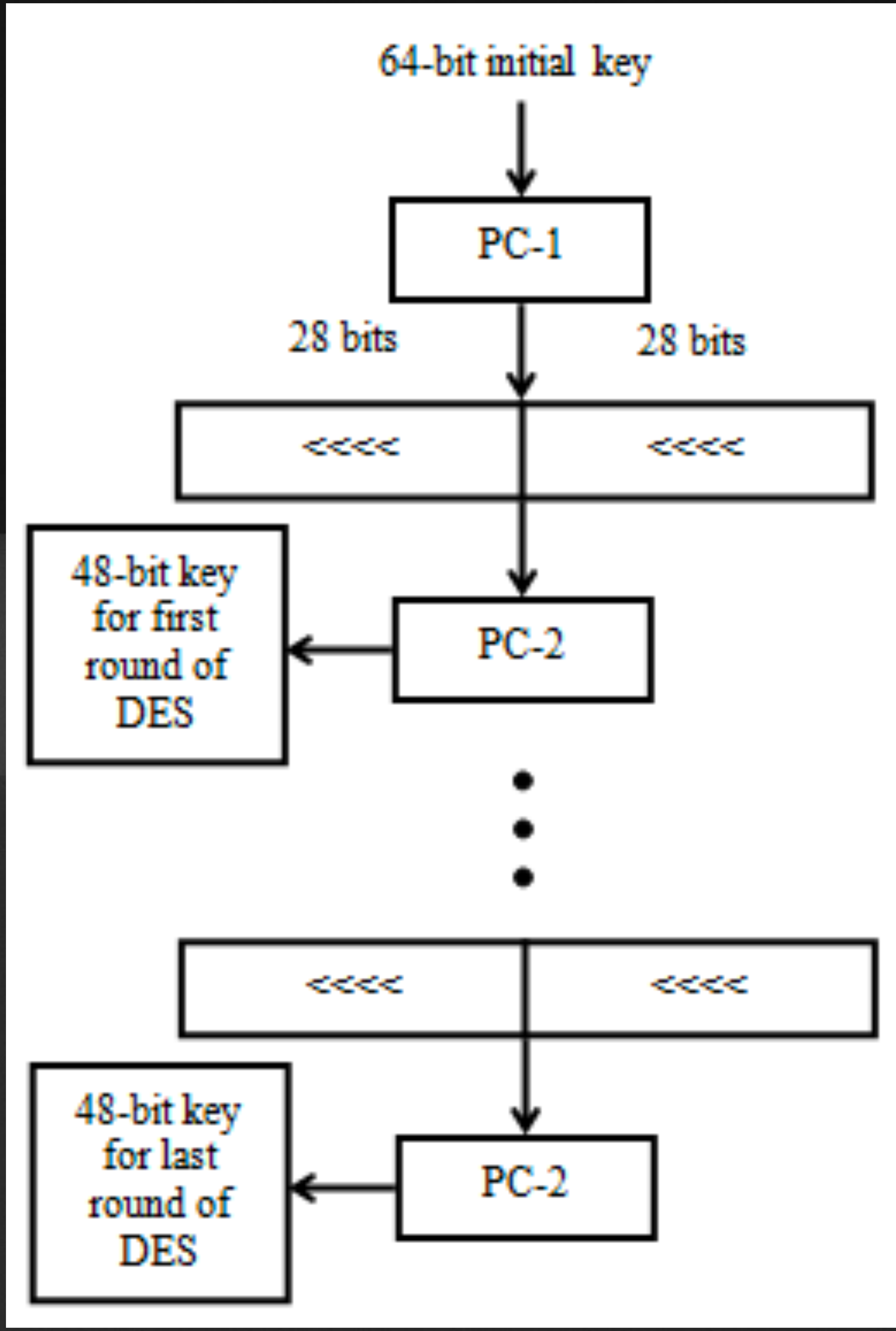
How to find key?

Key schedule

: not so complex..

라운드	필요한 S박스에 영향을 주는 키비트 위치
1 (18비트)	10 51 34 60 49 17 33 57 2 9 19 42 3 35 26 25 44 58
15 (18비트)	26 2 50 11 36 33 49 44 18 25 35 58 19 51 42 41 60 9
16 (24비트)	18 59 42 3 57 25 41 36 10 17 27 50 11 43 34 33 52 1 2 9 44 35 26 49

- Applying this a little bit, the number of bits of keys involved in the first and 15 rounds is 60, but excluding duplicates, it is **28.**
- In addition, the number of bits of the key which are used in 16 round is **24.**
- So we can calc (24 + 28) = 52 bits of the key !!



So how many plaintext?

: Comprehensive calculation

- One P per right plaintext pairs → 1.19
- One plaintext pairs per key candidates → 0.84 ($2^{52} \times \frac{2^{-32}}{0.8^{8}} \times \left(\frac{2^{-12}}{\frac{14}{16} \times \frac{13}{16} \times \frac{15}{16}}\right)^{2}$)
- One key candidates per whole key candidates → 2^{4}
- So number of key candidates per one P is $1.19 \times 0.84 \times 2^{4} \approx 16$

Finding key

: 1-16 round key bit's relation

- First round & 16th round are related closely (key schedule)
- There are duplicated key bits
- We can recover 13bit with brute-force attack !!

1 round's S3 box & 16 round's S1 box have common bits

		K_{16}									
		Left KEY Register (C)					Right KEY Register (D)				
		S_1	S_2	S_3	S_4	ETC	S_5	S_6	S_7	S_8	ETC
K_1	S_1	[illegible]	2	1	1	2	-	-	-	-	-
	S_2	2	-	1	2	1	-	-	-	-	-
	S_3	2	-	-	$\boxed{3}$	1	-	-	-	-	-
	S_4	2	3	1	-	-	-	-	-	-	-
	ETC	-	1	3	-	-	-	-	-	-	-
	S_5	-	-	-	-	-	-	1	2	2	1
	S_6	-	-	-	-	-	3	-	2	1	-
	S_7	-	-	-	-	-	-	2	-	2	2
	S_8	-	-	-	-	-	2	3	-	-	1
	ETC	-	-	-	-	-	1	-	2	1	-

Summary

: how complex is it?

Rounds	Chosen Plaintexts	Analyzed Plaintexts	Complexity of Analysis	Best Previous Time	Best Previous Space
8	2^{14}	4	2^{9}	2^{16}	2^{24}
9	2^{24}	2	2^{32}	2^{26}	2^{30}
10	2^{24}	2^{14}	2^{15}	2^{35}	—
11	2^{31}	2	2^{32}	2^{36}	—
12	2^{31}	2^{21}	2^{21}	2^{43}	—
13	2^{39}	2	2^{32}	2^{44}	2^{30}
14	2^{39}	2^{29}	2^{29}	2^{51}	—
15	2^{47}	2^{7}	2^{37}	2^{52}	2^{42}
16	2^{47}	2^{36}	2^{37}	2^{58}	—

- Complexity of the characteristic is ${\frac{1}{234}}^{6} = 2^{47.2}$
- 2^{12} pairs per one Plaintext → $2^{12} \times 2^{-47.2} = 2^{-35.2}$
- So we need more than 2^{35} plaintext !! → remaining pairs : $2^{35} \times 1.19 \approx 2^{35.25}$
- This leads to 58% attack success !!!