KU LEUVEN

Generalized Matsui Algorithm 1 with application for the full DES

Tomer Ashur, **Raluca Posteuca**, Danilo Šijačić and Stef D'haeseleer

SCN 2020 Conference

September 14-16, 2020

Outline

1. Introduction
   - Linear cryptanalysis
   - Related work
   - Our contribution
2. DES cipher
3. Strictly zero-correlation linear approximations
   - 1-round poisonous trail for DES
   - Poisonous trail for full DES
   - Key-recovery attack
4. Experimental verification
5. Conclusion. Research directions

Linear cryptanalysis

- Introduced in early 1990 by Mitsuru Matsui, who applied the technique to the DES cipher
- The idea: to find a linear approximation between a set of plaintext bits, ciphertext bits and key bits that holds with probability different from 0.5
- A linear approximation of a block cipher with mask vector (u, v): the relation

$$u \cdot p + v \cdot c = 0$$

("·" - inner product)

Linear cryptanalysis

- The quality of a linear approximation - the correlation: $corr = 2 \cdot prob - 1$;
- For iterated ciphers – sequentially linearize each round ⇒ linear trail
- The correlation of a linear trail = the product of each round's correlation (Piling-up lemma)

Related work

- The linear hull effect (Nyberg, 1994): more than one linear trail involving the same plaintext and ciphertext bits
- The correlation of a hull: the sum of the underlying linear trails' correlations
- Different linear trails will interfere, influencing the correlation in a constructive or destructive manner, or even canceling out one-another

Related work

- Ashur and Rijmen (Indocrypt 2016) – the linear hull effect may sometimes appear at a micro-level, inside a single round of the cipher – research on the SIMON cipher

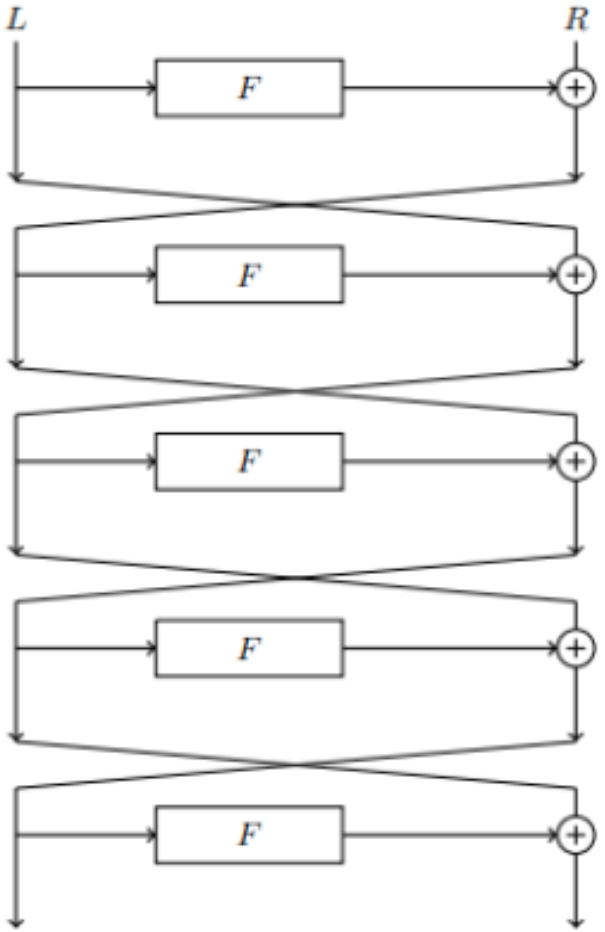
- Ashur and Posteuca (BalkanCryptSec 2018) – under certain constraints, the f-function of DES exhibits 0-correlation key-dependent one-round linear hulls

Our contribution

- A new type of attack based on linear cryptanalysis, called “strictly zero-correlation" attack;
- A new attack covering the full DES;
- Key-recovery attack based on the key-dependent behavior of a linear trail.

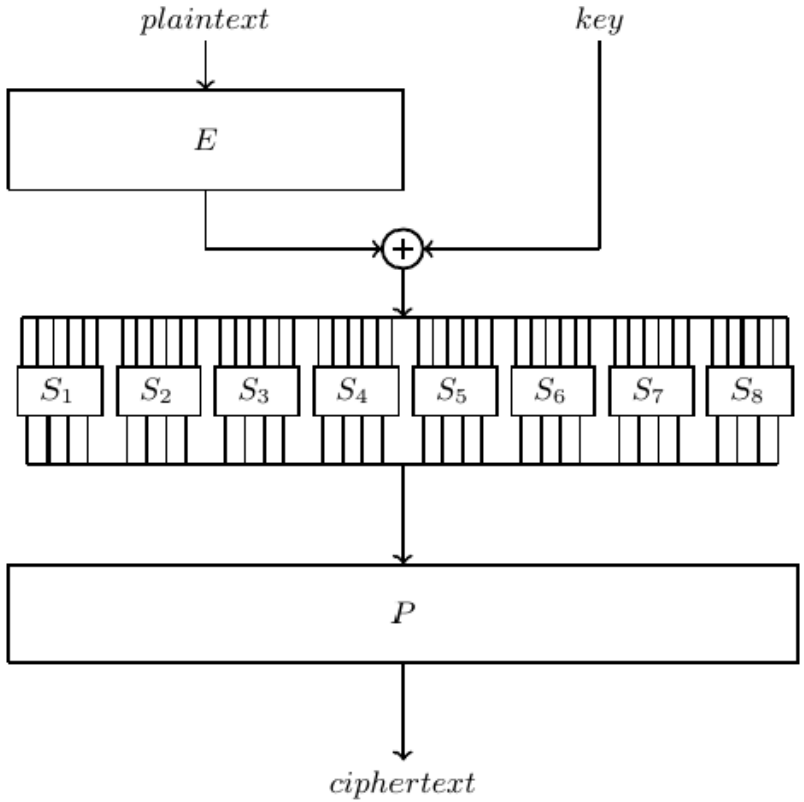
The DES cipher

- Feistel structure based on the non-linear function F
- 64-bit plaintext and key (only 56 key bits actually used)
- 16 rounds



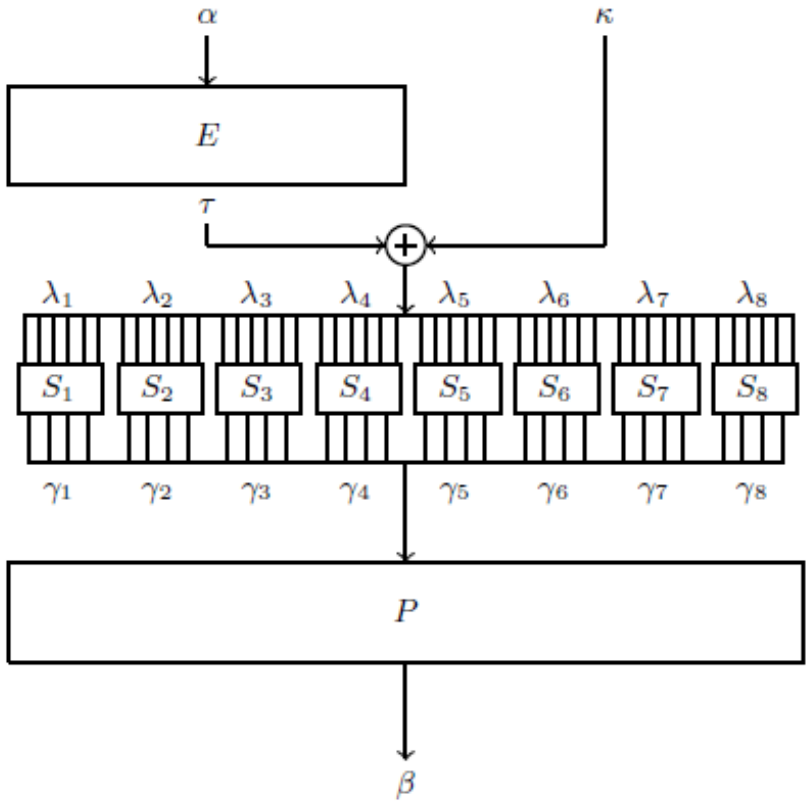
The F-function

- E: 32-bit input is expanded into a 48-bit output
- S_i: 6×4- bit S-boxes
- P: 32-bit permutation



A linear trail through the F-function

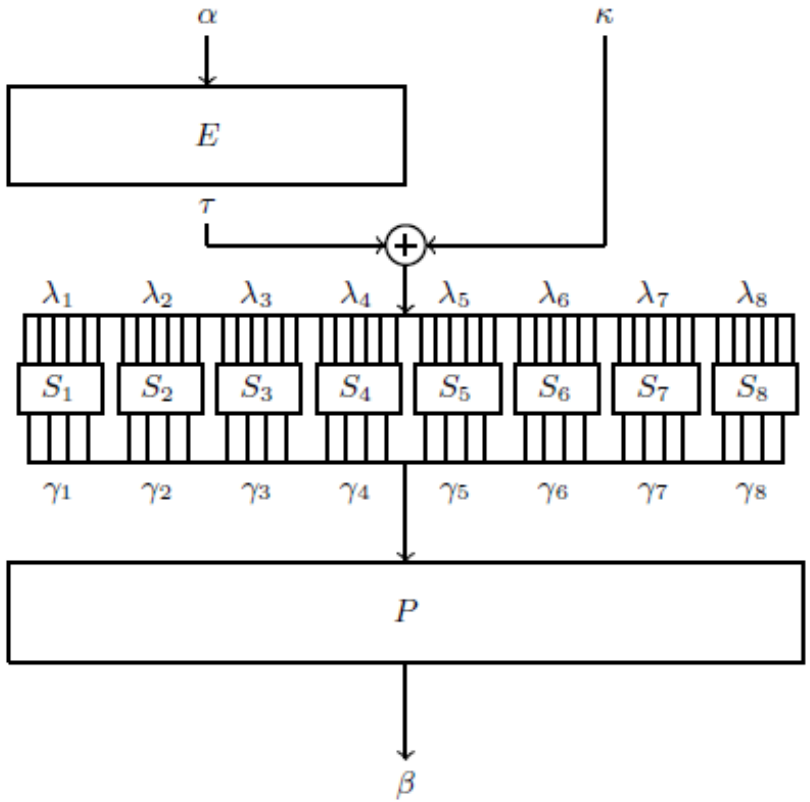
- τ, κ and λ must all be the same
- each pair (λ_i, γ_i) must be connectable respective to the i^{th} S-box's LAT
- $\beta = P(\gamma)$



A linear trail through the F-function

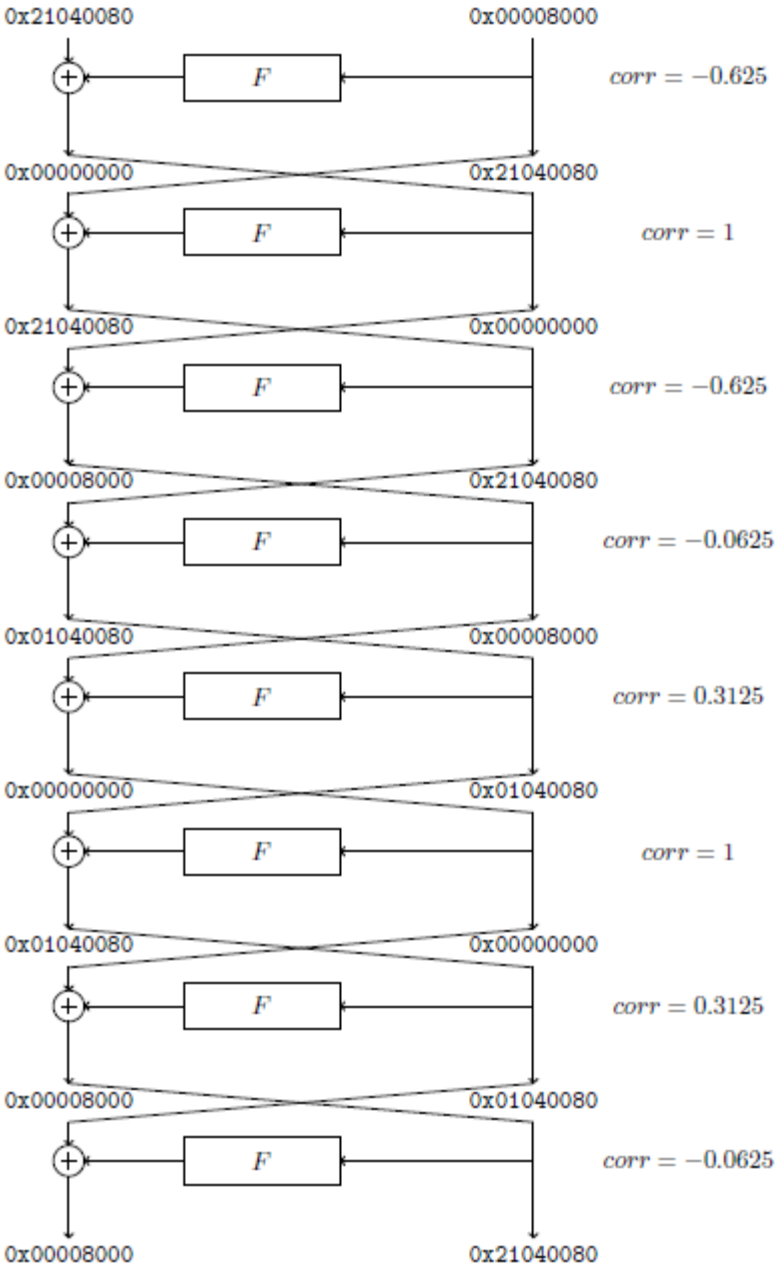
- τ, κ and λ must all be the same
- each pair (λ_i, γ_i) must be connectable respective to the i^{th} S-box's LAT
- $\beta = P(\gamma)$

If α and β are fixed, then τ might take multiple values



Matsui's linear trail

- Uses an 8-round iterative linear trail with correlation $2^{-12.71}$
- Original attack – the masks of the first and last rounds are replaced with locally better ones
- Since the trail is iterative – can start in any of the trail rounds and extended naturally over the next 7 rounds



1-round poisonous trail for DES

- $(\alpha, \beta) = (0x01CF8000, 0x00440000)$

Trail No.	τ_i	Correlation	Key masks
Trail 1	$(0, 0, \texttt{0x39}, \texttt{0x0F}, 0, 0, 0, 0)$	$2^{-8} \cdot 5$	$\{12, 13, 14, 20, 21, 22, 23\} \cup \{17\}$
Trail 2	$(0, 0, \texttt{0x3B}, \texttt{0x2F}, 0, 0, 0, 0)$	$2^{-8} \cdot 5$	$\{12, 13, 14, 20, 21, 22, 23\} \cup \{16, 17, 18\}$
Trail 3	$(0, 0, \texttt{0x38}, \texttt{0x1F}, 0, 0, 0, 0)$	$2^{-8} \cdot 12$	$\{12, 13, 14, 20, 21, 22, 23\} \cup \{19\}$
Trail 4	$(0, 0, \texttt{0x3A}, \texttt{0x3F}, 0, 0, 0, 0)$	$-2^{-8} \cdot 2$	$\{12, 13, 14, 20, 21, 22, 23\} \cup \{16, 18, 19\}$

$$corr = \begin{cases} \pm 2^{-8} \cdot 14 & k_{16} \neq k_{18} \\ \pm 2^{-8} \cdot 20 & k_{16} = k_{18} \text{ and } k_{17} = k_{19} \\ 0 & \text{otherwise} \end{cases}$$

1-round poisonous trail for DES

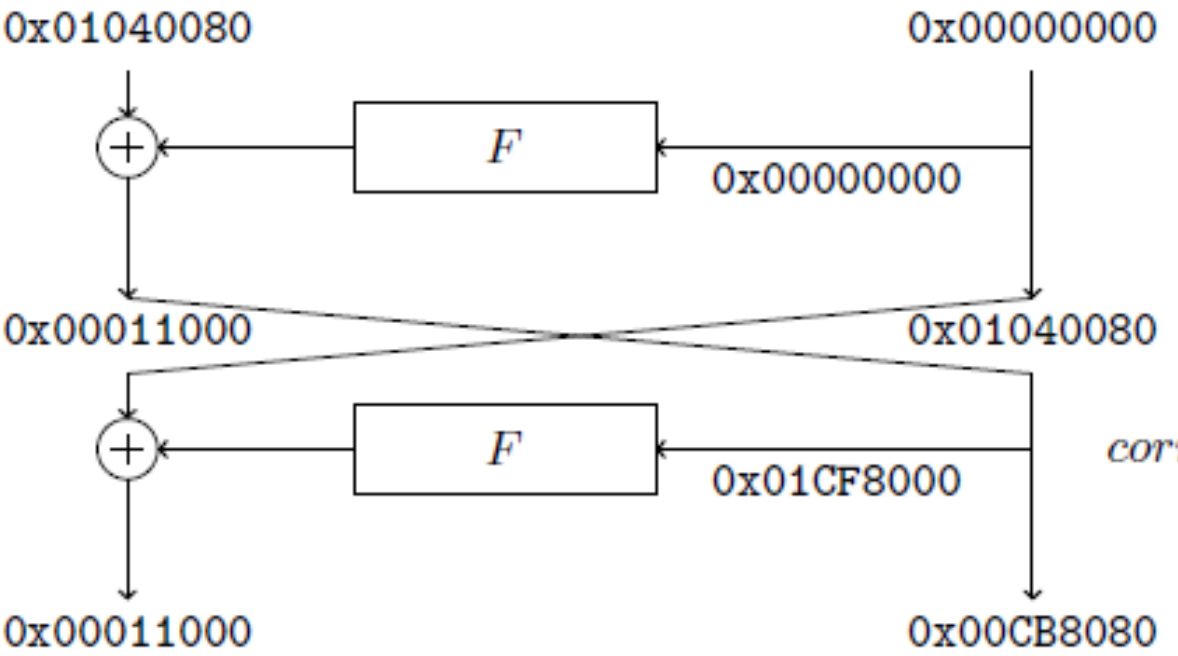
- $(\alpha, \beta) = (0x01CF8000, 0x00440000)$

Trail No.	τ_i	Correlation	Key masks
Trail 1	(0, 0, 0x39, 0x0F, 0, 0, 0, 0)	$2^{-8} \cdot 5$	$\{12, 13, 14, 20, 21, 22, 23\} \cup \{17\}$
Trail 2	(0, 0, 0x3B, 0x2F, 0, 0, 0, 0)	$2^{-8} \cdot 5$	$\{12, 13, 14, 20, 21, 22, 23\} \cup \{16, 17, 18\}$
Trail 3	(0, 0, 0x38, 0x1F, 0, 0, 0, 0)	$2^{-8} \cdot 12$	$\{12, 13, 14, 20, 21, 22, 23\} \cup \{19\}$
Trail 4	(0, 0, 0x3A, 0x3F, 0, 0, 0, 0)	$-2^{-8} \cdot 2$	$\{12, 13, 14, 20, 21, 22, 23\} \cup \{16, 18, 19\}$

$$corr = \begin{cases} \pm 2^{-8} \cdot 14 & k_{16} \neq k_{18} \\ \pm 2^{-8} \cdot 20 & k_{16} = k_{18} \text{ and } k_{17} = k_{19} \\ 0 & \text{otherwise} \end{cases}$$

Poisonous trail

2-round poisonous trail for DES



$$corr = 0.5$$

$$corr = \begin{cases} 0 \\ \pm 2^{-8} \cdot 20 \\ \pm 2^{-8} \cdot 14 \end{cases}$$

Note: the input mask is one of the masks used in Matsui's trail

16-round poisonous trail for DES

- We adapt Matsui's trail by replacing the last two rounds with our 2-round poisonous trail
- Taking into account the key schedule, the correlation based on the master key is:

$$corr = \begin{cases} \pm 2^{-24.95} & k_{51} \neq k_1 \\ \pm 2^{-24.42} & k_{51} = k_1 \text{ and } k_0 = k_8 \\ 0 & \text{otherwise} \end{cases}$$

- The new trail is 1.38 times better than the original one (for some keys)

Distinguishing in practice

- Our trail divides the set of master keys into three key-classes, depending on the correlation
- By observing the correlation – information regarding master key bits (relation between k_{51} and k_1 or relation between k_0 and k_8)
- One relation – equivalent to one key bit recovery (exhaustive search space is halved)

The key-recovery attack

- The attack:
  1. Compute the correlation using 2^{51} (plaintext, ciphertext) pairs
  2. Compare the empirical correlation to the three expected values
  3. Recover the key constraints met by the master key
- Data complexity: 2^{51} arbitrary plaintexts (computed according to the smallest non-zero correlation)

Experimental verification

- On the last 9 rounds of the trail:
  - 2^{38} data
  - Software implementation
  - Three experiments – one for each key class
  - The empirical correlations were very close to the expected one

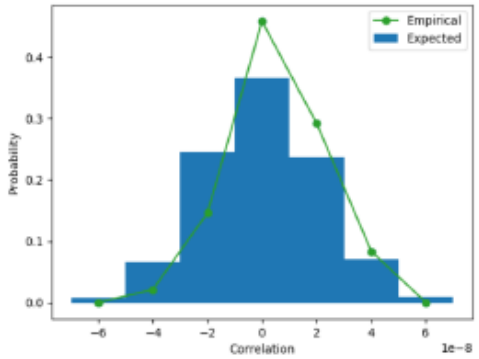
Expected weight	Empirical correlation	Key constraint on RK_9
$-\infty$	-18.608	$k_{16} = k_{18}$ and $k_{17} \neq k_{19}$
-16.245	-16.055	$k_{16} \neq k_{18}$
-15.714	-15.631	$k_{16} = k_{18}$ and $k_{17} = k_{19}$

Experimental verification

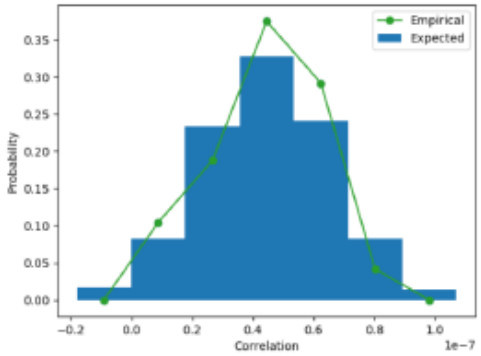
- On the full DES:
  - 2^{51} data
  - Hardware implementation - a custom DES accelerator
  - 144 experiments – 48 for each key class
  - For each key class - $\log_2$ of the absolute value of the mean of the empirical correlations

Expected weight	Average weight (empirical)	Key constraint (respective to the master key)	Success probability
-24.95	-24.90	$k_{51} \neq k_1$	62.5%
-24.42	-24.41	$k_{51} = k_1$ and $k_0 = k_8$	66.6 %
$-\infty$	-26.39	$k_{51} = k_1$ and $k_0 \neq k_8$	39.5 %
Average success probability: 51.9%			

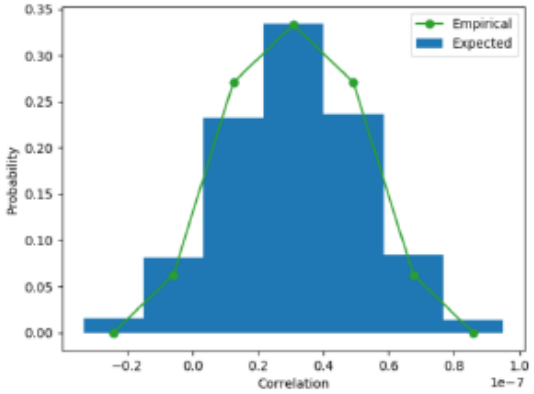
Experimental verification



(a) Expected correlation $= 0$. Each of the 7 bins is of size $2^{-25.57}$ starting from $-2^{-23.76}$.



(b) Expected correlation $= \pm 2^{-24.42}$. Each of the 7 bins is of size $2^{-25.73}$ starting from $2^{-25.72}$.



(c) Expected correlation $= \pm 2^{-24.95}$. Each of the 7 bins is of size $2^{-25.69}$ starting from $2^{-24.83}$.

Linear hull effect on DES

- The empirical results are “close enough”, but does DES exhibit the linear hull effect?
- Matsui’s linear attack – no linear hull effect considered
- Many subsequent works assume that:
  - DES does not exhibit the linear hull effect OR
  - Every linear hull contains one dominant linear trail

Linear hull effect on DES

- The empirical results are “close enough”, but does DES exhibit the linear hull effect? **YES**
- Matsui’s linear attack – no linear hull effect considered
- Many subsequent works assume that:
  - DES does not exhibit the linear hull effect OR
  - Every linear hull contains one dominant linear trail

Linear hull effect on DES

- The empirical results are “close enough”, but does DES exhibit the linear hull effect? **YES**
- Matsui’s linear attack – no linear hull effect considered
- Many subsequent works assume that:
  - DES does not exhibit the linear hull effect OR
  - Every linear hull contains one dominant linear trail
- For our trail - a second 5-round linear trail
- Correlation significantly smaller than our corresponding 5-round trail – can be treated as noise

Conclusion

- Construction of a 0-correlation key-dependent linear trail for more than 1 round (up until full DES)
- Key-recovery attack on full DES
- Experimental verification using a custom DES accelerator

Conclusion

- Construction of a 0-correlation key-dependent linear trail for more than 1 round (up until full DES)
- Key-recovery attack on full DES
- Experimental verification using a custom DES accelerator
- **Research directions:**
  - Other block ciphers that exhibit “poisonous” linear trails
  - Improvements of the key-recovery attack
  - Impact of this research over 3DES
  - Extension of the key-recovery attack to the case of multiple linear cryptanalysis

Thank you! ☺

tomer.ashur@esat.kuleuven.be

raluca.posteuca@esat.kuleuven.be