Conditional Linear Cryptanalysis

+ Breaking DES with $2^{41.9}$ known plaintexts

Stav Perle

Joint work with Eli Biham

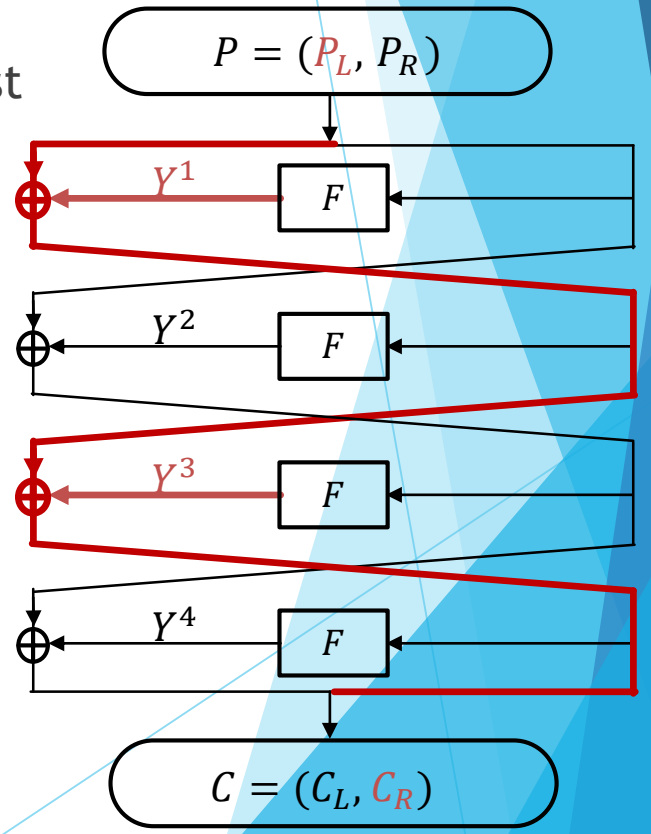
Technion – Israel Institute of Technology

Conditional Linear Cryptanalysis

- Using conditions to discard data
  - So the bias of the remaining data increase or decrease
- Conditions can be by any observable data available to the cryptanalyst
  - Plaintexts, ciphertexts, and formulae on them
- There are many kinds of conditions
- The most useful is applicable to Feistel ciphers

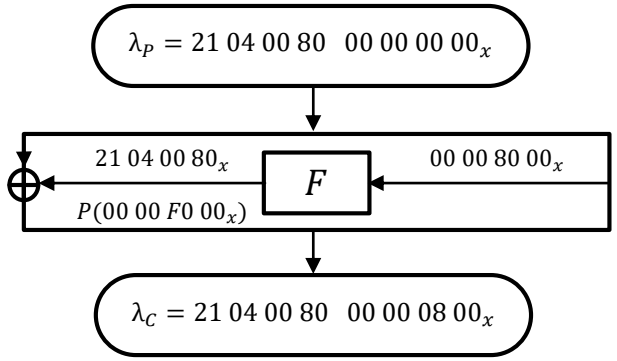
Conditional Linear Cryptanalysis

- Using conditions to discard data
  - So the bias of the remaining data increase or decrease
- Conditions can be by any observable data available to the cryptanalyst
  - Plaintexts, ciphertexts, and formulae on them
- There are many kinds of conditions
- The most useful is applicable to Feistel ciphers
- We condition on the XOR of plaintext and ciphertext bits
  - = XOR of outputs of F is odd (or even) rounds
- For example, on $P_L \oplus C_R = \oplus_{\mathrm{r}\ is\ odd} Y^{\mathrm{r}}$
  - which is the XOR of the output of F in all odd rounds



A Case of a Single Round

- The best non-trivial approximation of S5:

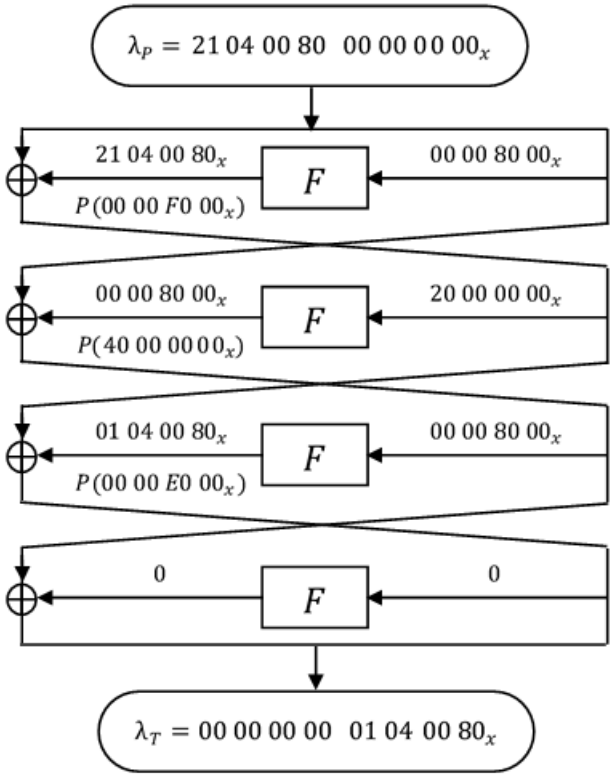


- It approximates the second bit of input to the XOR of the four output bits
  - Probability ½-20/64 = bias 0.312
- With a condition it increases to 0.468

All	0.312
LSB=0	0.156
LSB=1	0.468

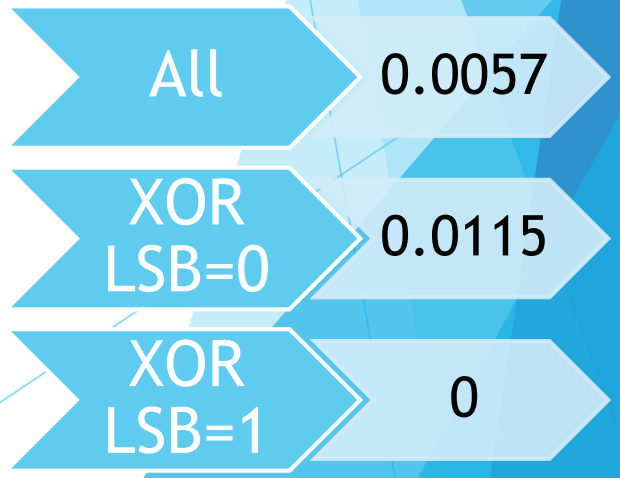
A Four-Round Example

- Consider four successive rounds taken from Matsui's best linear approximation
- This approximation uses three active S boxes:
  - S5 on the first and third rounds, and
  - S1 on the second round
- Both odd rounds have the same active S box.



A Four-Round Example

- Notice that this condition is based on the XOR of both odd rounds
  - Not just on one of them
- Under this condition the average bias is 0.0115
  - While the bias over all cases is 0.0057
- ➔ Using only these plaintexts increases the bias by a factor of two.
- ➔ We need a quarter of the data for analysis
  - Compared to a regular linear attack with the same approximation
  - But this is after we discard half of the given data that fails the condition
- ➔ We need half of the original known plaintexts
  - We discard half of it, and get the required quarter



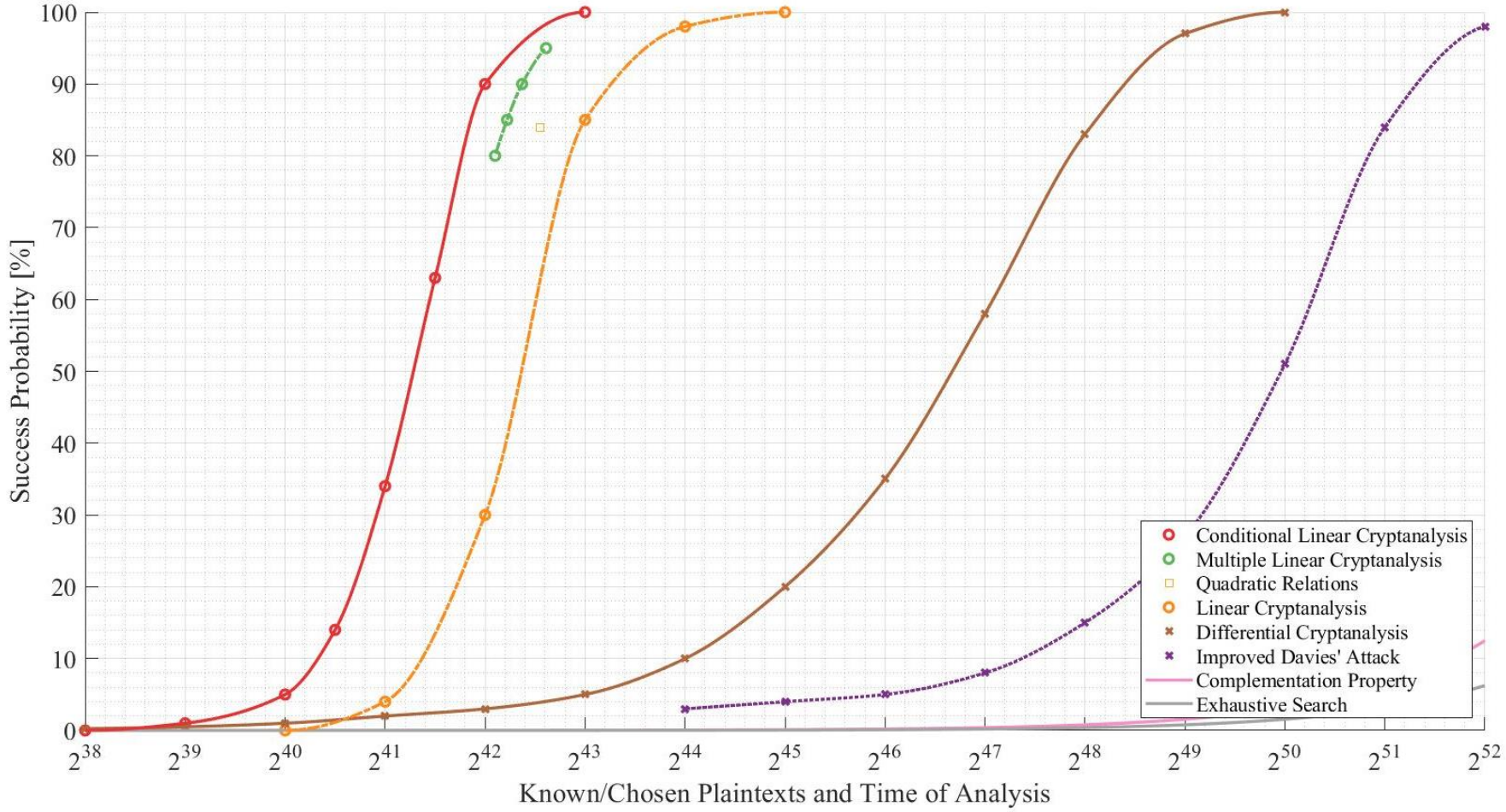
Conditional Linear Cryptanalysis of the Full 16-Round DES

- Matsui uses the best 14-round linear approximation
  - The attack requires about 2^{43} known plaintexts

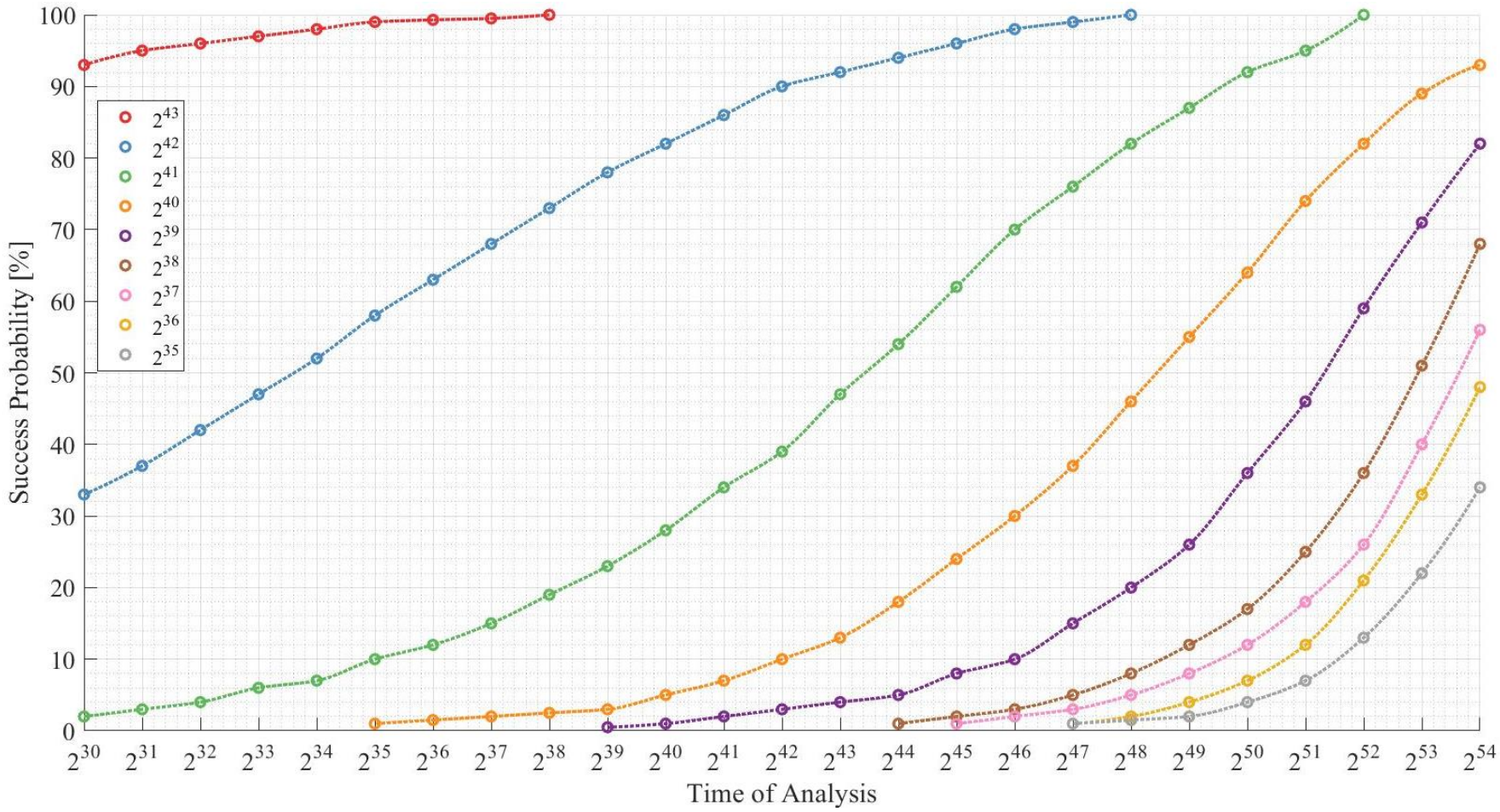
- Using conditions with improved bias and aux techniques, we can use a 13-round approximation
  - Using an FFT, we can perform the analysis very efficiently
    - (counting and key ordering takes only about a minute)
- The attack requires about $2^{41.9}$ known plaintexts

Attack	13-round bias	Complexity
LC	$2^{-20.06}$	2^{43}
CLC	$2^{-19.06}$	$2^{41.9}$

Results



- Our results are based on thousands of runs


Success Probability [%]
Time of Analysis
100
90
80
70
60
50
40
30
20
10
0
2^{30} 2^{31} 2^{32} 2^{33} 2^{34} 2^{35} 2^{36} 2^{37} 2^{38} 2^{39} 2^{40} 2^{41} 2^{42} 2^{43} 2^{44} 2^{45} 2^{46} 2^{47} 2^{48} 2^{49} 2^{50} 2^{51} 2^{52} 2^{53} 2^{54}
2^{43}
2^{42}
2^{41}
2^{40}
2^{39}
2^{38}
2^{37}
2^{36}
2^{35}

Thank You