GEMPLUS
beyond smart

Royal Holloway
University of London

Explaining Differential Fault Analysis on DES

Christophe Clavier

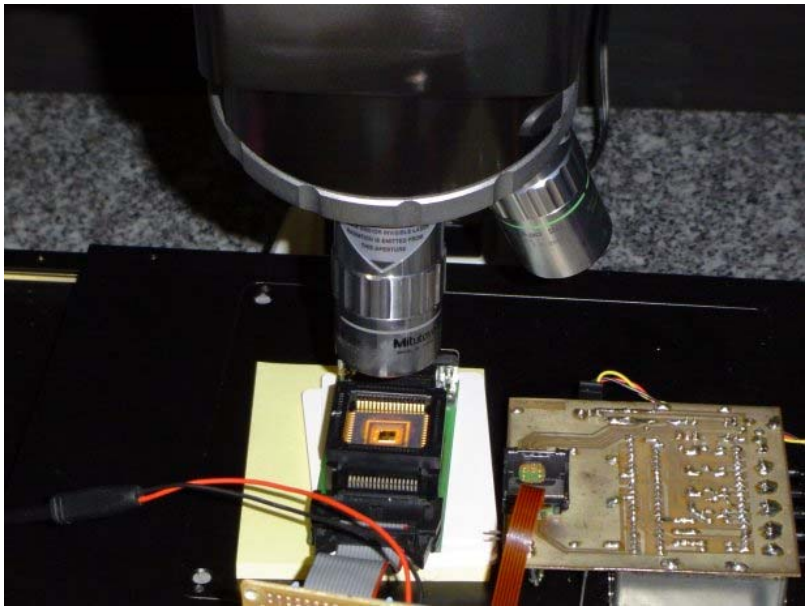
Michael Tunstall

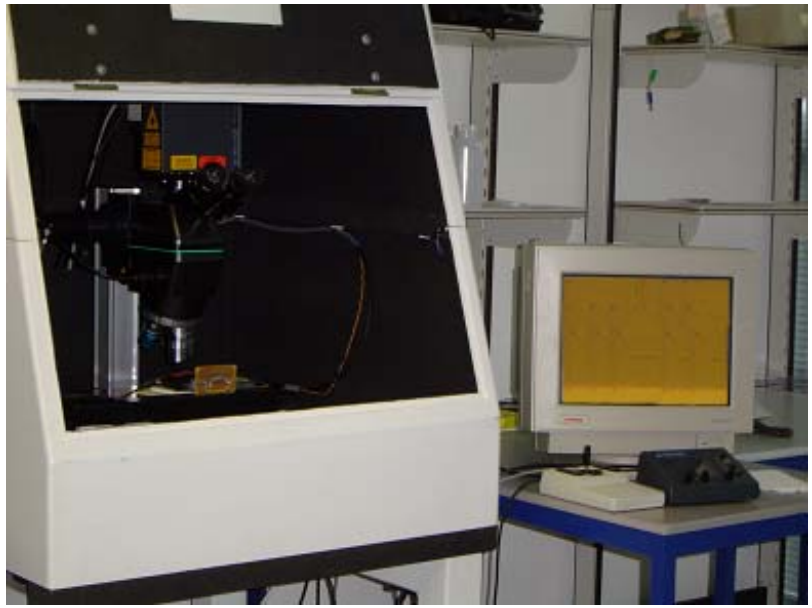
References

E. Biham and A. Shamir. Differential fault analysis of secret key cryptosystems. Technical Report, Technion - Computer Science Department, 1997.

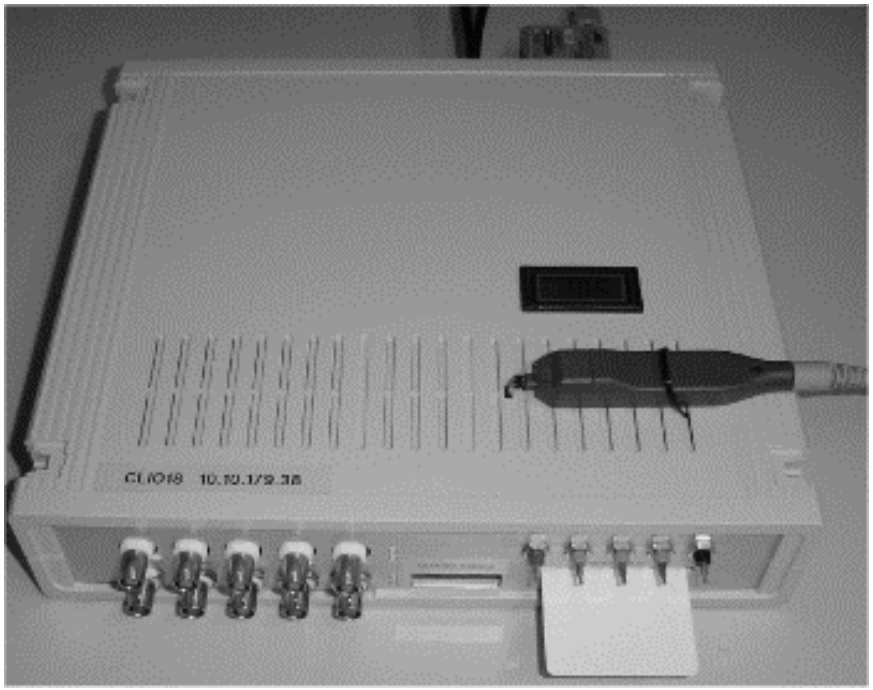
C. Giraud and H. Thiebeauld. A survey on fault attacks. In Y. Deswarte and A. A. El Kalam, editors, *Smart Card Research and Advanced Applications VI – 18th IFIP World Computer Congress*, pages 159–176. Kluwer Academic, 2004.

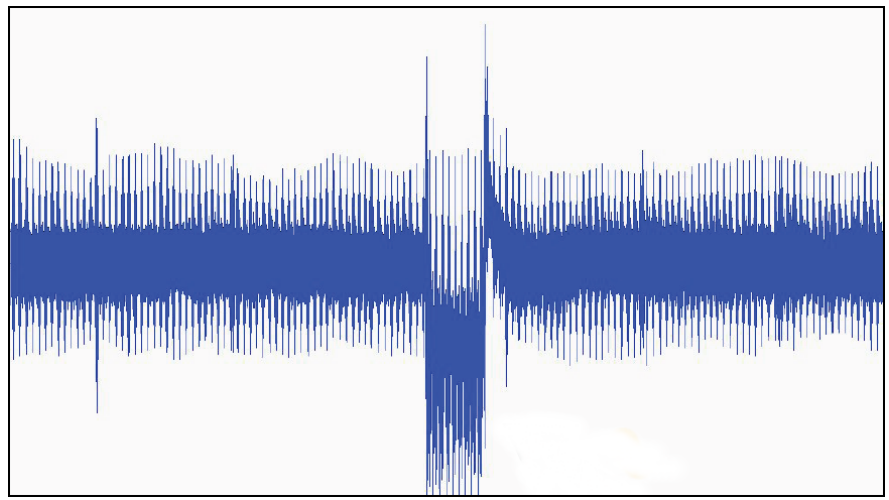
Fault Injection Equipment: Laser



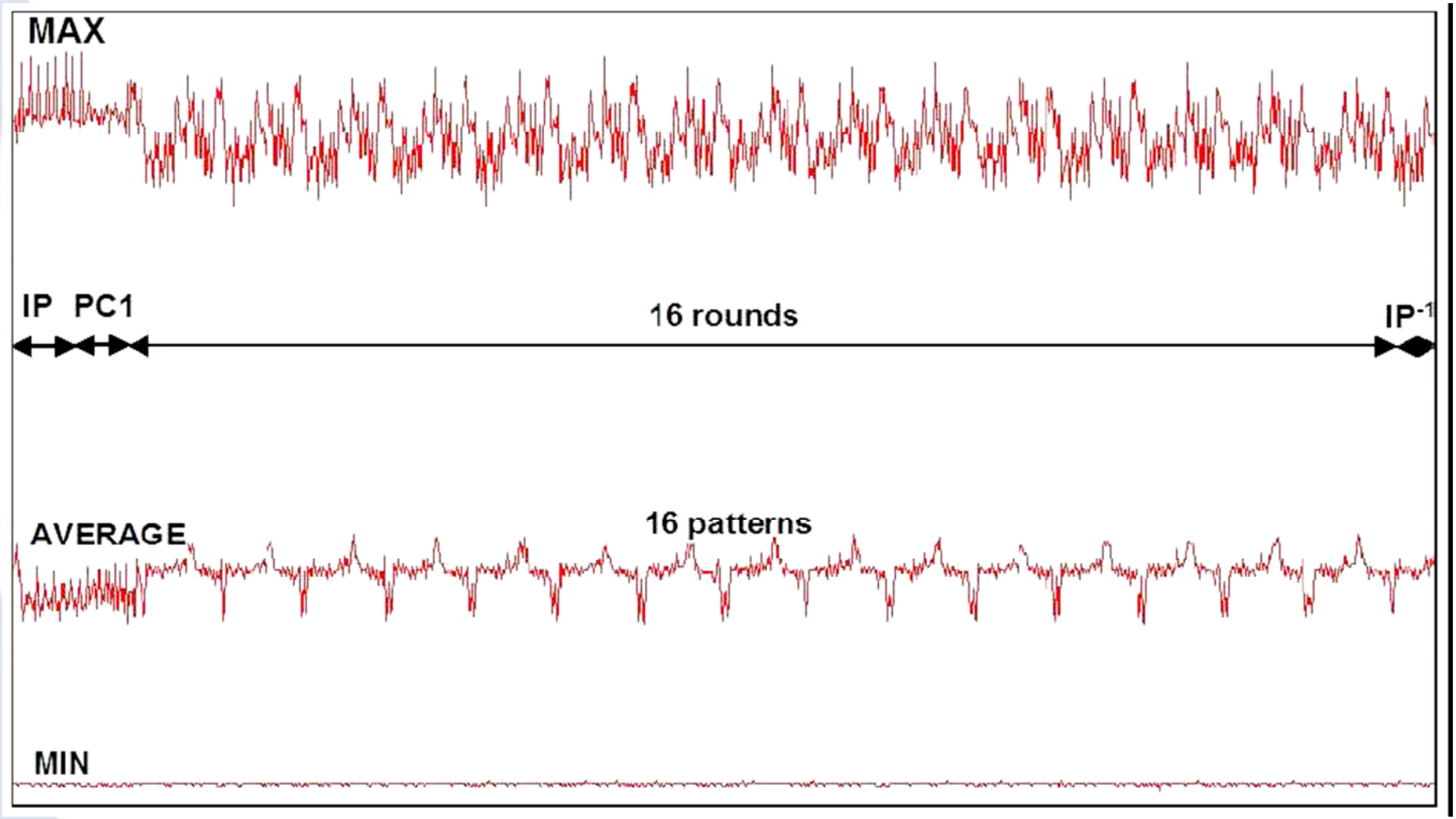


Fault Injection Equipment: CLIO Glitch Injector

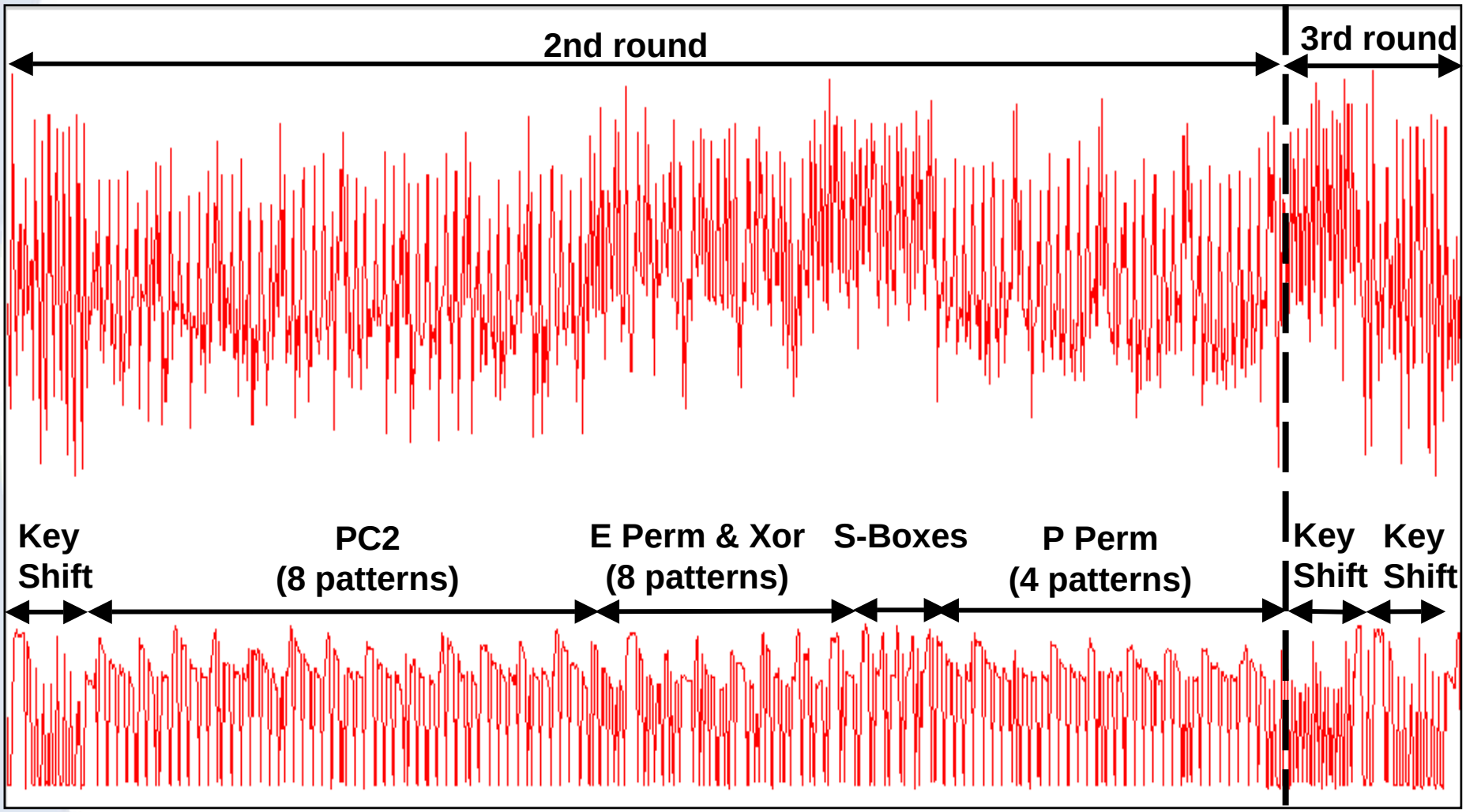




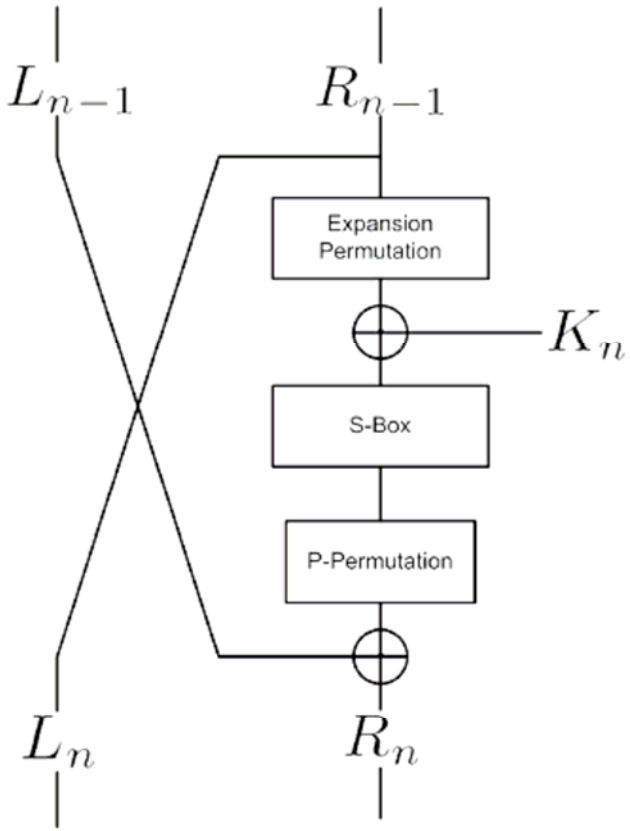
Where to inject a fault?



Looking Closer



Notation



- 16 Rounds, each a transform 2 32-bit variables.
- [L0,R0] – plaintext
- [L16,R16] – ciphertext
- Bitwise permutations are not always considered.

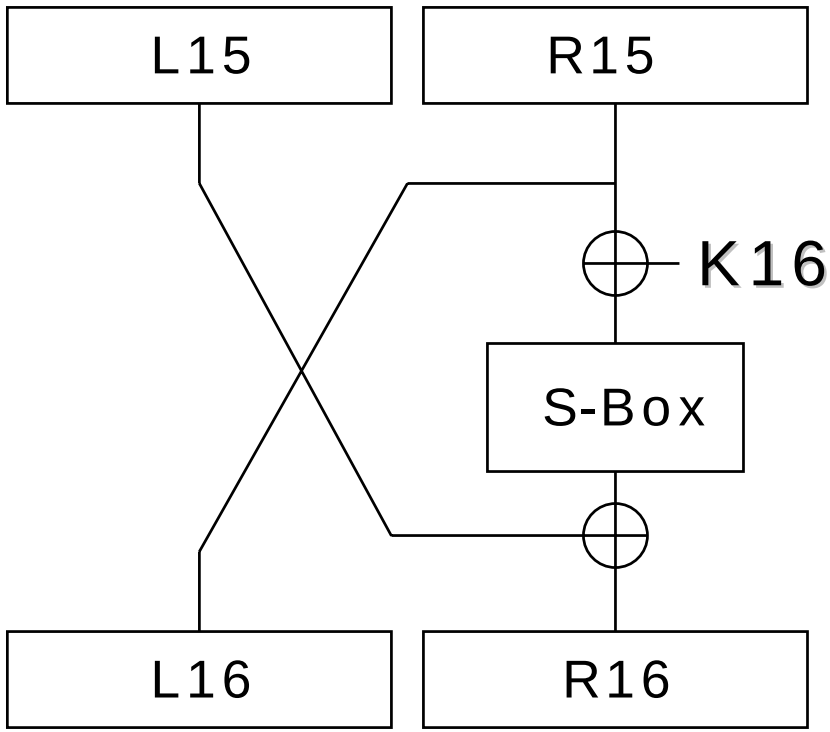
$$R_n = S(R_{n-1} \oplus K_n) \oplus L_{n-1}$$
$$L_n = R_{n-1}$$

GEMPLUS
beyond smart

Royal Holloway
University of London

DES-Fifteenth Round

DES last round structure



- Transformation of [L15,R15] to [L16,R16] using K16

$$L16 = R15$$

$$R16 = S(R15 \oplus K16) \oplus L15$$

Fault Injection in 15th round

- If R15 is changed to R15′, without changing L15

$$L16 = R15$$

$$R16 = S(R15 \oplus K16) \oplus L15$$

then

$$L16' = R15'$$

$$R16' = S(R15' \oplus K16) \oplus L15$$

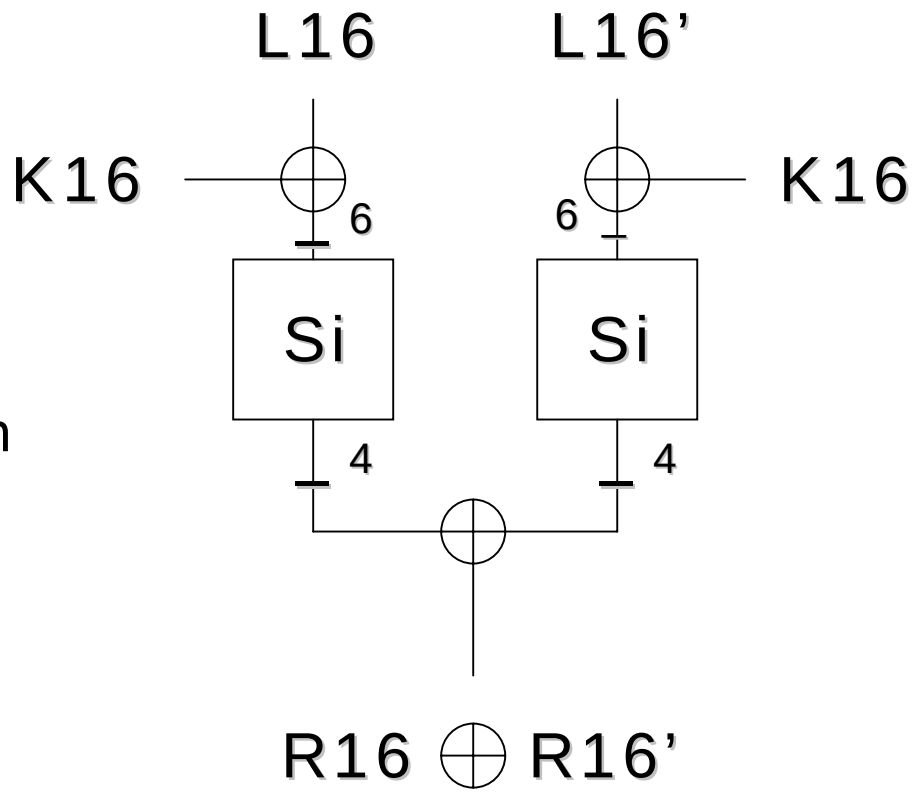
where S(x) is the S-box function

$$R16 \oplus R16' = S(R15 \oplus K16) \oplus L15 \oplus S(R15' \oplus K16) \oplus L15$$

$$= S(R15 \oplus K16) \oplus S(R15' \oplus K16)$$

Differential Fault Analysis

- For each S-box (Si), i Є[1..8] verify the following relation:
- Gives a list of possible key values 2^{32}
- Leads to an exhaustive search



Predicting the Key Space

- Why 2^{32}?
- The number of hypothesis' given for each six bits of the key can be found using the tables, described in, "Differential Cryptanalysis of DES-like Cryptosystems" by Biham and Shamir

$R16 \oplus R16'$ →

$S-in$
$\oplus$
$S-in'$ ↓

```
{ 64,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0 },
{  0,  0,  0,  6,  0,  2,  4,  4,  0, 10, 12,  4, 10,  6,  2,  4 },
{  0,  0,  0,  8,  0,  4,  4,  4,  0,  6,  8,  6, 12,  6,  4,  2 },
{ 14,  4,  2,  2, 10,  6,  4,  2,  6,  4,  4,  0,  2,  2,  2,  0 },
{  0,  0,  0,  6,  0, 10, 10,  6,  0,  4,  6,  4,  2,  8,  6,  2 },
{  4,  8,  6,  2,  2,  4,  4,  2,  0,  4,  4,  0, 12,  2,  4,  6 },
{  0,  4,  2,  4,  8,  2,  6,  2,  8,  4,  4,  2,  4,  2,  0, 12 },
{  2,  4, 10,  4,  0,  4,  8,  4,  2,  4,  8,  2,  2,  2,  4,  4 },
{  0,  0,  0, 12,  0,  8,  8,  4,  0,  6,  2,  8,  8,  2,  2,  4 },
{ 10,  2,  4,  0,  2,  4,  6,  0,  2,  2,  8,  0, 10,  0,  2, 12 },
{  0,  8,  6,  2,  2,  8,  6,  0,  6,  4,  6,  0,  4,  0,  2, 10 },
{  2,  4,  0, 10,  2,  2,  4,  0,  2,  6,  2,  6,  6,  4,  2, 12 },
{  0,  0,  0,  8,  0,  6,  6,  0,  0,  6,  6,  4,  6,  6, 14,  2 },
{  6,  6,  4,  8,  4,  8,  2,  6,  0,  6,  4,  6,  0,  2,  0,  2 },
{  0,  4,  8,  8,  6,  6,  4,  0,  6,  6,  4,  0,  0,  4,  0,  8 },
{  2,  0,  2,  4,  4,  6,  4,  2,  4,  8,  2,  2,  2,  6,  8,  8 },
...
```

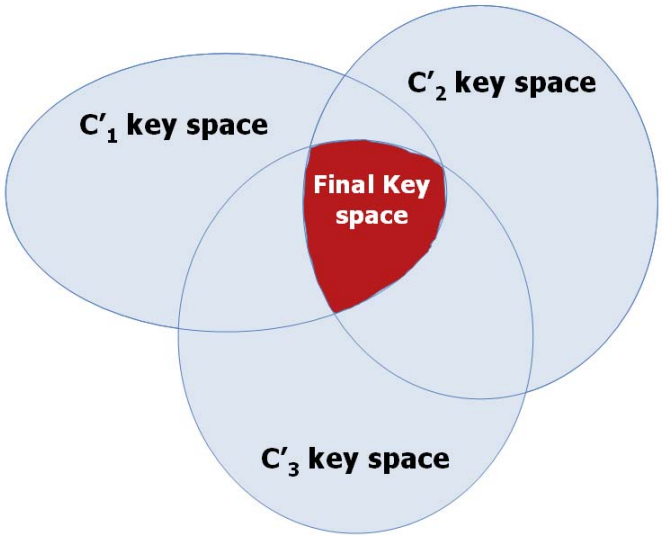
Predicting the Key Space

- For each s-box the expected number of hypotheses can be calculated:

S-box	$\mathbb{E}(x_{ij})$
1	7.54
2	7.67
3	7.58
4	8.36
5	7.73
6	7.41
7	7.91
8	7.66

- The predicted key space is the product of all the averages = 2^{24}.
- Eight bits are not included in this key and need to be added = 2^{32}.

Intersecting Keyspaces



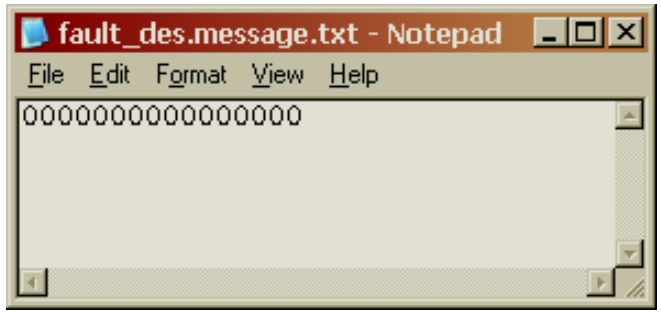
- With numerous faulty ciphertexts the key will be in the intersection of all the key spaces.

- e.g. two faulty ciphertext leading to 2^{14}

S-box	$\mathbb{E}(x_{ij} \cap x_{mn})$
1	1.68
2	1.70
3	1.69
4	1.86
5	1.72
6	1.65
7	1.76
8	1.70

A Real Example

- Plaintext file



- Ciphertext file

A Real Example

Faulty Ciphertext	Differential on s-box entry	Hypotheses Derived	Total Subkey Hypotheses
$EB327EBD0534712B_{16}$	00_{16}	64	
	06_{16}	10	
	20_{16}	2	
	00_{16}	64	
	00_{16}	64	
	00_{16}	64	
	00_{16}	64	
	00_{16}	64	2^{40}
$DA8AE85B4C55F358_{16}$	09_{16}	2	
	$1B_{16}$	2	
	35_{16}	10	
	16_{16}	8	
	22_{16}	2	
	25_{16}	4	
	19_{16}	6	
	18_{16}	6	2^{17}

A Real Example

- Searches of 2^{48} and 2^{25} for the different faulty ciphertexts.
- The intersection can be taken giving a search of around 2^{20} for the entire DES key.

GEMPLUS
beyond smart

Royal Holloway
University of London

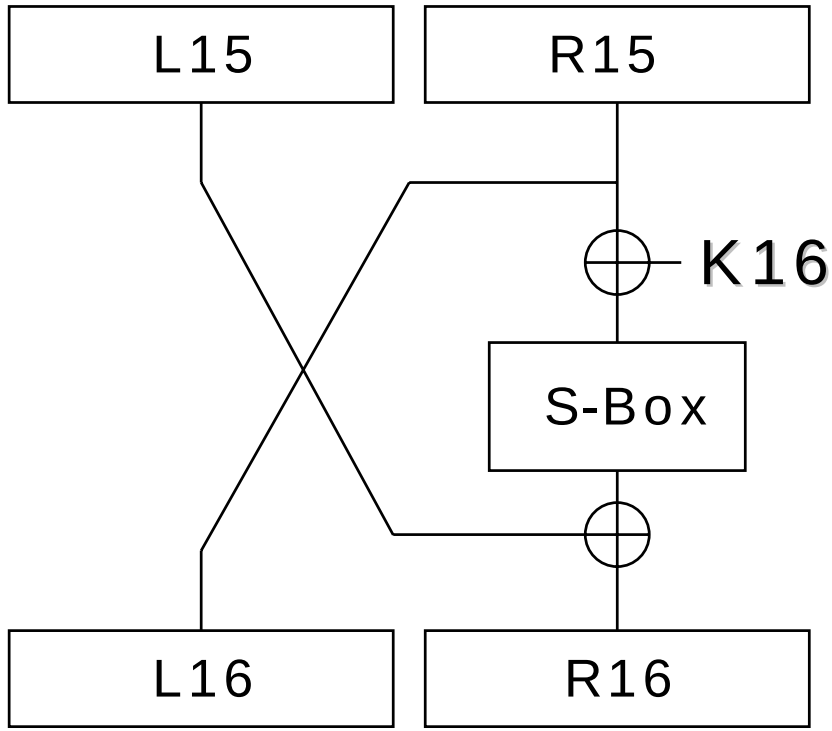
DES – Other Rounds

Differential Fault Analysis

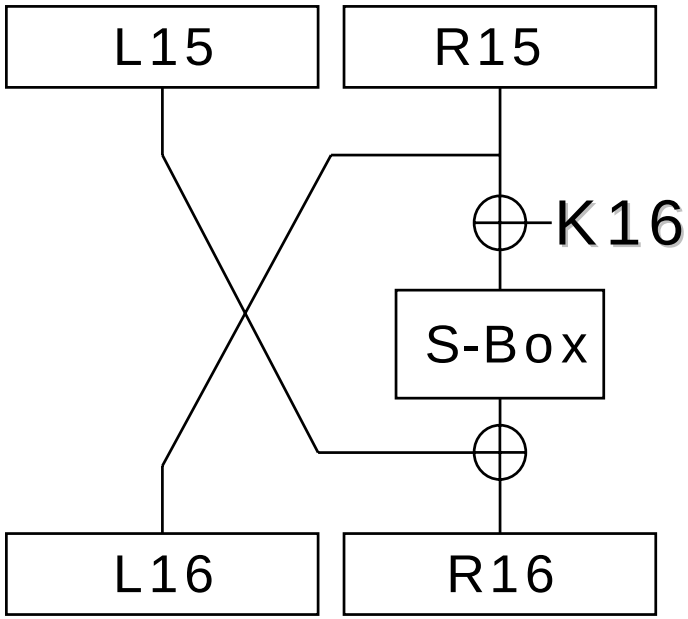
$$R16 \oplus R16' = S(L16 \oplus K16) \oplus L15 \oplus S(L16' \oplus K16) \oplus L15'$$
$$= S(L16 \oplus K16) \oplus S(L16' \oplus K16)$$

- Why does this work?
  - Because for each s-box $L15 \oplus L15' = 0$
- For two unrelated ciphertexts then $L15 \oplus L15' = 0$ with probability 1/16, for each s-box.
  - Hypotheses are uniformly distributed
- If a fault in a round towards the end of a DES then $L15 \oplus L15' = 0$ with probability *p*.

$$\frac{1}{16} < p \leq 1$$

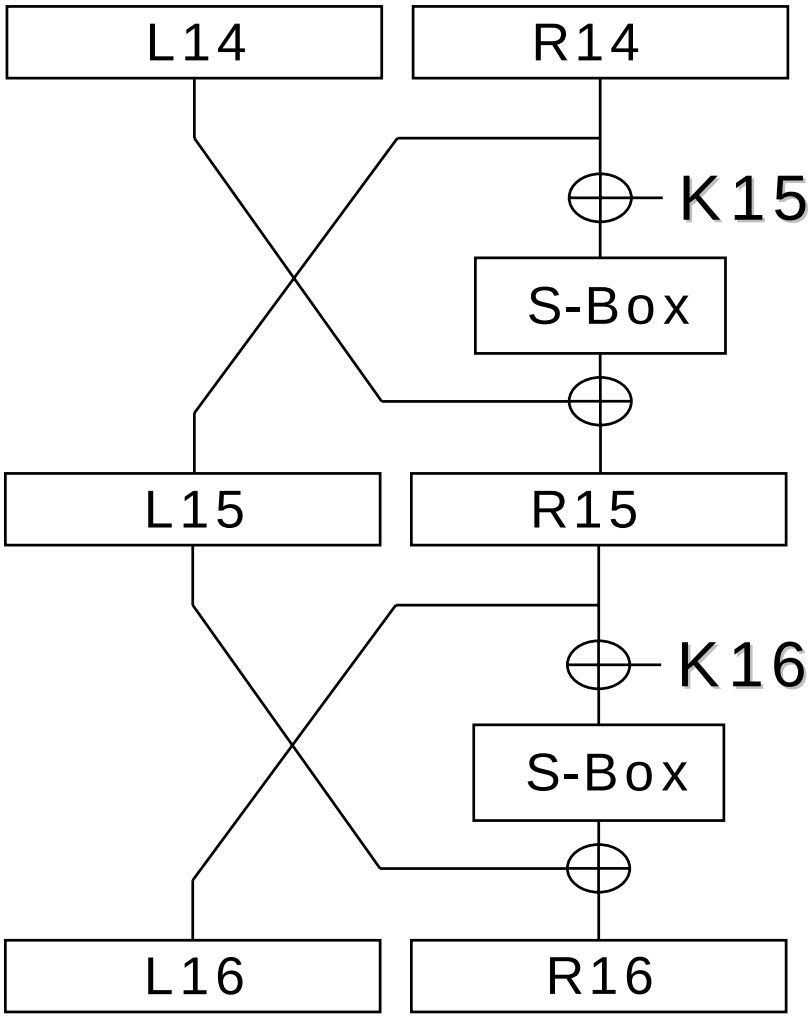


1 Bit Faults: Round 15



- 1 bit fault in R15
- Gives differentials over 1 or 2 s-boxes.
- Several samples will allow the key to be derived as before.

1 Bit Faults: Round 14



- 1 bit fault in R14, will also change one bit in L15.
- For 7 of the 8 s-boxes,

$$L15 \oplus L15' = 0$$

- For each s-box:

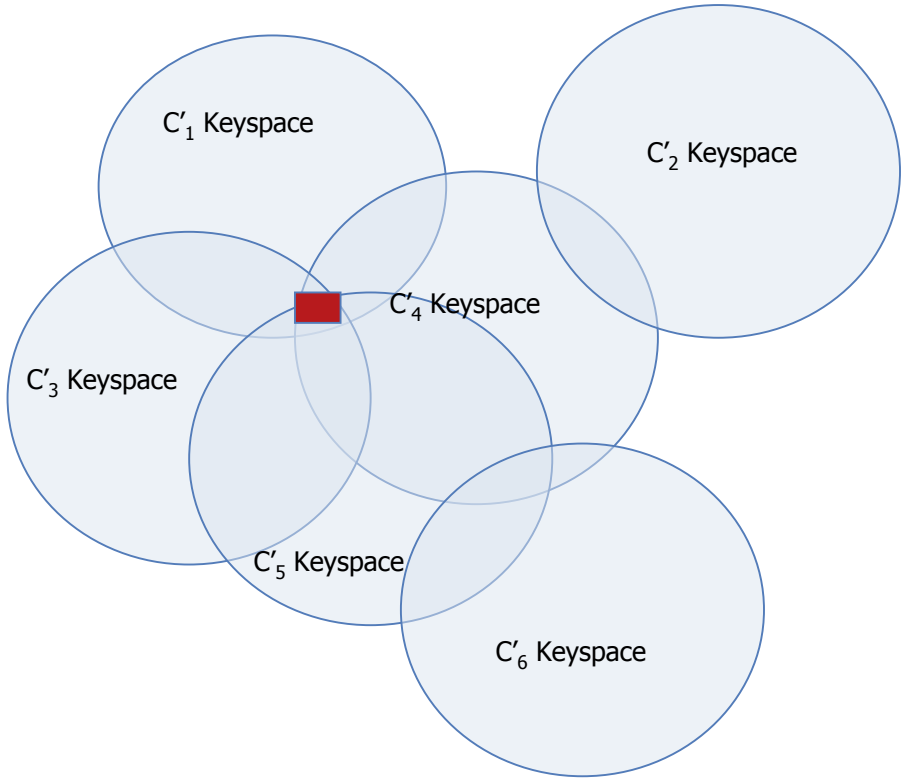
P($L15 \oplus L15' = 0$) = 7/8

- This probability will approach 1/16 the further into the algorithm the fault is injected.

Bull & Innovatron Patents

Differential Fault Analysis

- Keyspace generated in exactly the same way as for fifteenth round fault.
- There is no intersection of all keyspaces generated, a system of votes is conducted.
- The red area has the highest chance of being the key.

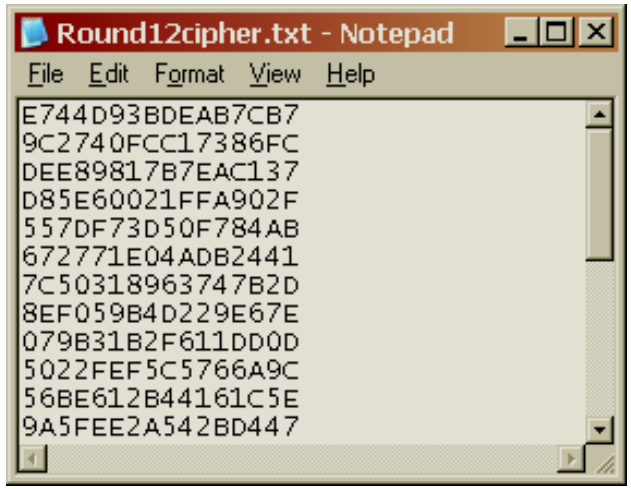


Differential Fault Analysis

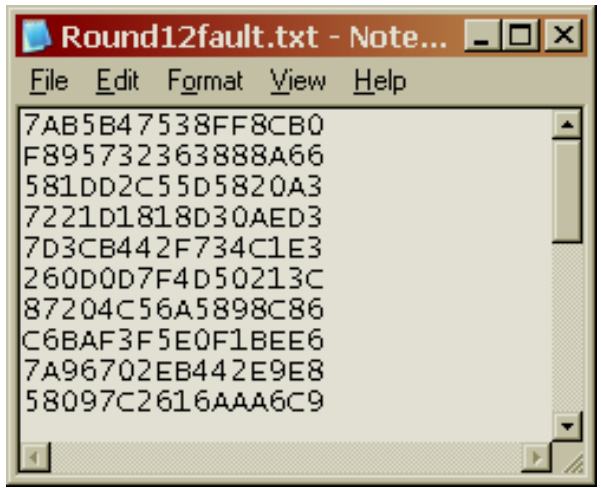
- The amount of faulty ciphertexts required increases the further away from the end of the DES the fault is, and the amount of bits modified.
- Theoretical results with 1 bit faults.
  - Easy until round 11 (less than 1000) ciphertexts
  - Round 10 requires several million ciphertexts
  - Round 9 ?
    - Attempt with 10's of millions failed …

A Simulated Example

- Ciphertex file



- Faulty Ciphertext file



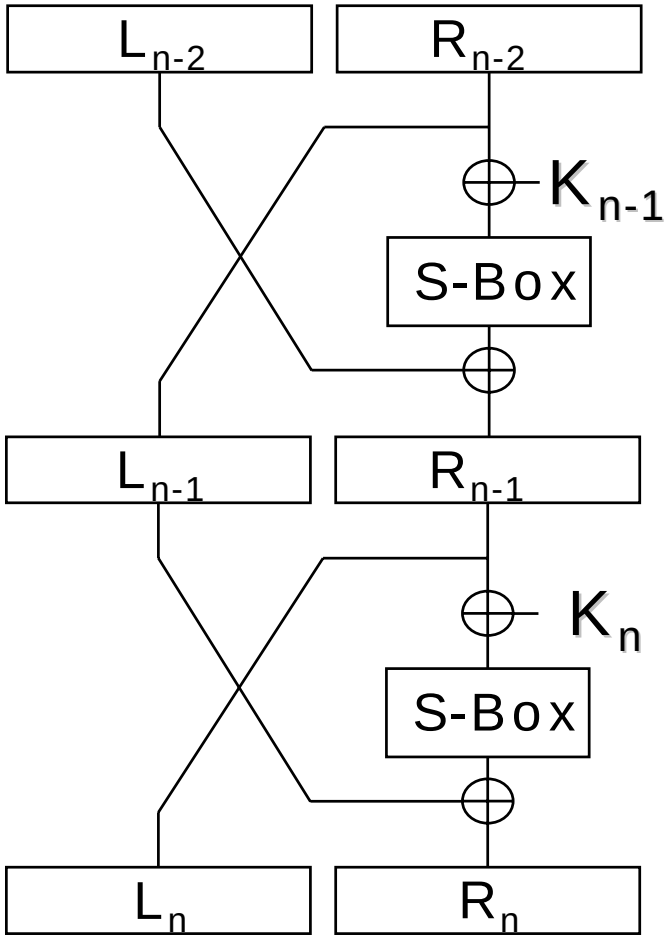
A Simulated Example

```
00 : 7 5 8 4 7 4 6 7
01 : 7 3 7 4 7 4 5 7
02 : 7 5 8 4 6 5 6 6
03 : 7 4 8 5 7 5 6 8
04 : 6 5 7 5 7 5 5 7
05 : 5 5 8 4 7 4 6 5
06 : 6 5 8 4 7 6 5 6
07 : 6 5 8 4 7 5 6 8
08 : 7 4 7 5 7 4 5 8
09 : 6 5 2 5 7 4 5 6
0a : 7 5 8 5 7 6 5 6
0b : 6 5 7 5 7 6 6 8
0c : 6 0 6 5 7 5 6 8
0d : 0 3 7 5 7 5 6 2
0e : 6 3 7 4 7 4 6 7
0f : 6 3 8 2 7 5 6 7
10 : 6 5 8 5 2 6 5 7
11 : 7 4 8 5 6 5 6 8
12 : 7 5 8 5 4 5 5 8
13 : 7 5 8 5 6 3 6 7
14 : 7 5 7 4 5 6 6 8
...
```

- Actual subkey:

```
0D 0C 09 34 10 38 3A 0D
```

Gaining Extra Rounds



- Any fault in $\mathbf{R_n}$ will have an equivalent fault in $\mathbf{L_{n-1}}$.
- $\mathbf{L_{n-1}}$ is static, therefore need to target the copying of $\mathbf{R_{n-2}}$.
  - Implementation Specific.
  - Several millions faults in 8th round.
  - Less than a thousand in the 9th.
- Advanced Simple Power Analysis

Bull & Innovatron Patents

GEMPLUS
beyond smart

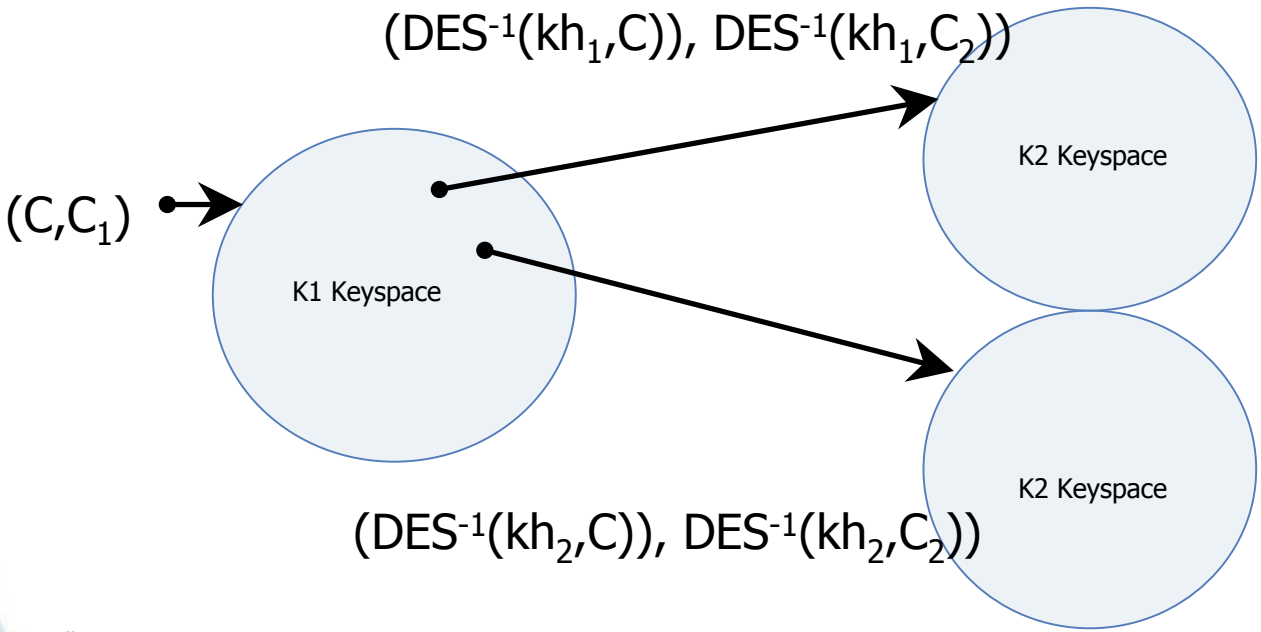
Royal Holloway
University of London

3DES

Differential Fault Analysis

- If injecting faults in the last and middle DES (the fifteenth round of each).
  - C correct ciphertext.
  - C_1 ciphertext with fault in fifteenth round of the last DES.
  - C_2 ciphertext with fault in fifteenth round of the middle DES.

- For each key hypothesis generated for K1, a keyspace can be generated and search for K2



Differential Fault Analysis

- Each hypothesis for K1 produces 2^{32} hypotheses for K2, the total number of keys (K1, K2) that need to be searched is:

  $2^{32} \times 2^{32} = 2^{64}$

- This can be improved upon with more acquisitions, with two faulty ciphertexts from each DES:

  $2^{14} \times 2^{14} = 2^{28}$

- This can still be improved upon …

Differential Fault Analysis

- If a given key hypothesis (kh_i) contains K1 then

$$(DES^{-1}(kh_i,C)), DES^{-1}(kh_i,C_2))$$

Will contain K2, and the differentials generated across each s-box in the last round will be distributed on:

Impossible Differentials

- Again using the table described in, ”Differential Cryptanalysis of DES-like Cryptosystems” by Biham and Shamir

$R16 \oplus R16'$ →

$S-in$ | $\oplus$ | $S-in'$ ↓

```
{ 64,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0 },
{  0,  0,  0,  6,  0,  2,  4,  4,  0, 10, 12,  4, 10,  6,  2,  4 },
{  0,  0,  0,  8,  0,  4,  4,  4,  0,  6,  8,  6, 12,  6,  4,  2 },
{ 14,  4,  2,  2, 10,  6,  4,  2,  6,  4,  4,  0,  2,  2,  2,  0 },
{  0,  0,  0,  6,  0, 10, 10,  6,  0,  4,  6,  4,  2,  8,  6,  2 },
{  4,  8,  6,  2,  2,  4,  4,  2,  0,  4,  4,  0, 12,  2,  4,  6 },
{  0,  4,  2,  4,  8,  2,  6,  2,  8,  4,  4,  2,  4,  2,  0, 12 },
{  2,  4, 10,  4,  0,  4,  8,  4,  2,  4,  8,  2,  2,  2,  4,  4 },
{  0,  0,  0, 12,  0,  8,  8,  4,  0,  6,  2,  8,  8,  2,  2,  4 },
{ 10,  2,  4,  0,  2,  4,  6,  0,  2,  2,  8,  0, 10,  0,  2, 12 },
{  0,  8,  6,  2,  2,  8,  6,  0,  6,  4,  6,  0,  4,  0,  2, 10 },
{  2,  4,  0, 10,  2,  2,  4,  0,  2,  6,  2,  6,  6,  4,  2, 12 },
{  0,  0,  0,  8,  0,  6,  6,  0,  0,  6,  6,  4,  6,  6, 14,  2 },
{  6,  6,  4,  8,  4,  8,  2,  6,  0,  6,  4,  6,  0,  2,  0,  2 },
{  0,  4,  8,  8,  6,  6,  4,  0,  6,  6,  4,  0,  0,  4,  0,  8 },
{  2,  0,  2,  4,  4,  6,  4,  2,  4,  8,  2,  2,  2,  6,  8,  8 },
...
```

Impossible Differentials

- If a given key hypothesis (kh_i) does not contains K1 then

$$(DES^{-1}(kh_i,C)), DES^{-1}(kh_i,C_2))$$

Will not contain K2, and the differentials generated across each s-box will be uniformly distributed over, i.e. they will be random values:

Impossible Differentials

- Again using the table described in, ”Differential Cryptanalysis of DES-like Cryptosystems” by Biham and Shamir

$R16 \oplus R16'$ →

$S-in$ ⊕ $S-in'$ ↓

```
{ 64,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0 },
{  0,  0,  0,  6,  0,  2,  4,  4,  0, 10, 12,  4, 10,  6,  2,  4 },
{  0,  0,  0,  8,  0,  4,  4,  4,  0,  6,  8,  6, 12,  6,  4,  2 },
{ 14,  4,  2,  2, 10,  6,  4,  2,  6,  4,  4,  0,  2,  2,  2,  0 },
{  0,  0,  0,  6,  0, 10, 10,  6,  0,  4,  6,  4,  2,  8,  6,  2 },
{  4,  8,  6,  2,  2,  4,  4,  2,  0,  4,  4,  0, 12,  2,  4,  6 },
{  0,  4,  2,  4,  8,  2,  6,  2,  8,  4,  4,  2,  4,  2,  0, 12 },
{  2,  4, 10,  4,  0,  4,  8,  4,  2,  4,  8,  2,  2,  2,  4,  4 },
{  0,  0,  0, 12,  0,  8,  8,  4,  0,  6,  2,  8,  8,  2,  2,  4 },
{ 10,  2,  4,  0,  2,  4,  6,  0,  2,  2,  8,  0, 10,  0,  2, 12 },
{  0,  8,  6,  2,  2,  8,  6,  0,  6,  4,  6,  0,  4,  0,  2, 10 },
{  2,  4,  0, 10,  2,  2,  4,  0,  2,  6,  2,  6,  6,  4,  2, 12 },
{  0,  0,  0,  8,  0,  6,  6,  0,  0,  6,  6,  4,  6,  6, 14,  2 },
{  6,  6,  4,  8,  4,  8,  2,  6,  0,  6,  4,  6,  0,  2,  0,  2 },
{  0,  4,  8,  8,  6,  6,  4,  0,  6,  6,  4,  0,  0,  4,  0,  8 },
{  2,  0,  2,  4,  4,  6,  4,  2,  4,  8,  2,  2,  2,  6,  8,  8 },
...
```

Impossible Differentials

- If for a given s-box, a given differential is produced that has a frequency of zero, it is an impossible differential.
- If an impossible differential occurs then the pair,

$$(DES^{-1}(kh_i,C)), DES^{-1}(kh_i,C_2))$$

is invalid (i.e. K1 is wrong) and can be discarded, avoiding a seach of 2^{32} keys.

Predicting the Key Space

- Looking at the fraction of zeros in the differentials:
  - S-box 0 : Fraction non-zero = 0.79
  - S-box 1 : Fraction non-zero = 0.78
  - S-box 2 : Fraction non-zero = 0.79
  - S-box 3 : Fraction non-zero = 0.68
  - S-box 4 : Fraction non-zero = 0.76
  - S-box 5 : Fraction non-zero = 0.80
  - S-box 6 : Fraction non-zero = 0.77
  - S-box 7 : Fraction non-zero = 0.77
- P(All differentials are non-zero | K1 is false)= 0.119
- P(can discard hypotheses | K1 is false) = 1 – 0.119
  = 0.8806

Differential Fault Analysis

- A each hypothesis for K1 produces 2^{32} hypotheses for K2, the total number of keys (K1, K2) that need to be searched is:

$$2^{32} \times (2^{32} \times 0.119) = 2^{32} \times 2^{29} = 2^{61}$$

- This can be improved upon with more acquisitions, with two faulty ciphertexts from each DES:

$$2^{14} \times (2^{14} \times 0.119^2) = 2^{14} \times 2^{8} = 2^{22}$$

- The same arguement can be applied to a 3DES using three different keys.

GEMPLUS
beyond smart

Royal Holloway
University of London

Conclusion

Conclusions

- Differential Fault Analysis could be expected to be as powerful as Differential Cryptanalysis
  - However, less data is generally available i.e. it takes a certain effort to inject a fault.
  - Lack of control of the message (fault) can be problematic.
- Countermeasures are well known.
  - Round/Algorithm Redundancy.
  - Variable Redundancy.
  - Random Delays.

GEMPLUS
beyond smart

Royal Holloway
University of London

Questions?