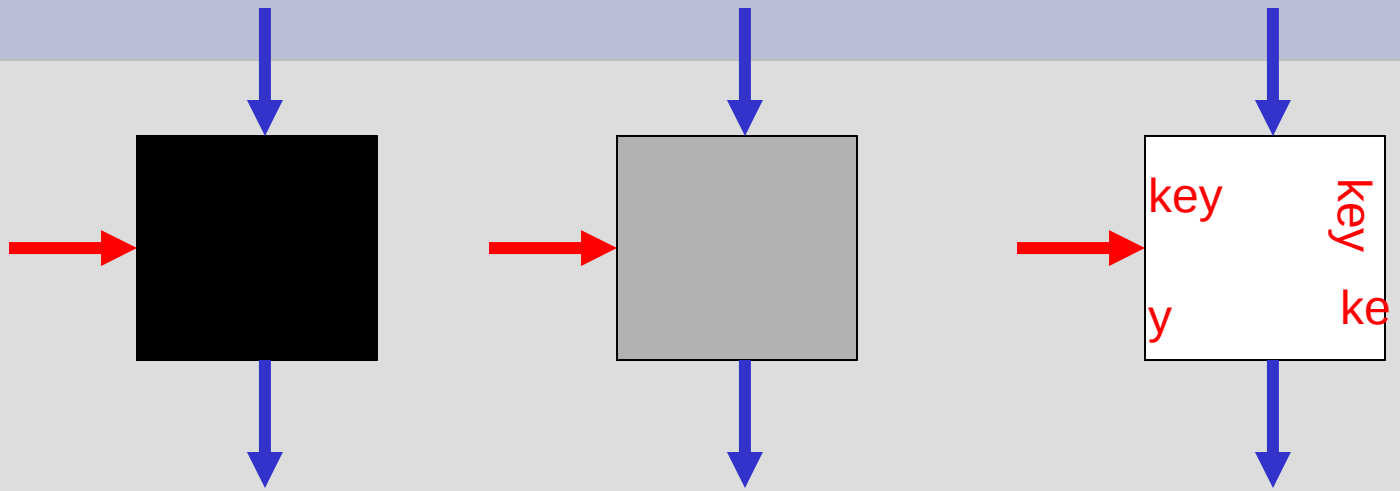
Cryptanalysis of White-Box DES Implementations with Arbitrary External Encodings

Brecht Wyseur, Wil Michiels, Paul Gorissen, Bart Preneel

COSIC – K.U.Leuven and Philips Research

March 27 2007

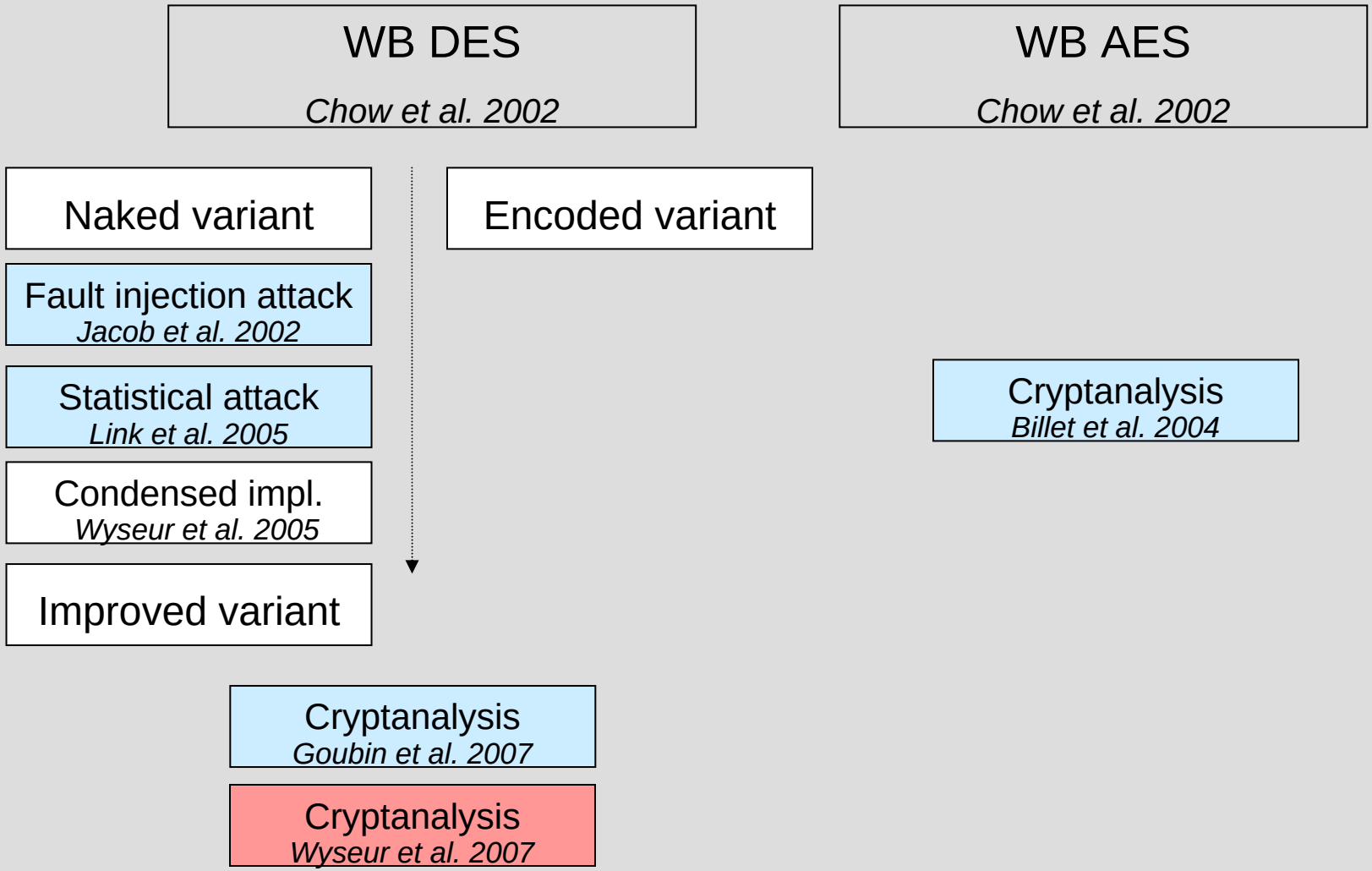
White-Box Attack Context



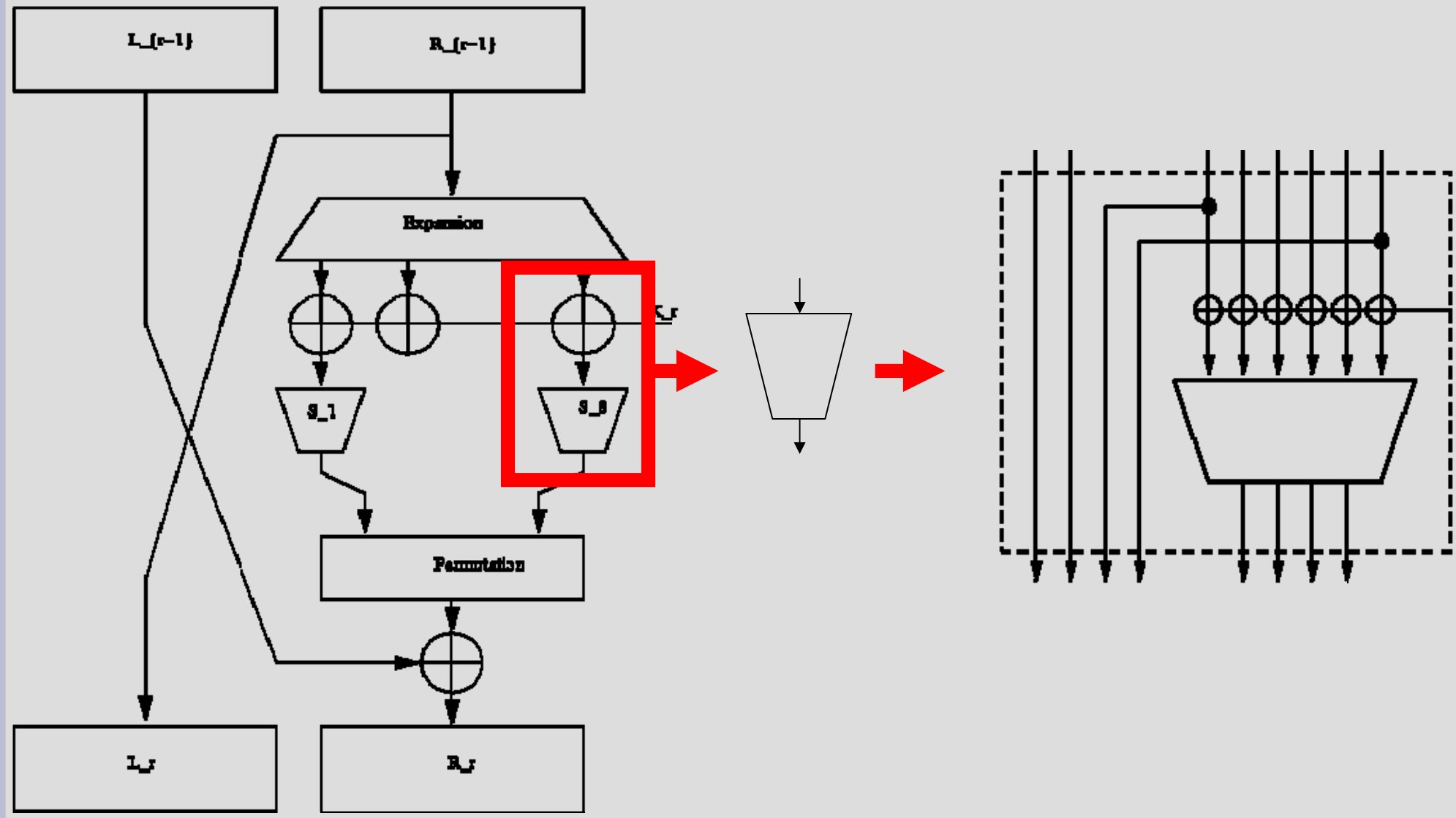
- Software running on host
- Dynamic execution can be observed
- Internal details both completely visible and alterable at will

Attacker's goal: extract the embedded secret key

State-of-the-art

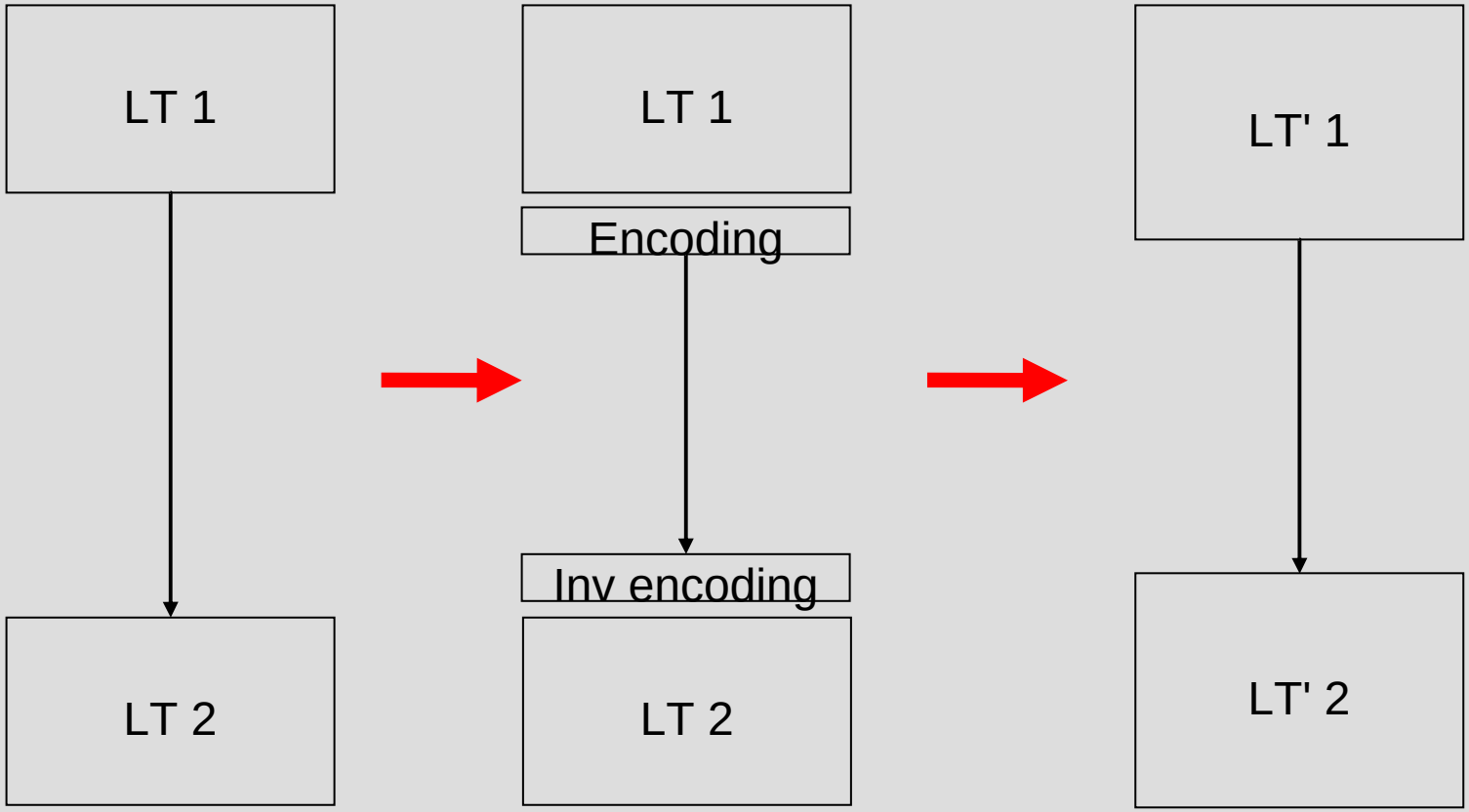


White-box transformation

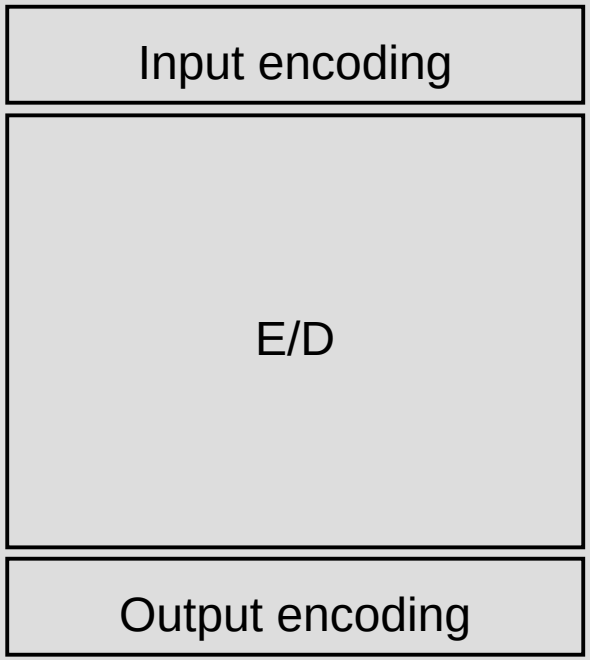


White-box transformations

- Internal encodings



White-box transformations

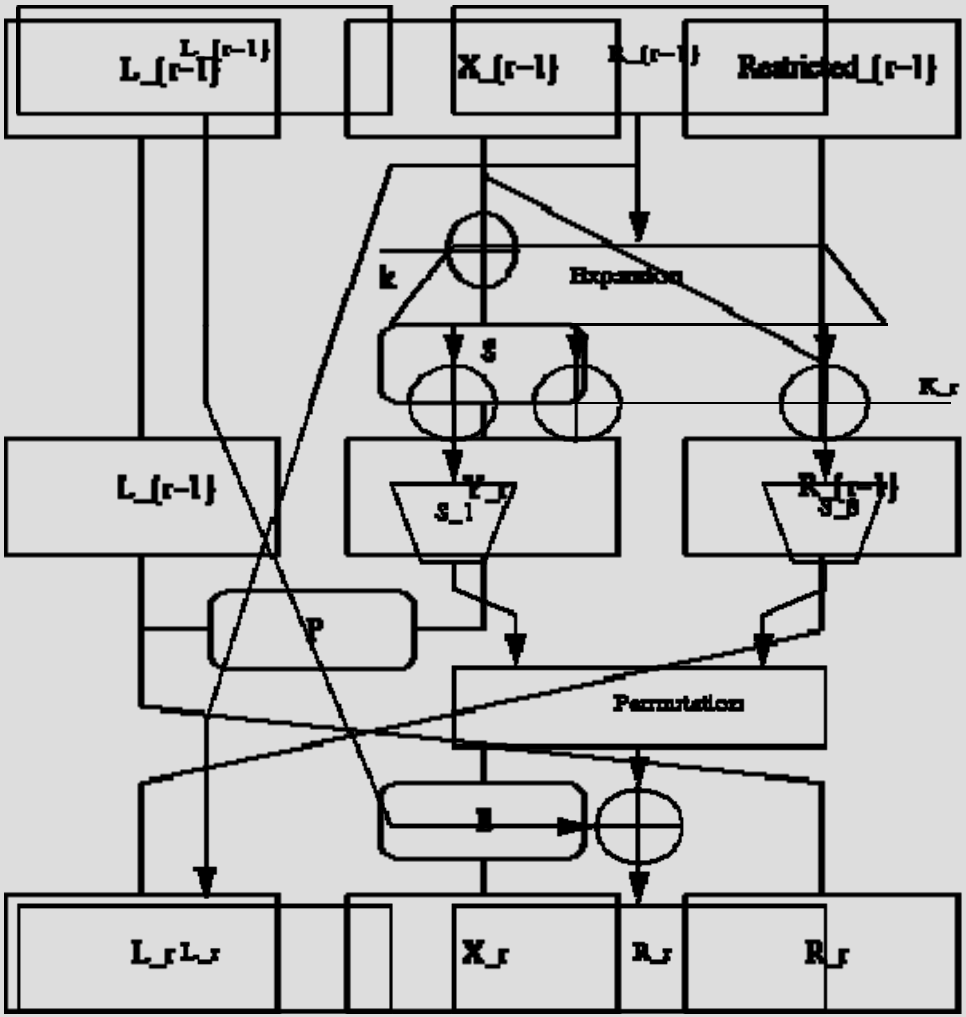


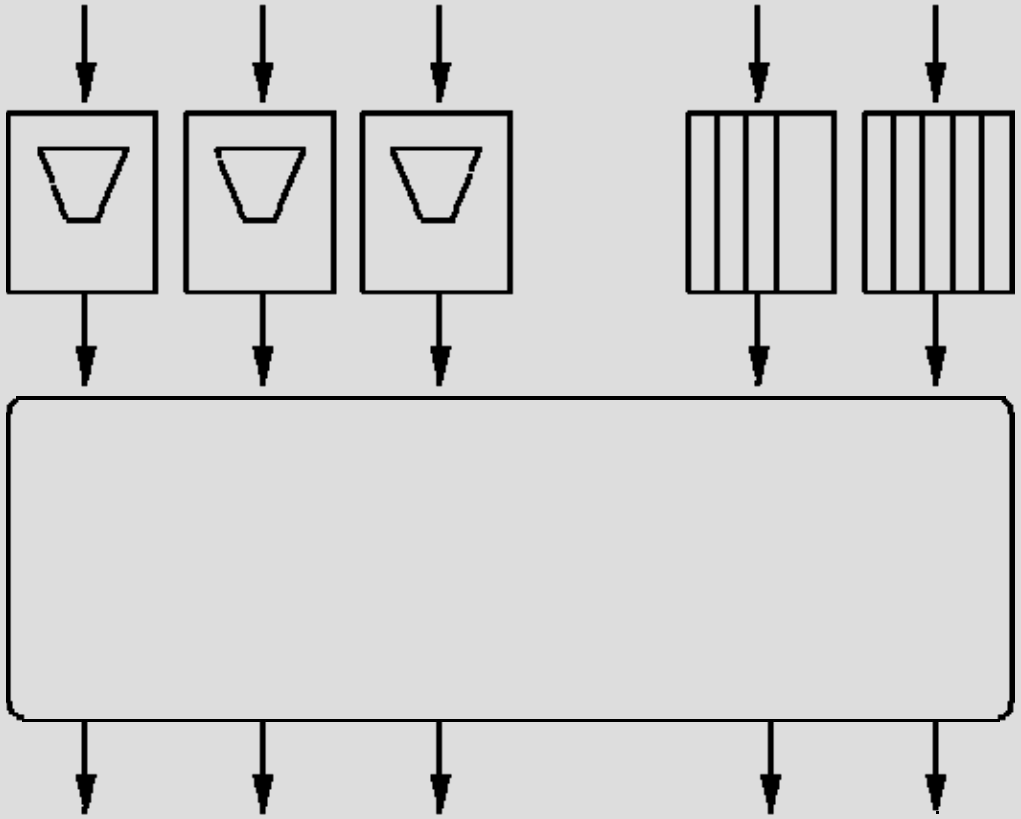
External encodings

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

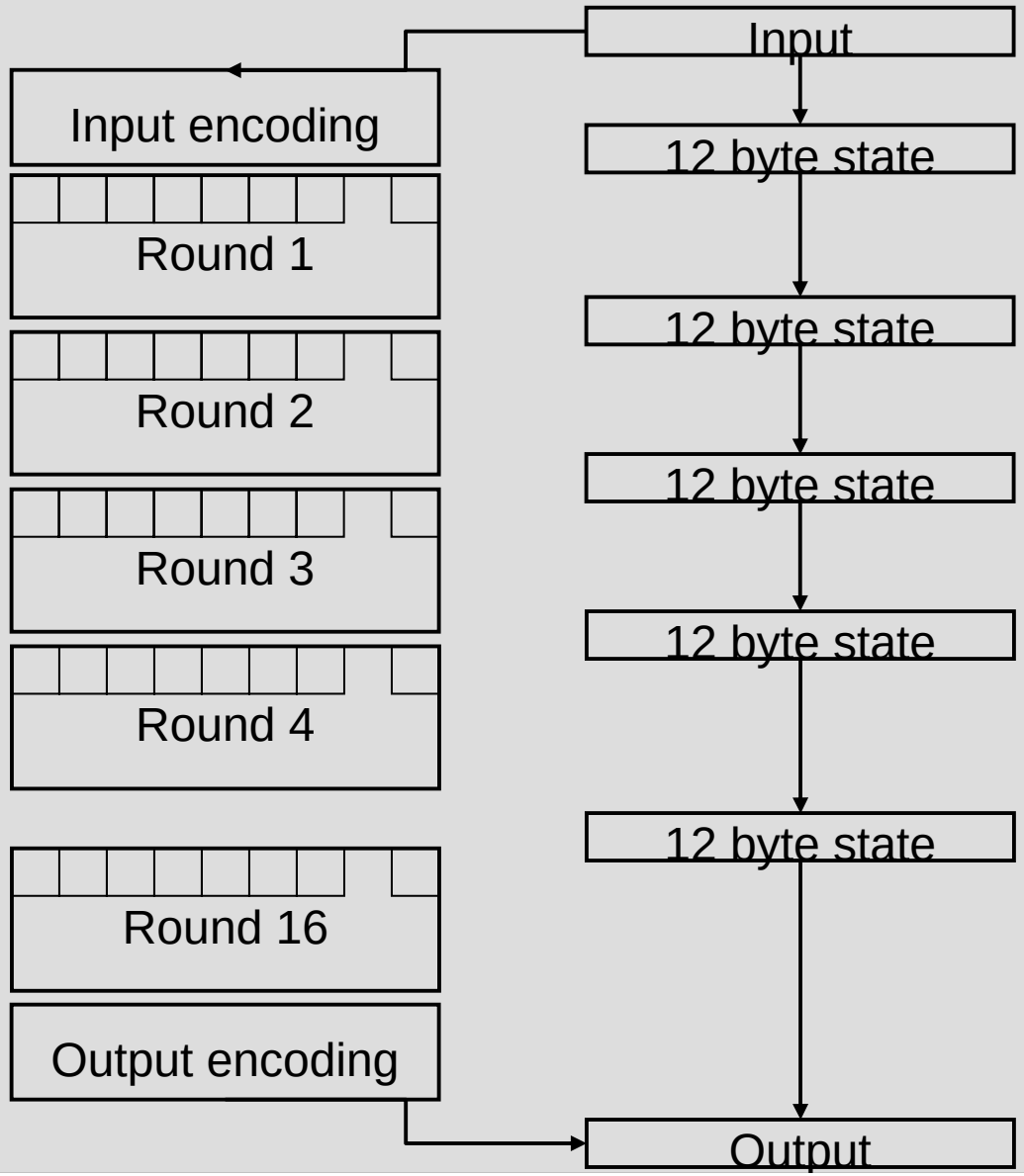
“Encoded variant”

White-box transformation





Differential Cryptanalysis



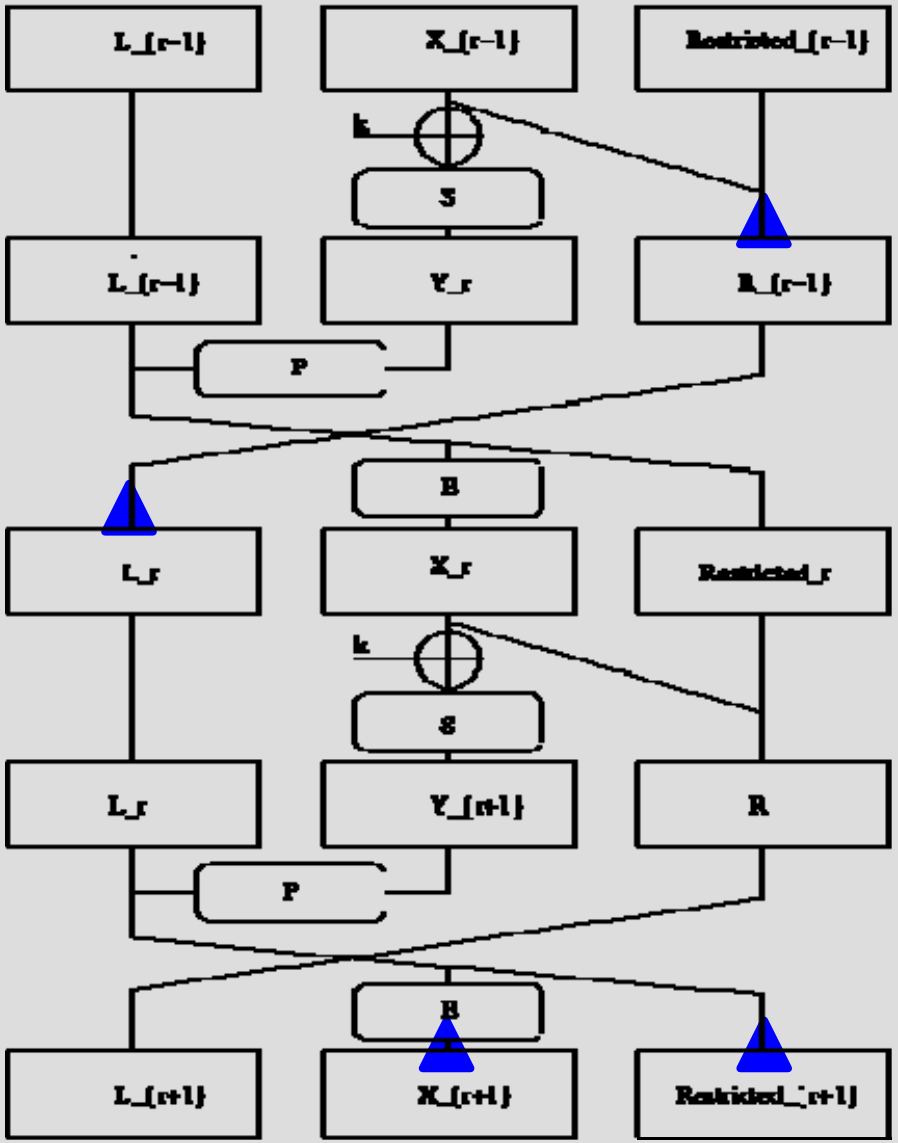
Difference propagation

Difference knowledge

S-box input recovery
S-box identification

Key recovery

Differential 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

Conclusion

- Attack with time complexity: 2^{14} independent of the external encodings
- Design choices that make DES “strong” in a black-box environment, make it weak in a black-box environment

- Paper at http://eprint.iacr.org