Cryptanalysis of White-Box DES Implementations

Brecht Wyseur

COSIC – K.U.Leuven (Belgium)
Paris, March 2007

Orientation

White-Box Attack Context

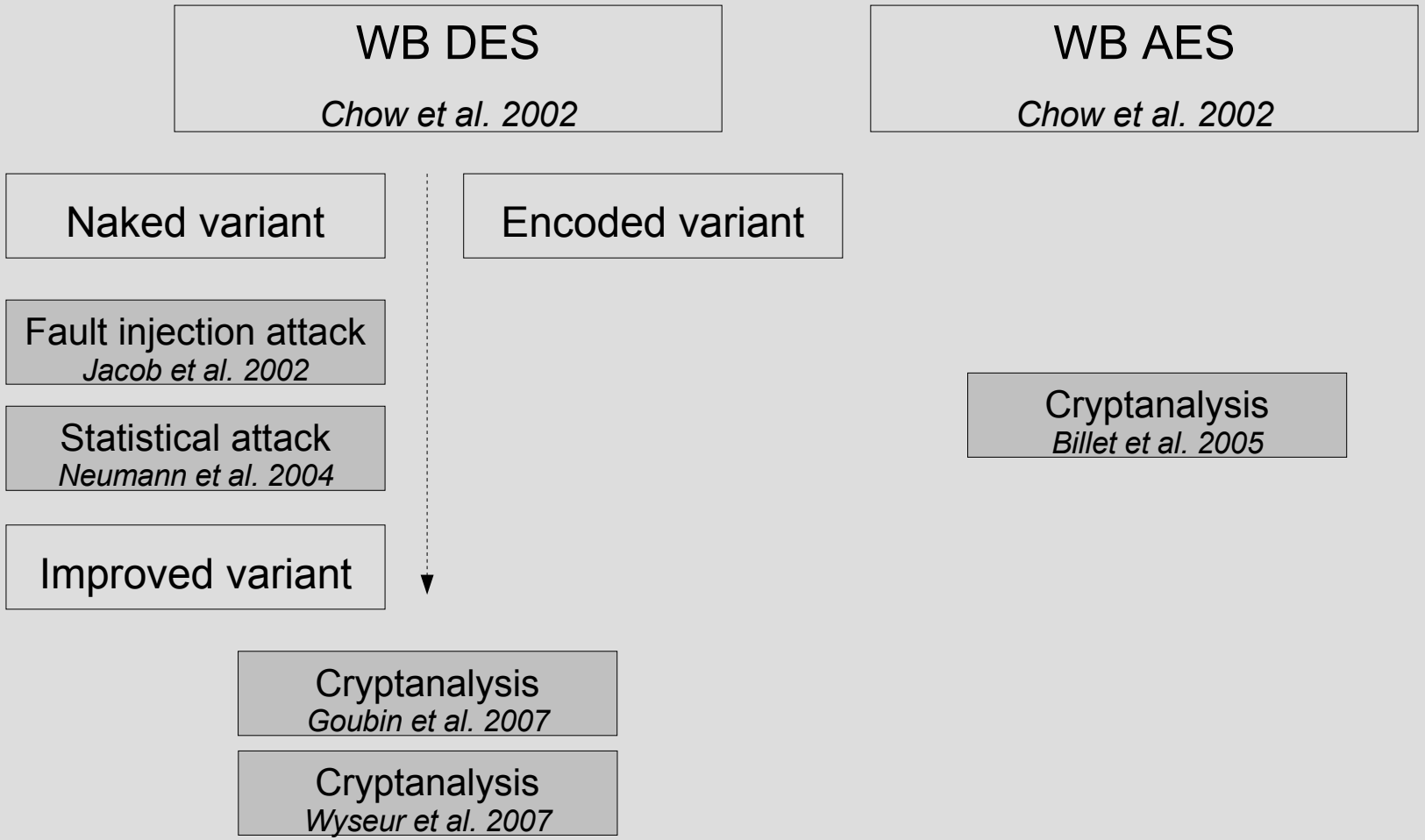
- Fully privileged attack software shares host
  => Complete access to the implementation of algorithms
- Dynamic execution can be observed
- Internal details both completely visible and alterable at will

Attacker's objective: extract the embedded cryptographic key

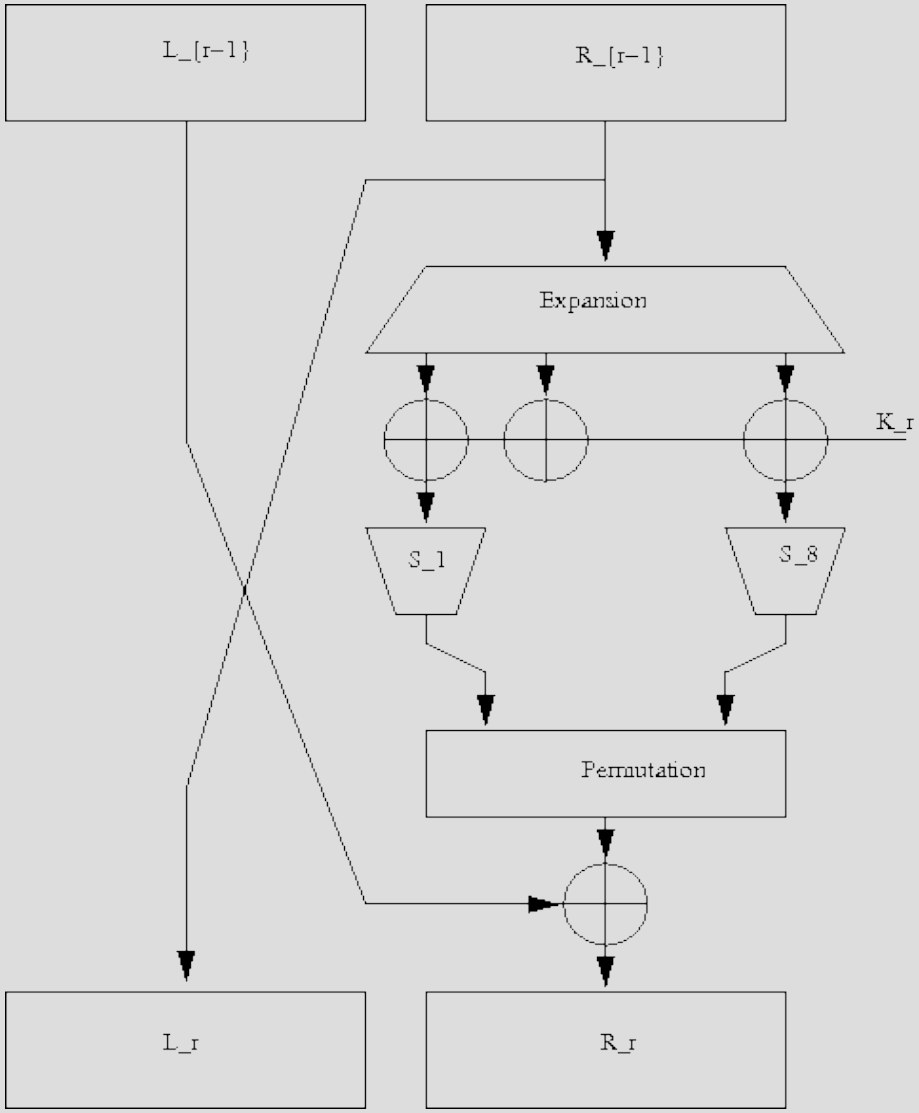
Outline

- State-of-the-art
- White-box DES implementations
- Cryptanalysis
- Demo
- Results and Conclusions

State-of-the-art



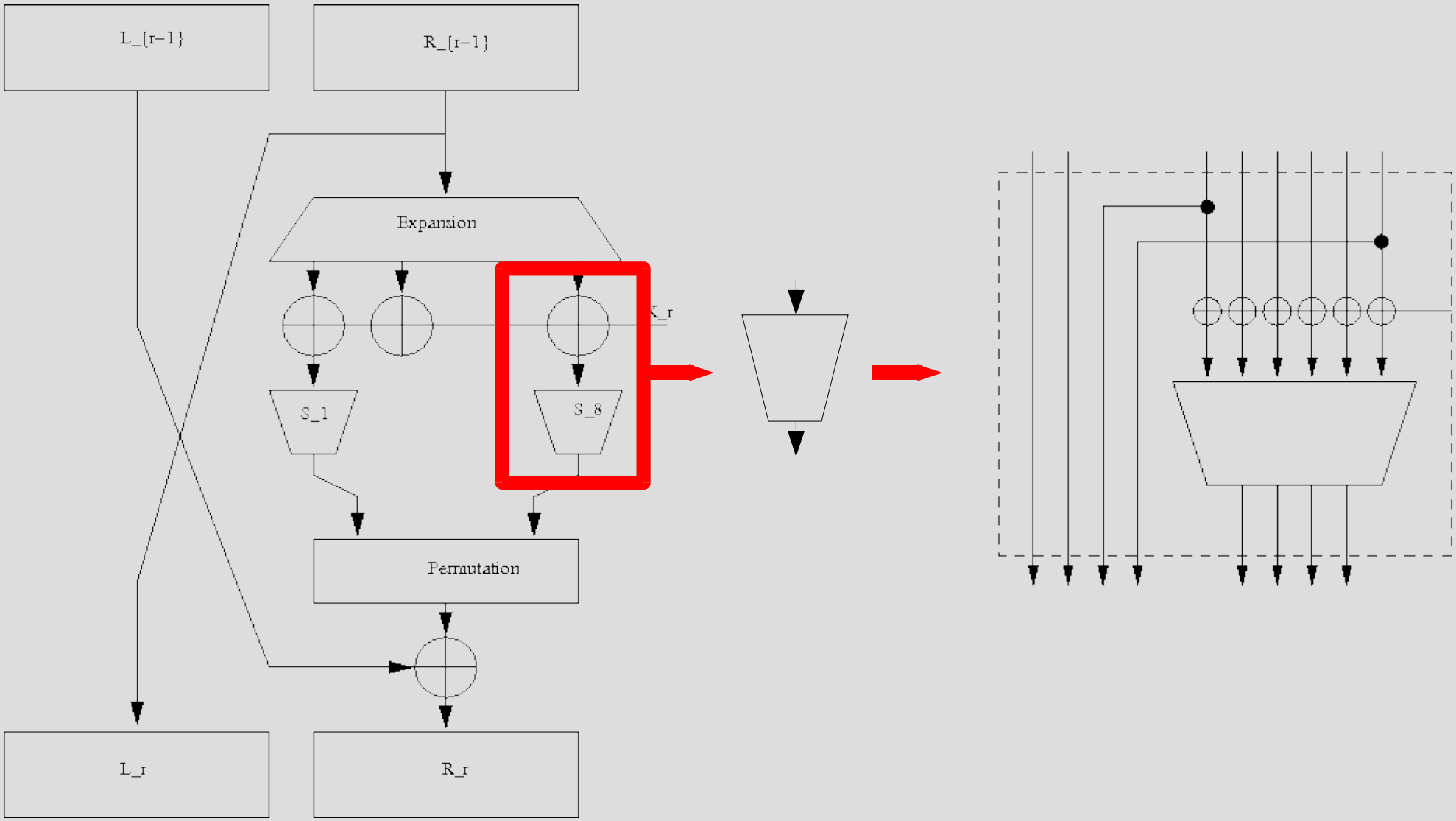
DES (Data Encryption Standard)



Overview

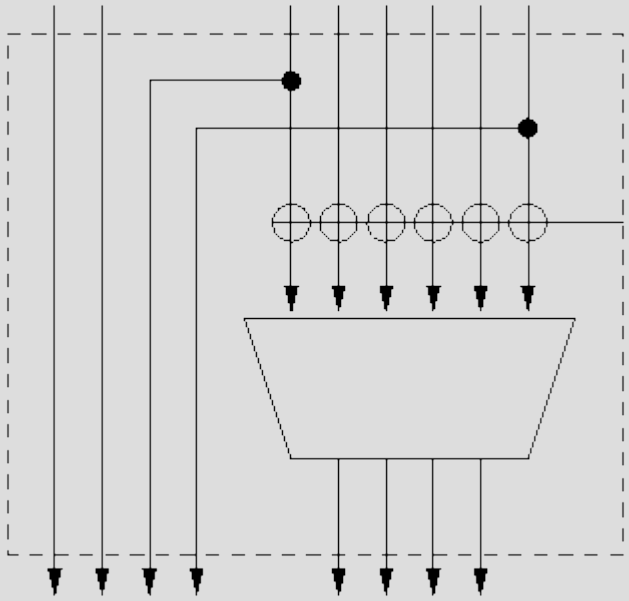
- Feistel structure
- 16 rounds
- Per round:
  - Expansion
  - RoundKey addition
  - 8 S-boxes
  - Permutation

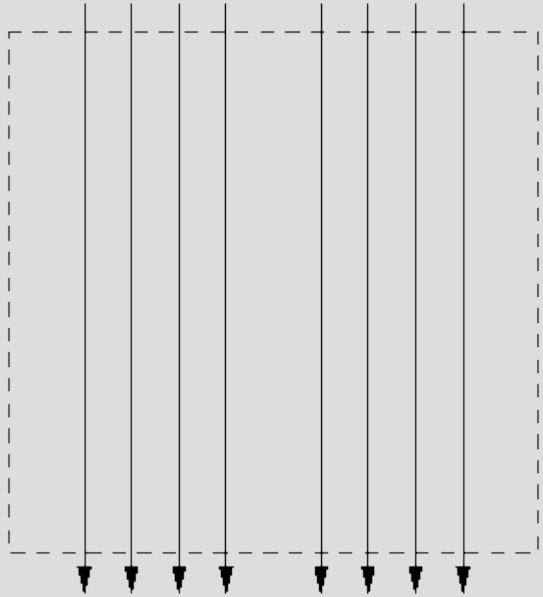
White-box transformation



White-box transformations

- T-boxes
  - 8 T-boxes with internal S-box
  - 4 Linear T-boxes (by-pass T-boxes)

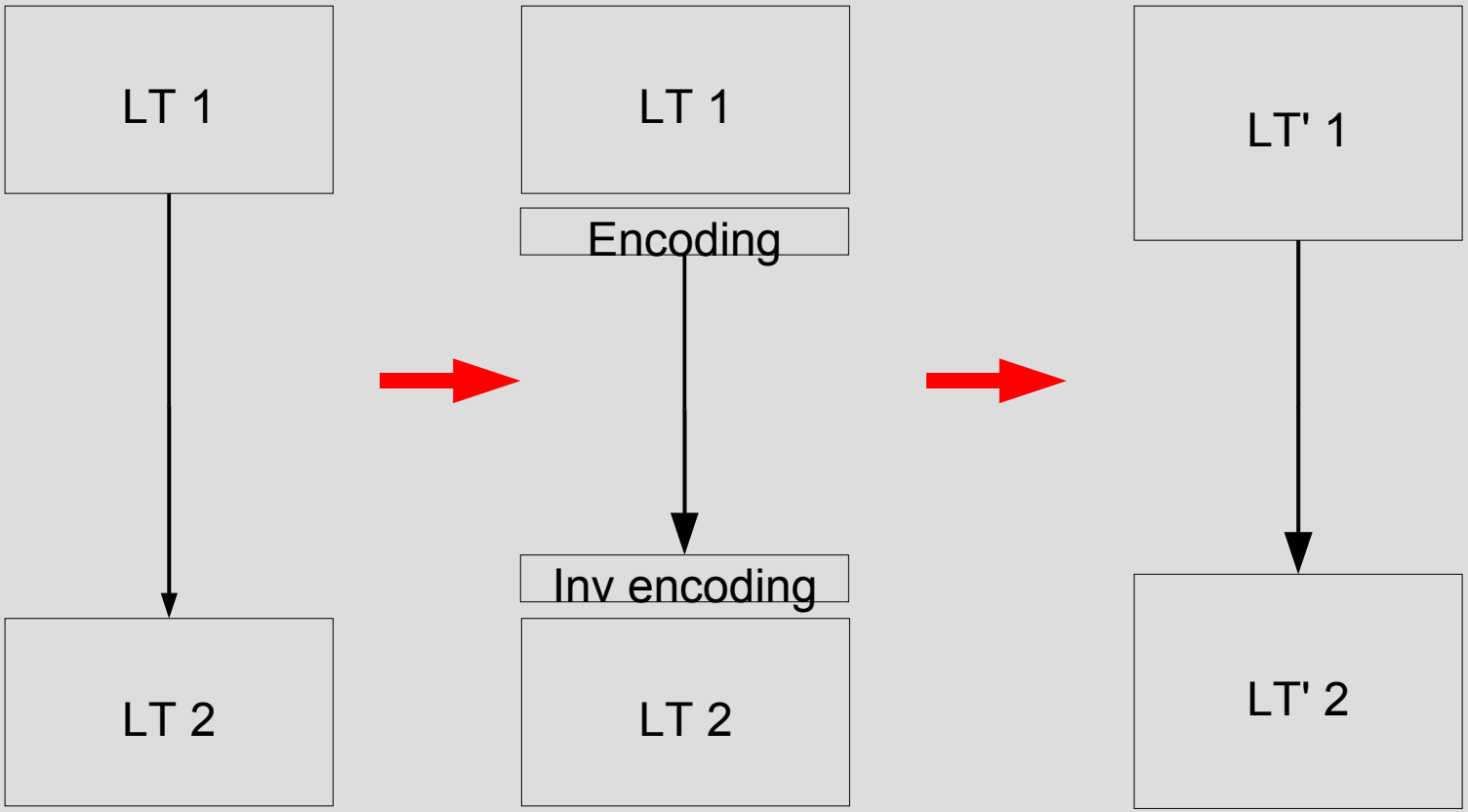




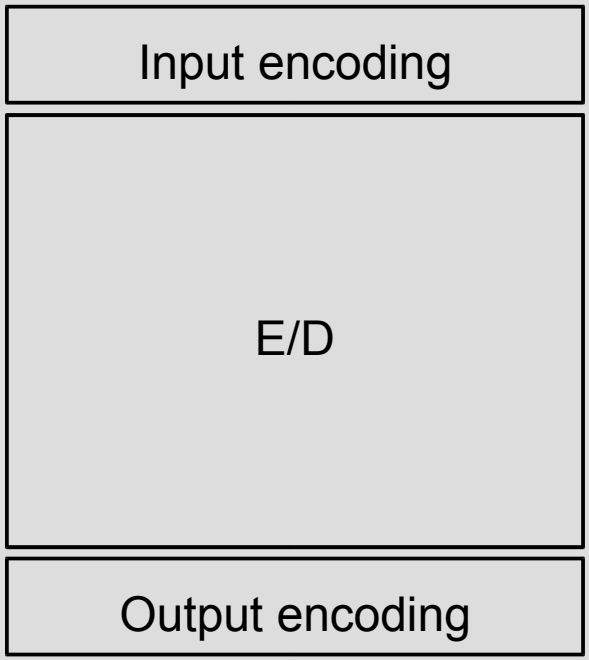
Expansion:	S1						S2						S3						
	32	1	2	3	4	5	4	5	6	7	8	9	8	9	10	11	12	13	...

White-box transformations

- Internal encodings



White-box transformations

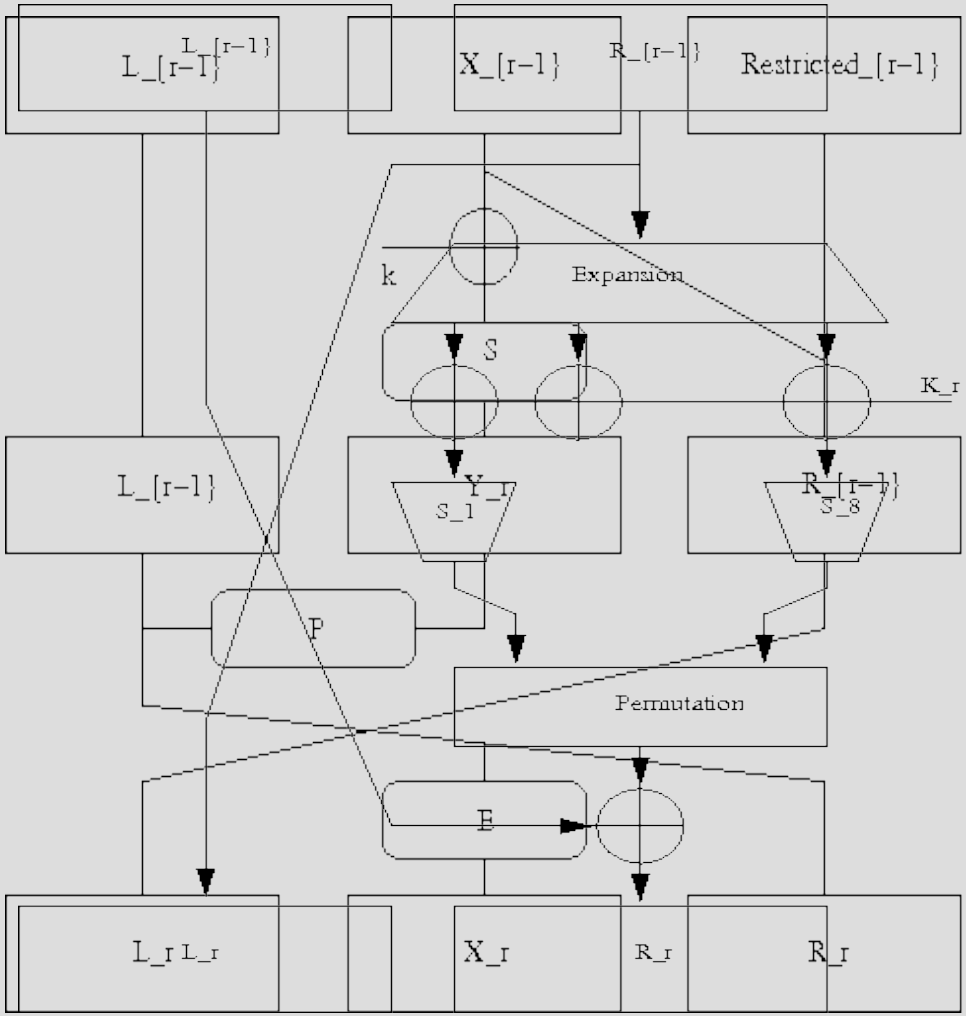


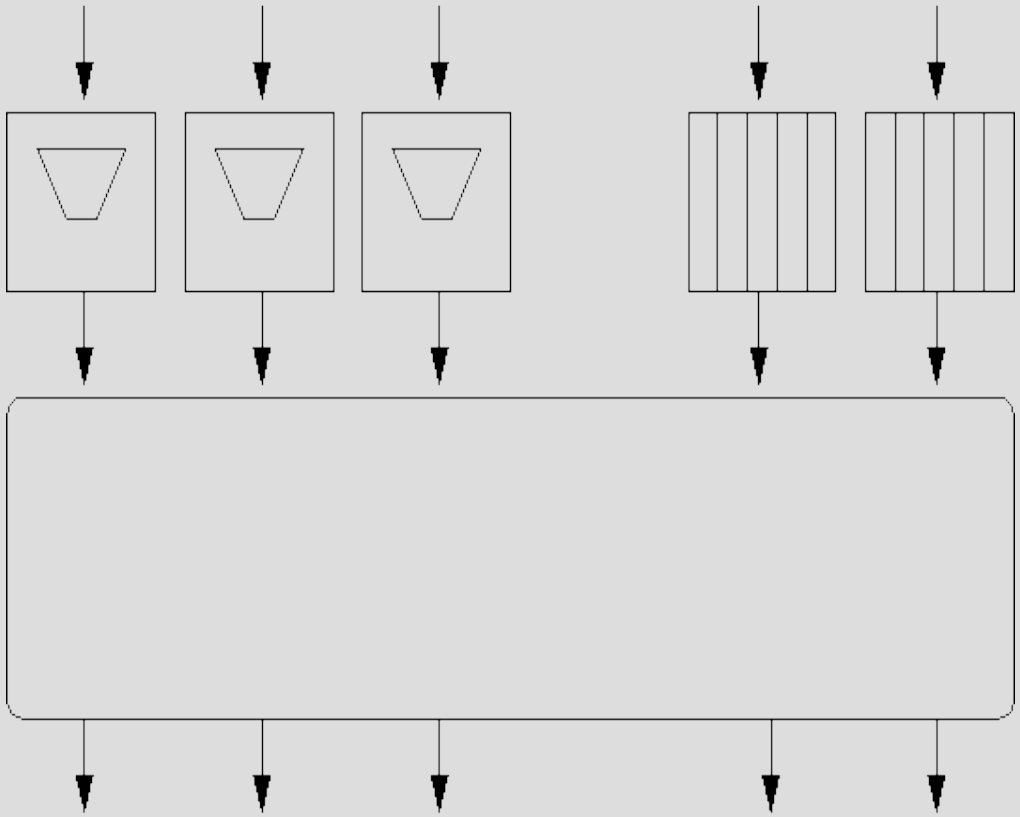
External encodings

- Protection against implementation extraction
- Protection against first and last round attacks

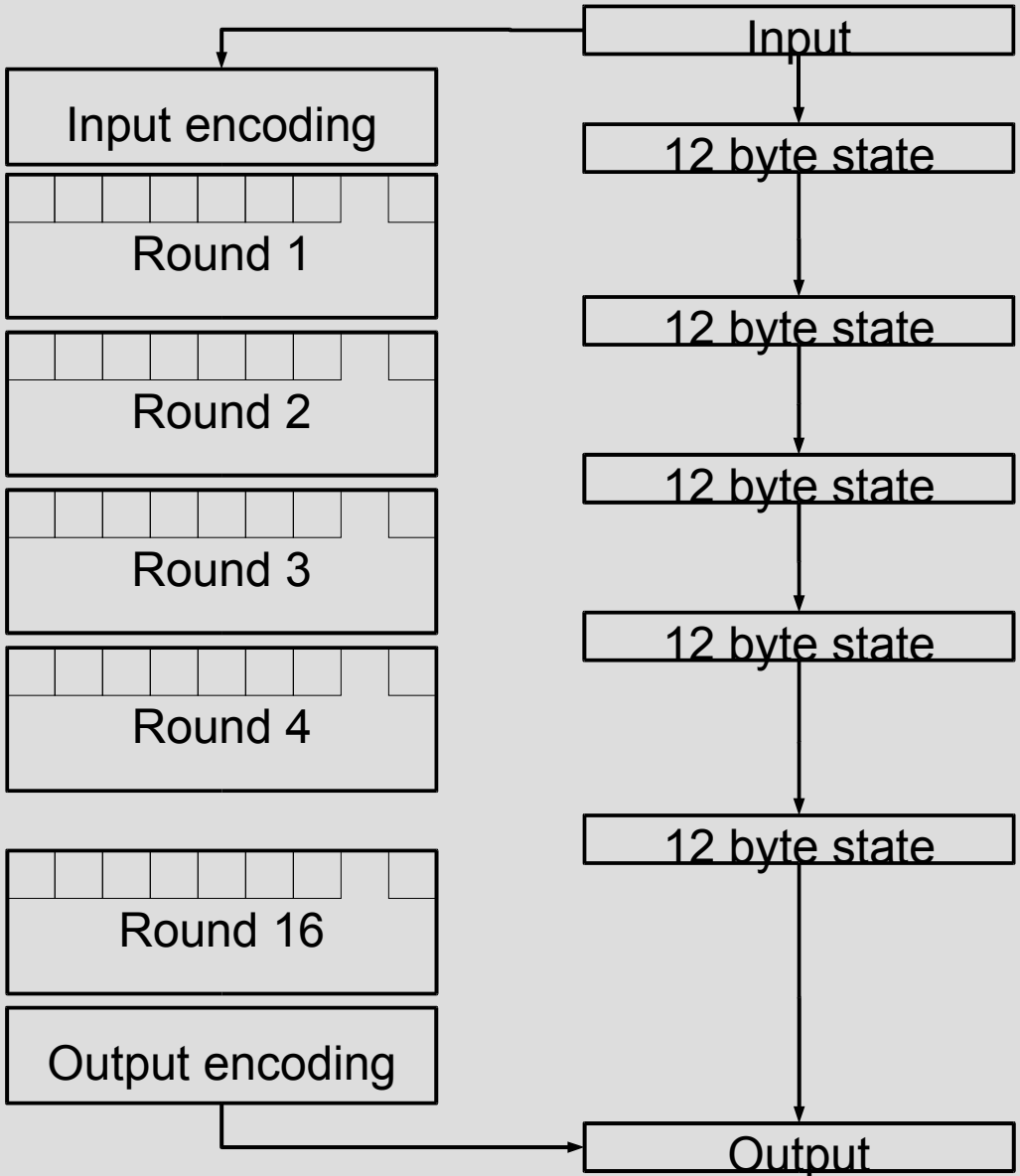
“Encoded variant”

White-box transformation





Cryptanalysis



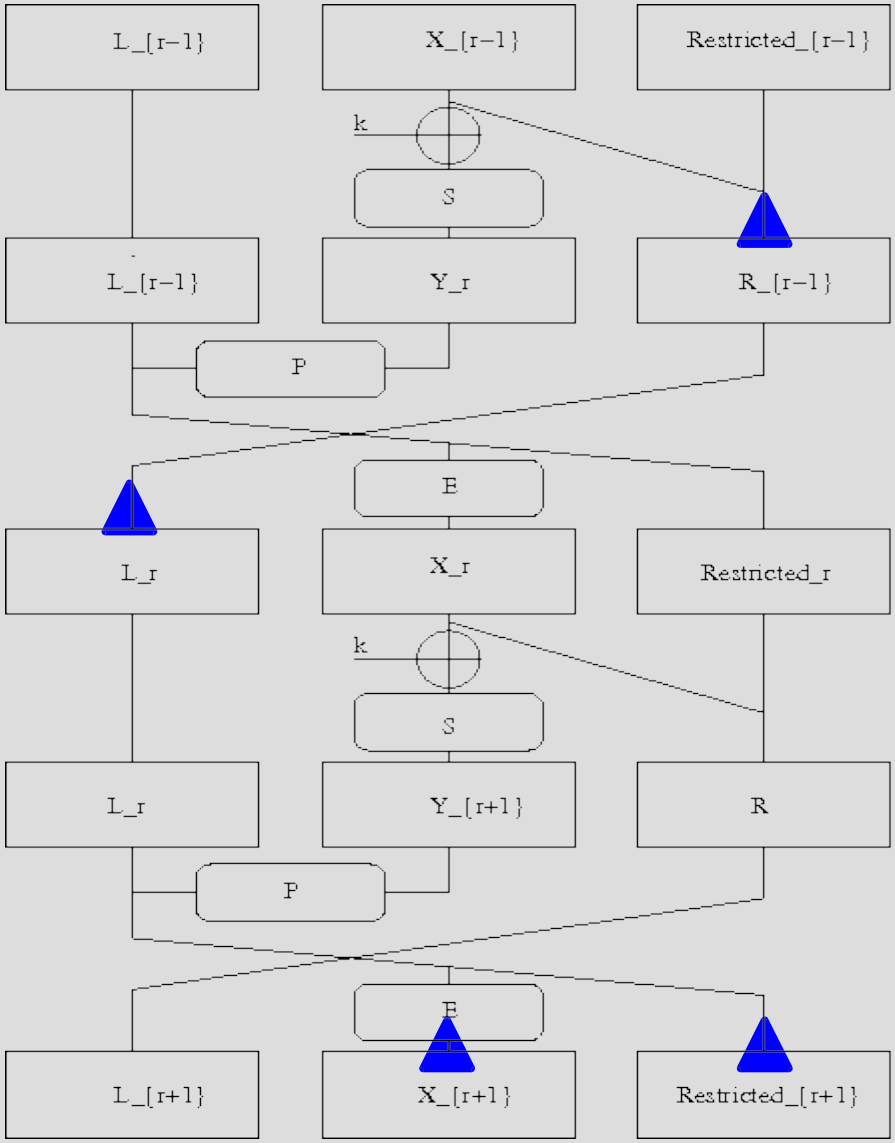
Difference propagation

Difference knowledge

S-box input recovery
S-box identification

Key recovery

Cryptanalysis

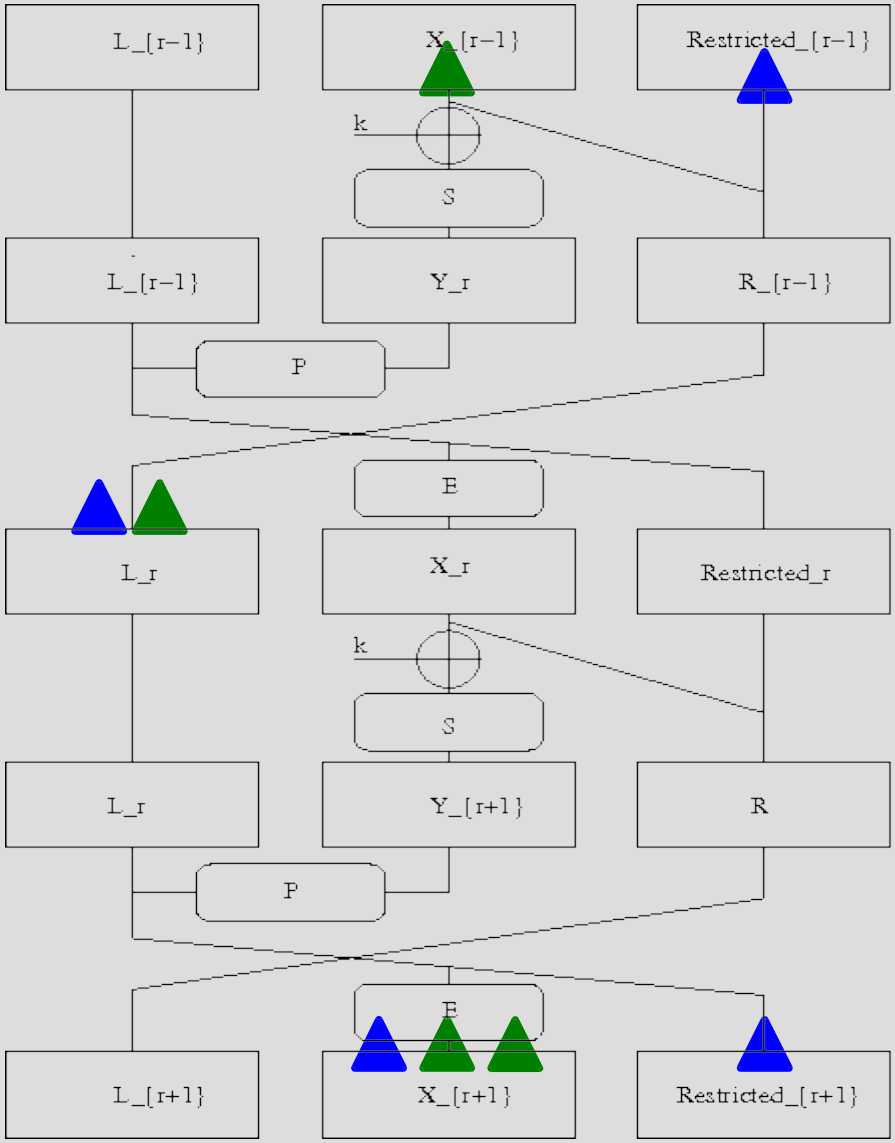


Detect single R-bit flips

- Change the input to a T-box in round 1
- Observe difference propagation at the input of round 3

Observe: 2 different T-boxes affected

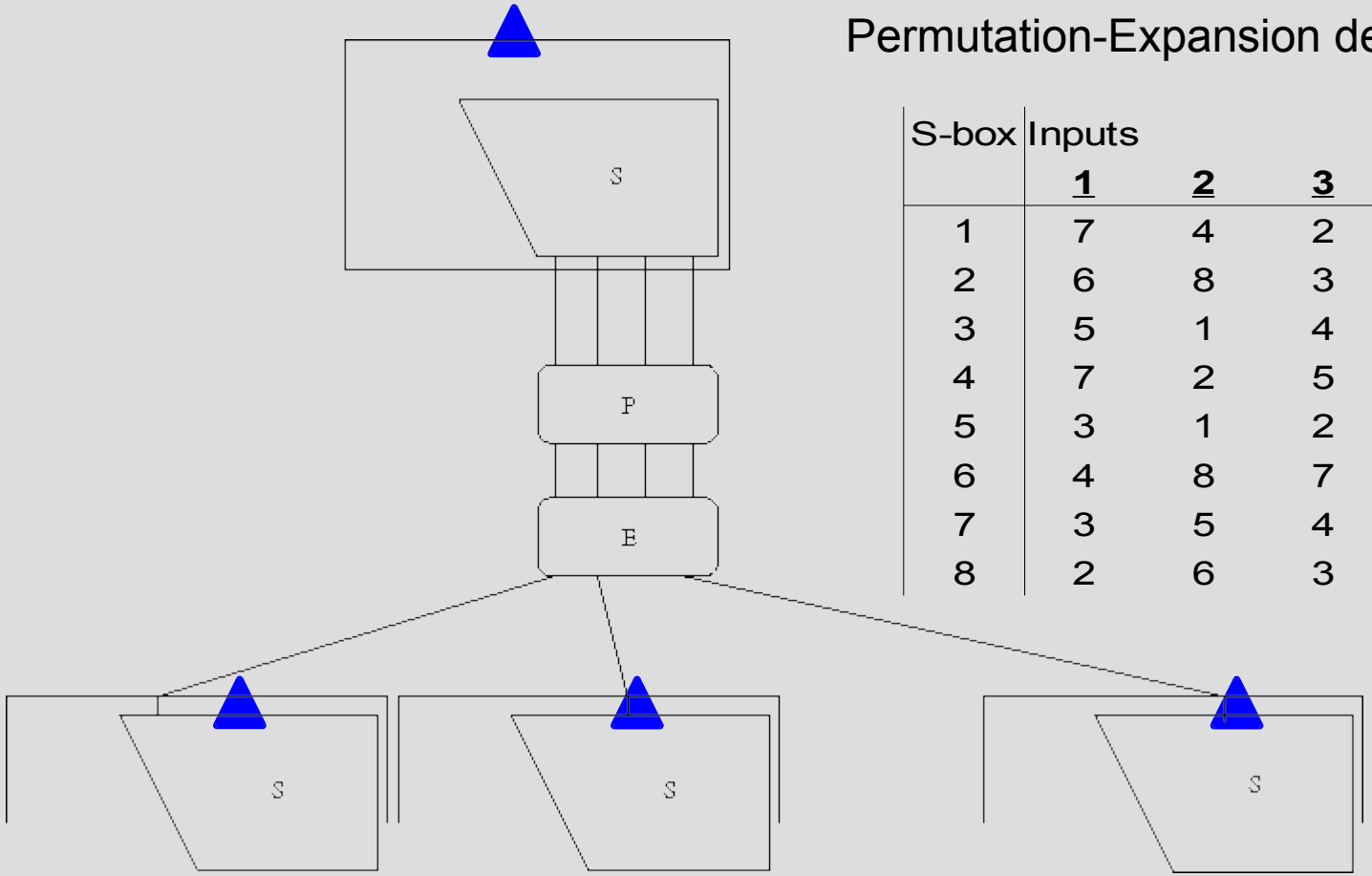
Cryptanalysis



Distinguish X-bit flips and Restricted bit flips

Cryptanalysis

Finding single bit flips



Permutation-Expansion design:

S-box	Inputs						Ex
	1	**2**	**3**	**4**	**5**	**6**	
1	7	4	2	5	6	8	3
2	6	8	3	7	5	1	4
3	5	1	4	6	7	2	8
4	7	2	5	8	3	1	6
5	3	1	2	6	4	8	7
6	4	8	7	1	3	5	2
7	3	5	4	8	2	6	1
8	2	6	3	1	7	4	5

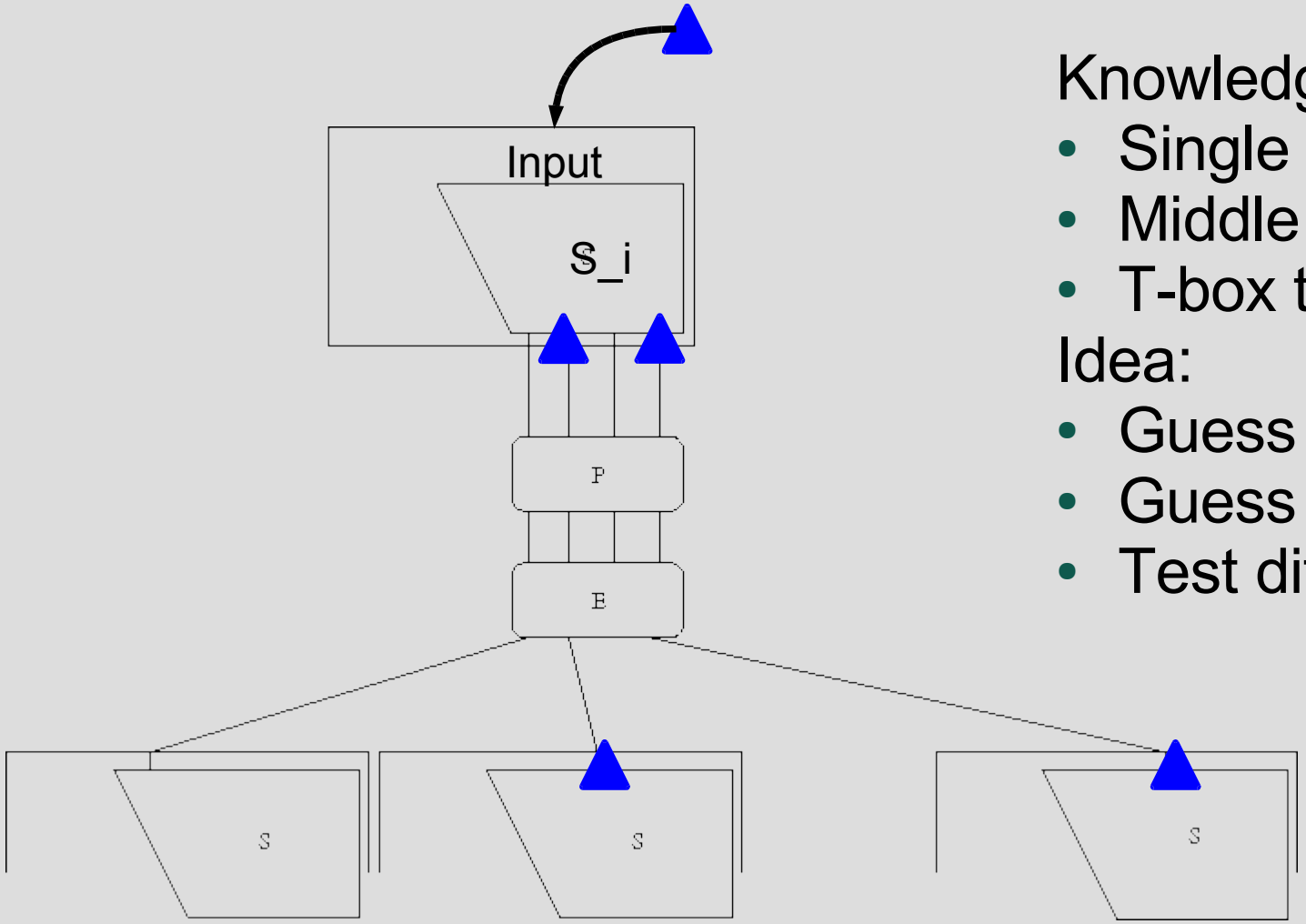
Cryptanalysis

- Overview

ROUND	INFORMATION	
1	Restricted bit flips	
2		Restricted bit flips
3	Middle bit flips, T-box type	
4	Single bit flips, T-box type	Middle bit flips, T-box type
5		Single bit flips, T-box type
...		

Cryptanalysis

Obtaining the inputs to the S-boxes



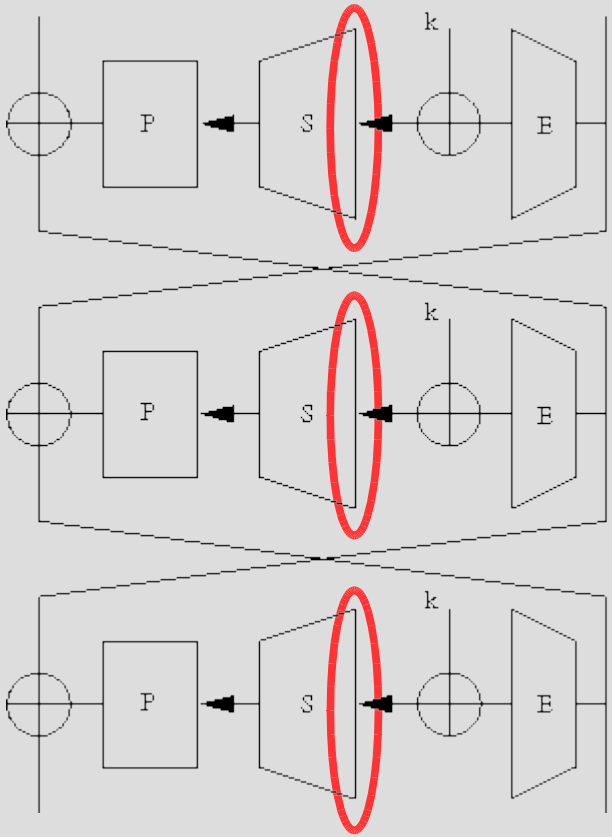
Knowledge:

- Single bit flips
- Middle bit flips
- T-box types

Idea:

- Guess S-box
- Guess Input
- Test differences

Cryptanalysis



Key recovery

- Via expansion function
- 3 round approach

Result: 2 complementary keys (DES complementation property)

Demo

- Demo

Conclusion

- Result
  - An efficient tool to extract the secret key from a white-box DES implementation
  - Time complexity: 2^{14} !
- Conclusion
  - Components and design choices that make DES “strong” in a black-box environment, make it weak in a black-box environment
  - Extending the idea to general 're-trust' white-box implementations (diffusion property etc.)

Uh oh!