Advancing the Meet-in-the-Filter Technique: Applications to CHAM and KATAN

Alex Biryukov[1], Je Sen Teh[1,2], Aleksei Udovenko[1]

[1] SnT, University of Luxembourg
[2] University Sains Malaysia

Selected Areas in Cryptography 2022
25th August 2022

Overview

Meet-in-the-Filter (MiF)

- Recently proposed framework for differential cryptanalysis (Biryukov, Santos, Teh, Udovenko, and Velichkov 2022)
- Combines (variations of) techniques from the literature:
  1. differential meet-in-the-middle, e.g. (Rechberger, Soleimany, and Tiessen 2018)
  2. trail-assisted bit-based key-recovery, e.g. (Dinur 2014)
  3. dynamic counting to trade data for time reduction
- Applied to **Speck**, automated but tedious complexity analysis

Overview

Meet-in-the-Filter (MiF)

- Recently proposed framework for differential cryptanalysis (Biryukov, Santos, Teh, Udovenko, and Velichkov 2022)
- Combines (variations of) techniques from the literature:
  1. differential meet-in-the-middle, e.g. (Rechberger, Soleimany, and Tiessen 2018)
  2. trail-assisted bit-based key-recovery, e.g. (Dinur 2014)
  3. dynamic counting to trade data for time reduction
- Applied to **Speck**, automated but tedious complexity analysis

This work:

1. Theoretical aspects and understanding of MiF
2. Simplified analysis methods (pen-and-paper)
3. Based on trail counting
4. Applications: CHAM-64 and KATAN-32/48/64

Plan

Differential Cryptanalysis

$$\Delta_{IN} \xrightarrow[\text{differential}]{r \text{ rounds}} \Delta_{OUT}$$

Differential Cryptanalysis

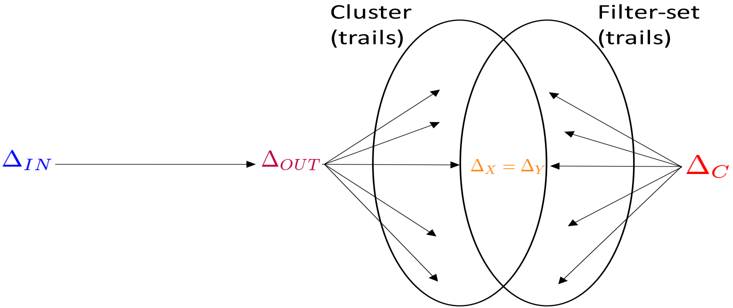
Δ_{IN} —— r rounds / differential ——→ Δ_{OUT} ←—— k rounds / key recovery —— Δ_C, C_1, C_2

Differential Cryptanalysis

$$\Delta_{IN} \xrightarrow[\text{differential}]{r \text{ rounds}} \Delta_{OUT} \xleftarrow[\text{key recovery}]{k \text{ rounds}} \Delta_C, C_1, C_2$$

1. how to find key candidates efficiently?
2. when is such attack worth it?

Meet-in-the-Filter



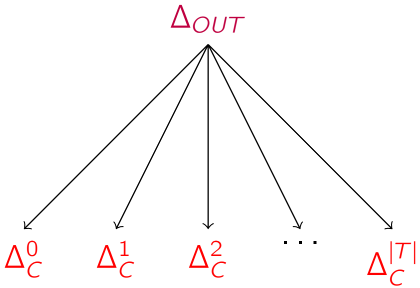
1. precompute the cluster of *trails* $\Delta_{OUT} \rightarrow \Delta_X$
2. for each *observed* Δ_C:
    1. compute the filter-set of *trails* $\Delta_Y \rightarrow \Delta_C$
    2. intersect to get trails $\Delta_{OUT} \rightarrow (\Delta_X = \Delta_Y) \rightarrow \Delta_C$
    3. run trail-assisted key recovery

Plan

Trail Count vs Average Trail Probability

Theorem

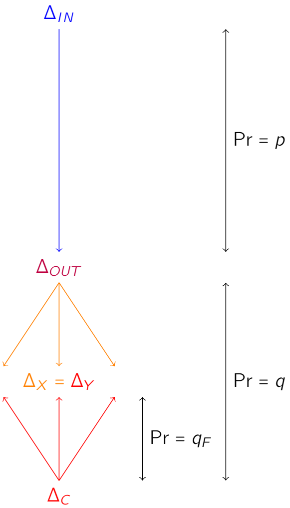
*Let T be the set of **all** k-round trails starting at Δ.*
Then, the average probability of a trail in T is equal to $1/|T|$.



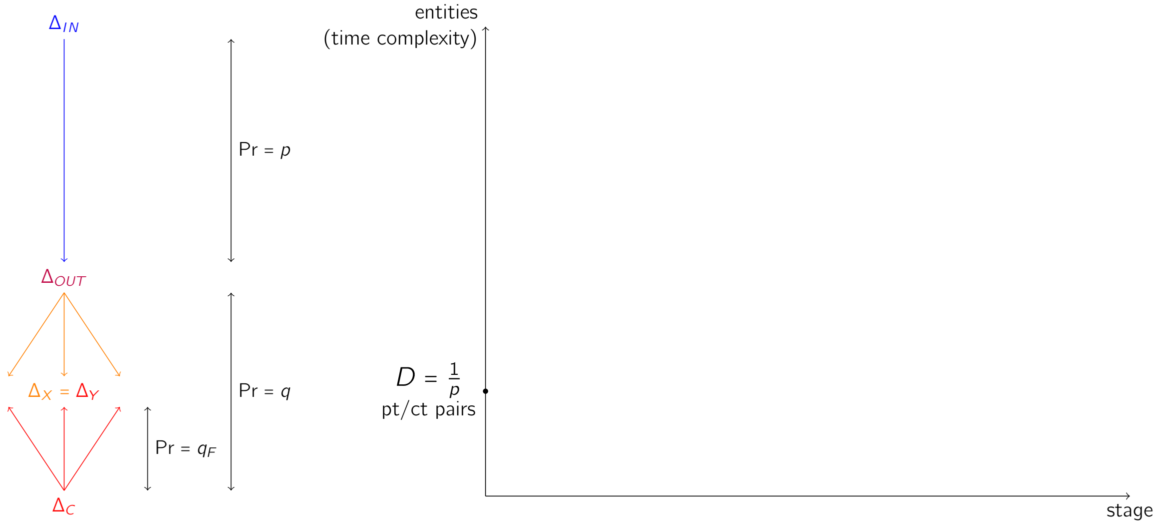
Total Pr = 1

Avg Pr = $\frac{1}{|T|}$

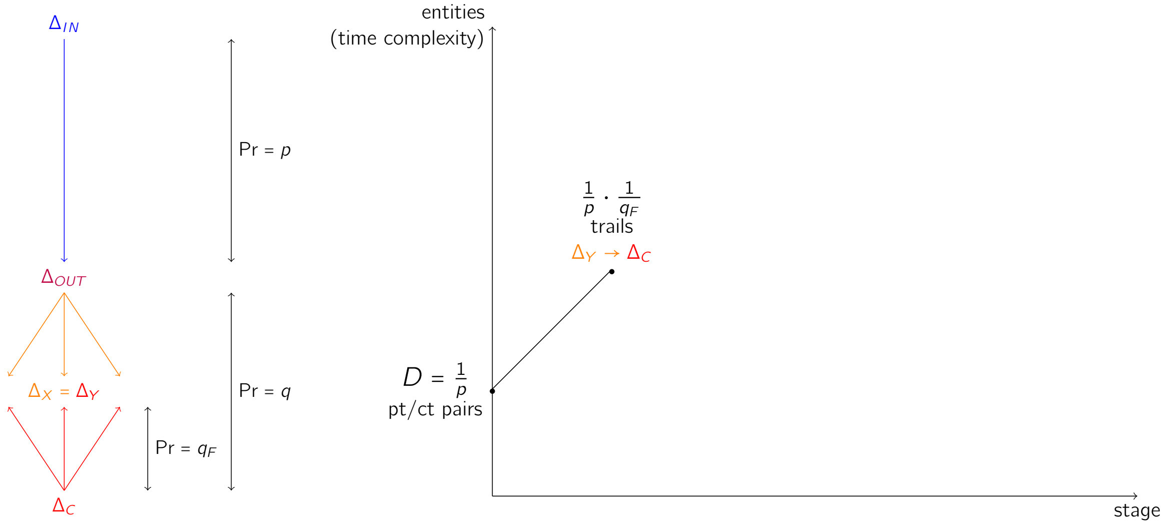
Complexity Analysis Overview



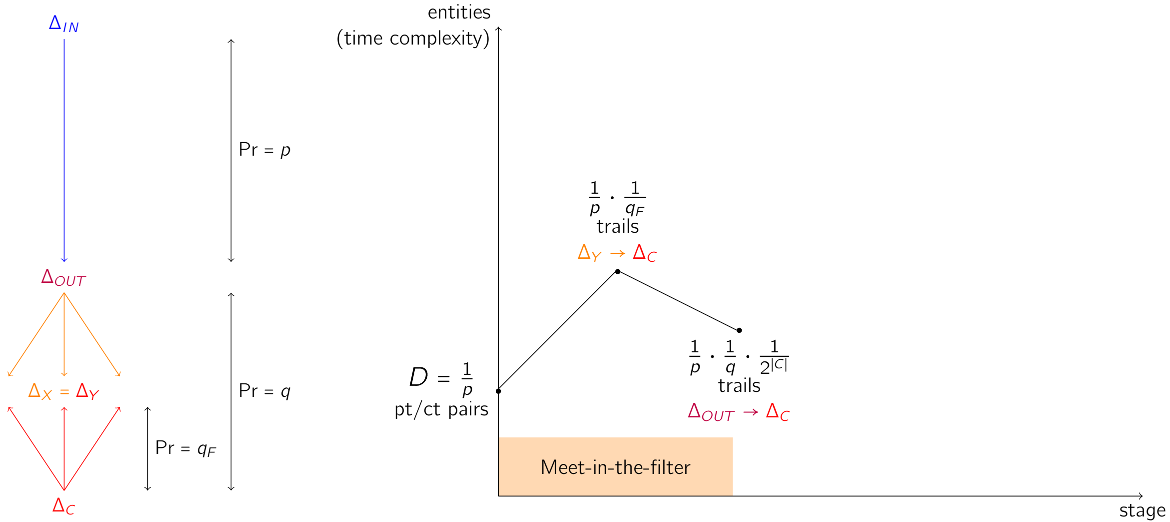
Complexity Analysis Overview



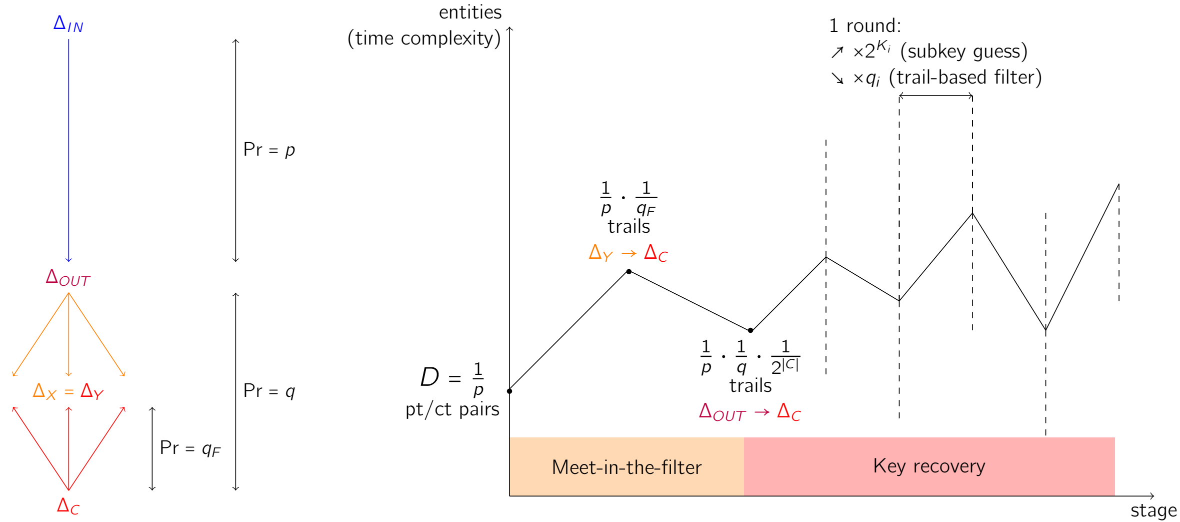
Complexity Analysis Overview



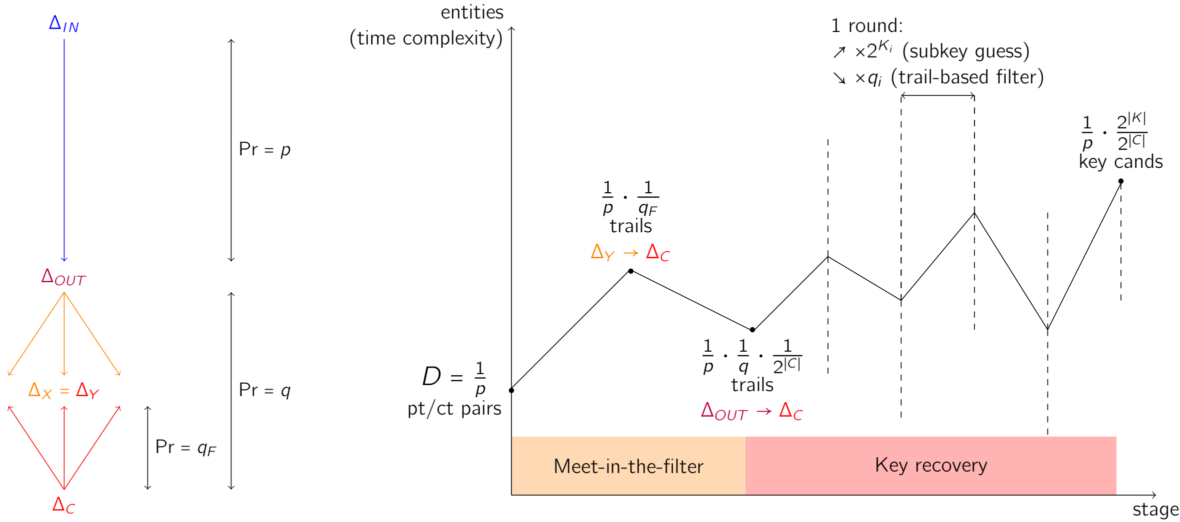
Complexity Analysis Overview



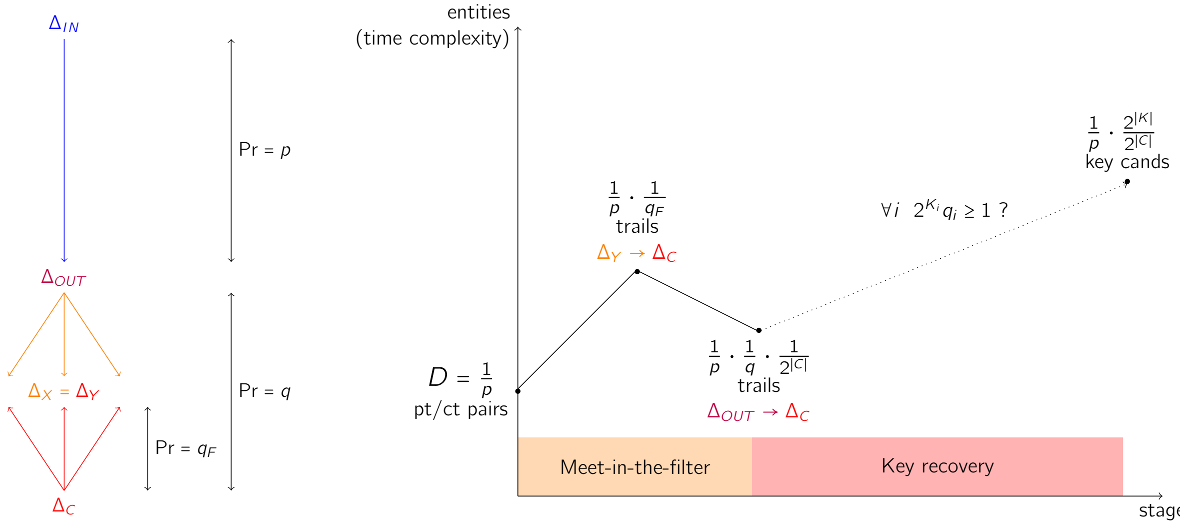
Complexity Analysis Overview



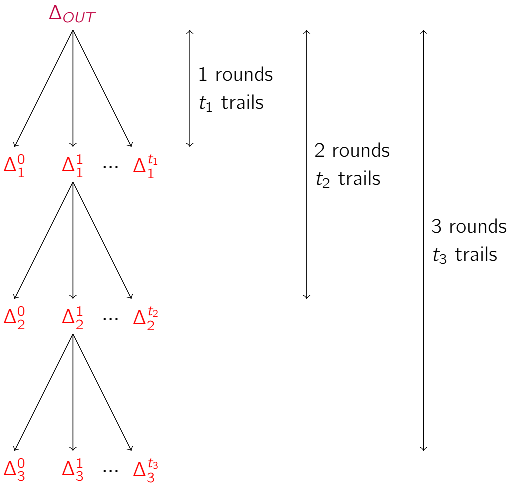
Complexity Analysis Overview



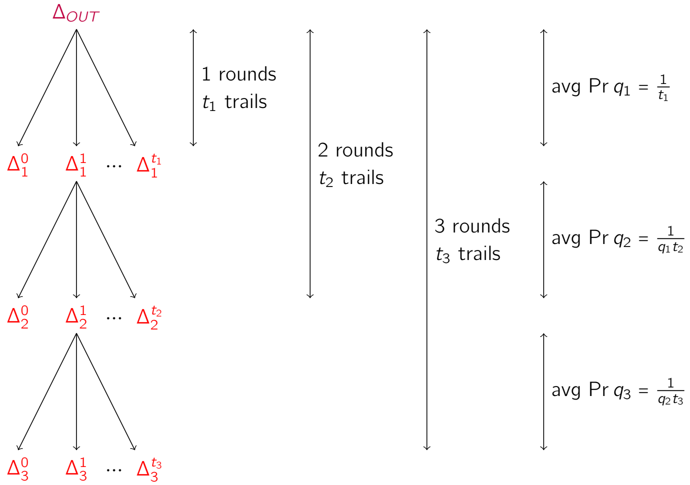
Complexity Analysis Overview



Computing/Estimating Round Filter Strength



Computing/Estimating Round Filter Strength



Computing/Estimating Round Filter Strength

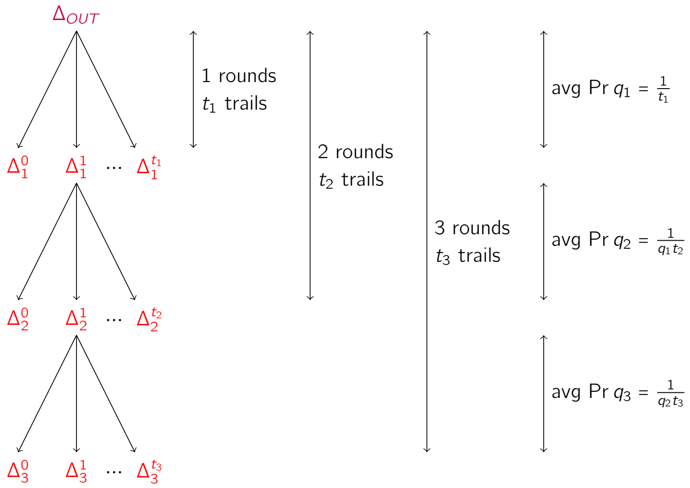
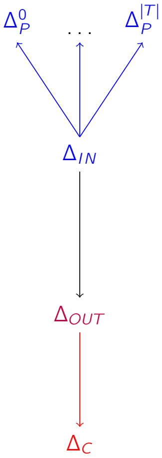


Table: CHAM-64 ext. from $\Delta_{OUT} = (2000, 1000, 2810, 0020)$.

Round	#Trails	Avg.wt/R
1	$2^{1.58}$	1.58
2	$2^{8.12}$	6.54
3	$2^{15.46}$	7.34
4	$2^{19.55}$	4.09
5	$2^{29.89}$	10.34
6	$2^{39.95}$	10.06
7	$2^{52.57}$	12.62
8	$2^{64.84}$	12.27

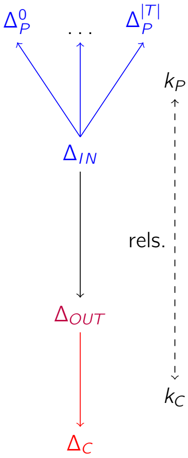
Trail-based Plaintext Structures



- Compute all possible backwards trails $\Delta_{IN} \rightarrow \Delta_P$
- As long as all ${\Delta_P}^i$ fit a structure, e.g.

$$ {\Delta_P}^i \preceq 00*****0* $$

Trail-based Plaintext Structures



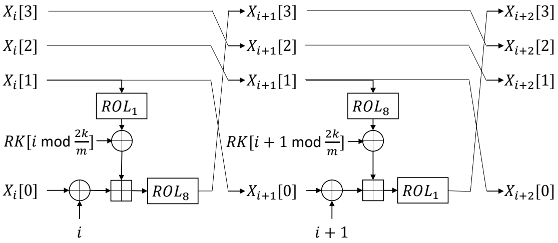
- Compute all possible backwards trails $\Delta_{IN} \rightarrow \Delta_P$
- As long as all ${\Delta_P}^i$ fit a structure, e.g.

$${\Delta_P}^i \preceq 00*****0*$$

- "Free" rounds if can combine the top/bottom filters: 1/q trails of prob. q

Plan

CHAM cipher



- Based on the ARX construction
  1. CHAM-64/128 - 88 rounds
  2. CHAM-128/128 - 112 rounds
  3. CHAM-128/256 - 120 rounds
- Key schedule updates subkey words linearly and independently
- No trail clustering over 4 rounds
  1. 4-round trail fully determined from its input & output differences

Attack Complexities for CHAM-64 (+Literature)

Table: Summary of differential attacks on CHAM-64 (single-key setting).

Type	Rounds	Time	Data	Memory	Ref
Single Trail Distinguisher	39	-	-	-	(Huang and Wang 2019)
Diff. Distinguisher	44	-	-	-	(Roh, Koo, Jung, Jeong, Lee, Kwon, and Kim
Diff. Key-recovery	52	2^{114}	2^{61}	2^{54}	This Paper

- No prior key recovery attacks
  1. Previous work focused on finding differential trails

High-level Attack description

Round split:

1. 4 rounds: plaintext structure, enumerated trails
2. 40 rounds: differential trail ($\Pr = 2^{-60.05}$)
3. 8 rounds: meet-in-the-filter (4 cluster + 4 filter)

High-level Attack description

Round split:

1. 4 rounds: plaintext structure, enumerated trails
2. 40 rounds: differential trail ($\Pr = 2^{-60.05}$)
3. 8 rounds: meet-in-the-filter (4 cluster + 4 filter)

Attack procedure:

1. Encrypt plaintext structures
2. Enumerate pt/ct pairs and pt-side trails
3. Obtain ct-side trails using MiF
4. Guess-and-determine procedure for two-sided MiF key recovery (exploit relations between subkeys from both sides)

Guessing Illustration (1/2)

Table: Backward extension from difference $\Delta_{IN} = (0020, 0010, 1020, 2800)$.

Round	#Trails	Avg.wt/R
-4	$2^{35.67}$	11.87
-3	$2^{23.8}$	11.91
-2	$2^{11.89}$	7.72
-1	$2^{4.17}$	4.17

Table: Forward extension from difference $\Delta_{OUT} = (2000, 1000, 2810, 0020)$.

Round	#Trails	Avg.wt/R
+1	$2^{1.58}$	1.58
+2	$2^{8.12}$	6.54
+3	$2^{15.46}$	7.34
+4	$2^{19.55}$	4.09
+5	$2^{29.89}$	10.34
+6	$2^{39.95}$	10.06
+7	$2^{52.57}$	12.62
+8	$2^{64.84}$	12.27

Guessing Illustration (2/2)

Master key word	Round	Filter	Round	Filter	Total
$K[0]$	1	$2^{-11.87}$	49	$2^{-10.34}$	$2^{-22.21}$
$K[1]$	2	$2^{-11.91}$	50	$2^{-10.06}$	$2^{-21.97}$
$K[2]$	3	$2^{-7.72}$	51	$2^{-12.62}$	$2^{-20.34}$
$K[3]$	4	$2^{-4.17}$	52	$2^{-12.27}$	$2^{-16.44}$
$K[4]$	5	$2^{-1.00}$	46	$2^{-6.54}$	$2^{-7.54}$
$K[5]$	6	$2^{-2.00}$	45	$2^{-1.58}$	$2^{-3.58}$
$K[6]$	7	$2^{-3.00}$	48	$2^{-4.09}$	$2^{-7.09}$
$K[7]$	8	$2^{-2.00}$	47	$2^{-7.34}$	$2^{-9.34}$
all	1-8	$2^{-43.68}$	43-50	$2^{-64.84}$	$2^{-108.52}$

- Time: $2^{0.00}$
- Trail-keys: $2^{60.05+35.67+64.84-64} = 2^{96.56}$

Guessing Illustration (2/2)

Master key word	Round	Filter	Round	Filter	Total
$K[0]$	1	$2^{-11.87}$	49	$2^{-10.34}$	$2^{-22.21}$
$K[1]$	2	$2^{-11.91}$	50	$2^{-10.06}$	$2^{-21.97}$
$K[2]$	3	$2^{-7.72}$	51	$2^{-12.62}$	$2^{-20.34}$
$K[3]$	4	$2^{-4.17}$	52	$2^{-12.27}$	$2^{-16.44}$
$K[4]$	5	$2^{-1.00}$	46	$2^{-6.54}$	$2^{-7.54}$
$K[5]$	6	$2^{-2.00}$	45	$2^{-1.58}$	$2^{-3.58}$
$K[6]$	7	$2^{-3.00}$	48	$2^{-4.09}$	$2^{-7.09}$
$K[7]$	8	$2^{-2.00}$	47	$2^{-7.34}$	$2^{-9.34}$
all	1-8	$2^{-43.68}$	43-50	$2^{-64.84}$	$2^{-108.52}$

- Time: $+2^{100.29} \to 2^{100.29}$
- Trail-keys: $\times 2^{3.73} \to 2^{100.29}$

Guessing Illustration (2/2)

Master key word	Round	Filter	Round	Filter	Total
$K[0]$	1	$2^{-11.87}$	49	$2^{-10.34}$	$2^{-22.21}$
$K[1]$	2	$2^{-11.91}$	50	$2^{-10.06}$	$2^{-21.97}$
$K[2]$	3	$2^{-7.72}$	51	$2^{-12.62}$	$2^{-20.34}$
$K[3]$	4	$2^{-4.17}$	52	$2^{-12.27}$	$2^{-16.44}$
$K[4]$	5	$2^{-1.00}$	46	$2^{-6.54}$	$2^{-7.54}$
$K[5]$	6	$2^{-2.00}$	45	$2^{-1.58}$	$2^{-3.58}$
$K[6]$	7	$2^{-3.00}$	48	$2^{-4.09}$	$2^{-7.09}$
$K[7]$	8	$2^{-2.00}$	47	$2^{-7.34}$	$2^{-9.34}$
all	1-8	$2^{-43.68}$	43-50	$2^{-64.84}$	$2^{-108.52}$

- Time: $+2^{103.67} \rightarrow 2^{103.80}$
- Trail-keys: $\times 2^{3.38} \rightarrow 2^{103.67}$

Guessing Illustration (2/2)

Master key word	Round	Filter	Round	Filter	Total
$K[0]$	1	$2^{-11.87}$	49	$2^{-10.34}$	$2^{-22.21}$
$K[1]$	2	$2^{-11.91}$	50	$2^{-10.06}$	$2^{-21.97}$
$K[2]$	3	$2^{-7.72}$	51	$2^{-12.62}$	$2^{-20.34}$
$K[3]$	4	$2^{-4.17}$	52	$2^{-12.27}$	$2^{-16.44}$
$K[4]$	5	$2^{-1.00}$	46	$2^{-6.54}$	$2^{-7.54}$
$K[5]$	6	$2^{-2.00}$	45	$2^{-1.58}$	$2^{-3.58}$
$K[6]$	7	$2^{-3.00}$	48	$2^{-4.09}$	$2^{-7.09}$
$K[7]$	8	$2^{-2.00}$	47	$2^{-7.34}$	$2^{-9.34}$
all	1-8	$2^{-43.68}$	43-50	$2^{-64.84}$	$2^{-108.52}$

- Time: $+2^{103.67} \rightarrow 2^{104.74}$
- Trail-keys: $\times 2^{-7.72} \rightarrow 2^{95.95}$

Guessing Illustration (2/2)

Master key word	Round	Filter	Round	Filter	Total
$K[0]$	1	$2^{-11.87}$	49	$2^{-10.34}$	$2^{-22.21}$
$K[1]$	2	$2^{-11.91}$	50	$2^{-10.06}$	$2^{-21.97}$
$K[2]$	3	$2^{-7.72}$	51	$2^{-12.62}$	$2^{-20.34}$
$K[3]$	4	$2^{-4.17}$	52	$2^{-12.27}$	$2^{-16.44}$
$K[4]$	5	$2^{-1.00}$	46	$2^{-6.54}$	$2^{-7.54}$
$K[5]$	6	$2^{-2.00}$	45	$2^{-1.58}$	$2^{-3.58}$
$K[6]$	7	$2^{-3.00}$	48	$2^{-4.09}$	$2^{-7.09}$
$K[7]$	8	$2^{-2.00}$	47	$2^{-7.34}$	$2^{-9.34}$
all	1-8	$2^{-43.68}$	43-50	$2^{-64.84}$	$2^{-108.52}$

- Time: $+2^{100.04} \rightarrow 2^{104.79}$
- Trail-keys: $\times 2^{4.09} \rightarrow 2^{100.04}$

Guessing Illustration (2/2)

Master key word	Round	Filter	Round	Filter	Total
$K[0]$	1	$2^{-11.87}$	49	$2^{-10.34}$	$2^{-22.21}$
$K[1]$	2	$2^{-11.91}$	50	$2^{-10.06}$	$2^{-21.97}$
$K[2]$	3	$2^{-7.72}$	51	$2^{-12.62}$	$2^{-20.34}$
$K[3]$	4	$2^{-4.17}$	52	$2^{-12.27}$	$2^{-16.44}$
$K[4]$	5	$2^{-1.00}$	46	$2^{-6.54}$	$2^{-7.54}$
$K[5]$	6	$2^{-2.00}$	45	$2^{-1.58}$	$2^{-3.58}$
$K[6]$	7	$2^{-3.00}$	48	$2^{-4.09}$	$2^{-7.09}$
$K[7]$	8	$2^{-2.00}$	47	$2^{-7.34}$	$2^{-9.34}$
all	1-8	$2^{-43.68}$	43-50	$2^{-64.84}$	$2^{-108.52}$

- Time: $+2^{100.04} \to 2^{104.84}$
- Trail-keys: $\times 2^{-10.06} \to 2^{89.98}$

Guessing Illustration (2/2)

Master key word	Round	Filter	Round	Filter	Total
$K[0]$	1	$2^{-11.87}$	49	$2^{-10.34}$	$2^{-22.21}$
$K[1]$	2	$2^{-11.91}$	50	$2^{-10.06}$	$2^{-21.97}$
$K[2]$	3	$2^{-7.72}$	51	$2^{-12.62}$	$2^{-20.34}$
$K[3]$	4	$2^{-4.17}$	52	$2^{-12.27}$	$2^{-16.44}$
$K[4]$	5	$2^{-1.00}$	46	$2^{-6.54}$	$2^{-7.54}$
$K[5]$	6	$2^{-2.00}$	45	$2^{-1.58}$	$2^{-3.58}$
$K[6]$	7	$2^{-3.00}$	48	$2^{-4.09}$	$2^{-7.09}$
$K[7]$	8	$2^{-2.00}$	47	$2^{-7.34}$	$2^{-9.34}$
all	1-8	$2^{-43.68}$	43-50	$2^{-64.84}$	$2^{-108.52}$

- Time: $+2^{94.11} \rightarrow 2^{104.85}$
- Trail-keys: $\times 2^{4.13} \rightarrow 2^{94.11}$

Guessing Illustration (2/2)

Master key word	Round	Filter	Round	Filter	Total
$K[0]$	1	$2^{-11.87}$	49	$2^{-10.34}$	$2^{-22.21}$
$K[1]$	2	$2^{-11.91}$	50	$2^{-10.06}$	$2^{-21.97}$
$K[2]$	3	$2^{-7.72}$	51	$2^{-12.62}$	$2^{-20.34}$
$K[3]$	4	$2^{-4.17}$	52	$2^{-12.27}$	$2^{-16.44}$
$K[4]$	5	$2^{-1.00}$	46	$2^{-6.54}$	$2^{-7.54}$
$K[5]$	6	$2^{-2.00}$	45	$2^{-1.58}$	$2^{-3.58}$
$K[6]$	7	$2^{-3.00}$	48	$2^{-4.09}$	$2^{-7.09}$
$K[7]$	8	$2^{-2.00}$	47	$2^{-7.34}$	$2^{-9.34}$
all	1-8	$2^{-43.68}$	43-50	$2^{-64.84}$	$2^{-108.52}$

- Time: $+2^{94.11} \to 2^{104.85}$
- Trail-keys: $\times 2^{-10.34} \to 2^{83.77}$

Guessing Illustration (2/2)

Master key word	Round	Filter	Round	Filter	Total
$K[0]$	1	$2^{-11.87}$	49	$2^{-10.34}$	$2^{-22.21}$
$K[1]$	2	$2^{-11.91}$	50	$2^{-10.06}$	$2^{-21.97}$
$K[2]$	3	$2^{-7.72}$	51	$2^{-12.62}$	$2^{-20.34}$
$K[3]$	4	$2^{-4.17}$	52	$2^{-12.27}$	$2^{-16.44}$
$K[4]$	5	$2^{-1.00}$	46	$2^{-6.54}$	$2^{-7.54}$
$K[5]$	6	$2^{-2.00}$	45	$2^{-1.58}$	$2^{-3.58}$
$K[6]$	7	$2^{-3.00}$	48	$2^{-4.09}$	$2^{-7.09}$
$K[7]$	8	$2^{-2.00}$	47	$2^{-7.34}$	$2^{-9.34}$
all	1-8	$2^{-43.68}$	43-50	$2^{-64.84}$	$2^{-108.52}$

- Time: $+2^{83.77} \rightarrow 2^{104.85}$
- Trail-keys: $\times 2^{-4.17} \rightarrow 2^{79.60}$

Guessing Illustration (2/2)

Master key word	Round	Filter	Round	Filter	Total
$K[0]$	1	$2^{-11.87}$	49	$2^{-10.34}$	$2^{-22.21}$
$K[1]$	2	$2^{-11.91}$	50	$2^{-10.06}$	$2^{-21.97}$
$K[2]$	3	$2^{-7.72}$	51	$2^{-12.62}$	$2^{-20.34}$
$K[3]$	4	$2^{-4.17}$	52	$2^{-12.27}$	$2^{-16.44}$
$K[4]$	5	$2^{-1.00}$	46	$2^{-6.54}$	$2^{-7.54}$
$K[5]$	6	$2^{-2.00}$	45	$2^{-1.58}$	$2^{-3.58}$
$K[6]$	7	$2^{-3.00}$	48	$2^{-4.09}$	$2^{-7.09}$
$K[7]$	8	$2^{-2.00}$	47	$2^{-7.34}$	$2^{-9.34}$
all	1-8	$2^{-43.68}$	43-50	$2^{-64.84}$	$2^{-108.52}$

- Time: $+2^{91.51} \rightarrow 2^{104.85}$
- Trail-keys: $\times 2^{11.91} \rightarrow 2^{91.51}$

Guessing Illustration (2/2)

Master key word	Round	Filter	Round	Filter	Total
$K[0]$	1	$2^{-11.87}$	49	$2^{-10.34}$	$2^{-22.21}$
$K[1]$	2	$2^{-11.91}$	50	$2^{-10.06}$	$2^{-21.97}$
$K[2]$	3	$2^{-7.72}$	51	$2^{-12.62}$	$2^{-20.34}$
$K[3]$	4	$2^{-4.17}$	52	$2^{-12.27}$	$2^{-16.44}$
$K[4]$	5	$2^{-1.00}$	46	$2^{-6.54}$	$2^{-7.54}$
$K[5]$	6	$2^{-2.00}$	45	$2^{-1.58}$	$2^{-3.58}$
$K[6]$	7	$2^{-3.00}$	48	$2^{-4.09}$	$2^{-7.09}$
$K[7]$	8	$2^{-2.00}$	47	$2^{-7.34}$	$2^{-9.34}$
all	1-8	$2^{-43.68}$	43-50	$2^{-64.84}$	$2^{-108.52}$

- Time: $+2^{91.51} \rightarrow 2^{104.85}$
- Trail-keys: $\times 2^{-3.00} \rightarrow 2^{88.51}$

Guessing Illustration (2/2)

Master key word	Round	Filter	Round	Filter	Total
$K[0]$	1	$2^{-11.87}$	49	$2^{-10.34}$	$2^{-22.21}$
$K[1]$	2	$2^{-11.91}$	50	$2^{-10.06}$	$2^{-21.97}$
$K[2]$	3	$2^{-7.72}$	51	$2^{-12.62}$	$2^{-20.34}$
$K[3]$	4	$2^{-4.17}$	52	$2^{-12.27}$	$2^{-16.44}$
$K[4]$	5	$2^{-1.00}$	46	$2^{-6.54}$	$2^{-7.54}$
$K[5]$	6	$2^{-2.00}$	45	$2^{-1.58}$	$2^{-3.58}$
$K[6]$	7	$2^{-3.00}$	48	$2^{-4.09}$	$2^{-7.09}$
$K[7]$	8	$2^{-2.00}$	47	$2^{-7.34}$	$2^{-9.34}$
all	1-8	$2^{-43.68}$	43-50	$2^{-64.84}$	$2^{-108.52}$

- Time:
  $+2^{97.17} \to 2^{104.85}$
- Trail-keys:
  $\times 2^{8.66} \to 2^{97.17}$

Guessing Illustration (2/2)

Master key word	Round	Filter	Round	Filter	Total
$K[0]$	1	$2^{-11.87}$	49	$2^{-10.34}$	$2^{-22.21}$
$K[1]$	2	$2^{-11.91}$	50	$2^{-10.06}$	$2^{-21.97}$
$K[2]$	3	$2^{-7.72}$	51	$2^{-12.62}$	$2^{-20.34}$
$K[3]$	4	$2^{-4.17}$	52	$2^{-12.27}$	$2^{-16.44}$
$K[4]$	5	$2^{-1.00}$	46	$2^{-6.54}$	$2^{-7.54}$
$K[5]$	6	$2^{-2.00}$	45	$2^{-1.58}$	$2^{-3.58}$
$K[6]$	7	$2^{-3.00}$	48	$2^{-4.09}$	$2^{-7.09}$
$K[7]$	8	$2^{-2.00}$	47	$2^{-7.34}$	$2^{-9.34}$
all	1-8	$2^{-43.68}$	43-50	$2^{-64.84}$	$2^{-108.52}$

- Time: $+2^{106.63} \rightarrow 2^{107.00}$
- Trail-keys: $\times 2^{9.46} \rightarrow 2^{106.63}$

Guessing Illustration (2/2)

Master key word	Round	Filter	Round	Filter	Total
$K[0]$	1	$2^{-11.87}$	49	$2^{-10.34}$	$2^{-22.21}$
$K[1]$	2	$2^{-11.91}$	50	$2^{-10.06}$	$2^{-21.97}$
$K[2]$	3	$2^{-7.72}$	51	$2^{-12.62}$	$2^{-20.34}$
$K[3]$	4	$2^{-4.17}$	52	$2^{-12.27}$	$2^{-16.44}$
$K[4]$	5	$2^{-1.00}$	46	$2^{-6.54}$	$2^{-7.54}$
$K[5]$	6	$2^{-2.00}$	45	$2^{-1.58}$	$2^{-3.58}$
$K[6]$	7	$2^{-3.00}$	48	$2^{-4.09}$	$2^{-7.09}$
$K[7]$	8	$2^{-2.00}$	47	$2^{-7.34}$	$2^{-9.34}$
all	1-8	$2^{-43.68}$	43-50	$2^{-64.84}$	$2^{-108.52}$

- Time: $+2^{106.63} \rightarrow 2^{107.83}$
- Trail-keys: $\times 2^{-1.00} \rightarrow 2^{105.63}$

Guessing Illustration (2/2)

Master key word	Round	Filter	Round	Filter	Total
$K[0]$	1	$2^{-11.87}$	49	$2^{-10.34}$	$2^{-22.21}$
$K[1]$	2	$2^{-11.91}$	50	$2^{-10.06}$	$2^{-21.97}$
$K[2]$	3	$2^{-7.72}$	51	$2^{-12.62}$	$2^{-20.34}$
$K[3]$	4	$2^{-4.17}$	52	$2^{-12.27}$	$2^{-16.44}$
$K[4]$	5	$2^{-1.00}$	46	$2^{-6.54}$	$2^{-7.54}$
$K[5]$	6	$2^{-2.00}$	45	$2^{-1.58}$	$2^{-3.58}$
$K[6]$	7	$2^{-3.00}$	48	$2^{-4.09}$	$2^{-7.09}$
$K[7]$	8	$2^{-2.00}$	47	$2^{-7.34}$	$2^{-9.34}$
all	1-8	$2^{-43.68}$	43-50	$2^{-64.84}$	$2^{-108.52}$

- Time: $+2^{105.63} \rightarrow 2^{108.11}$
- Trail-keys: $\times 2^{-2.00} \rightarrow 2^{103.63}$

Guessing Illustration (2/2)

Master key word	Round	Filter	Round	Filter	Total
$K[0]$	1	$2^{-11.87}$	49	$2^{-10.34}$	$2^{-22.21}$
$K[1]$	2	$2^{-11.91}$	50	$2^{-10.06}$	$2^{-21.97}$
$K[2]$	3	$2^{-7.72}$	51	$2^{-12.62}$	$2^{-20.34}$
$K[3]$	4	$2^{-4.17}$	52	$2^{-12.27}$	$2^{-16.44}$
$K[4]$	5	$2^{-1.00}$	46	$2^{-6.54}$	$2^{-7.54}$
$K[5]$	6	$2^{-2.00}$	45	$2^{-1.58}$	$2^{-3.58}$
$K[6]$	7	$2^{-3.00}$	48	$2^{-4.09}$	$2^{-7.09}$
$K[7]$	8	$2^{-2.00}$	47	$2^{-7.34}$	$2^{-9.34}$
all	1-8	$2^{-43.68}$	43-50	$2^{-64.84}$	$2^{-108.52}$

- Time: $+2^{117.63} \rightarrow 2^{117.63}$
- Trail-keys: $\times 2^{14.00} \rightarrow 2^{117.63}$

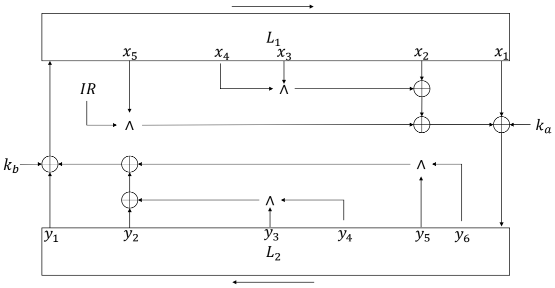
Guessing Illustration (2/2)

Master key word	Round	Filter	Round	Filter	Total
$K[0]$	1	$2^{-11.87}$	49	$2^{-10.34}$	$2^{-22.21}$
$K[1]$	2	$2^{-11.91}$	50	$2^{-10.06}$	$2^{-21.97}$
$K[2]$	3	$2^{-7.72}$	51	$2^{-12.62}$	$2^{-20.34}$
$K[3]$	4	$2^{-4.17}$	52	$2^{-12.27}$	$2^{-16.44}$
$K[4]$	5	$2^{-1.00}$	46	$2^{-6.54}$	$2^{-7.54}$
$K[5]$	6	$2^{-2.00}$	45	$2^{-1.58}$	$2^{-3.58}$
$K[6]$	7	$2^{-3.00}$	48	$2^{-4.09}$	$2^{-7.09}$
$K[7]$	8	$2^{-2.00}$	47	$2^{-7.34}$	$2^{-9.34}$
all	1-8	$2^{-43.68}$	43-50	$2^{-64.84}$	$2^{-108.52}$

- Time: $+2^{117.63} \rightarrow 2^{118.63}$
- Trail-keys: $\times 2^{-1.58} \rightarrow 2^{116.05}$

Plan

KATAN cipher



b	$\lvert L_1 \rvert$	$\lvert L_2 \rvert$	x_1	x_2	x_3	x_4	x_5	y_1	y_2	y_3	y_4	y_5	y_6
32	13	19	12	7	8	5	3	18	7	12	10	8	3
48	19	29	18	12	15	7	6	28	19	21	13	15	6
64	25	39	24	15	20	11	9	38	25	33	21	14	9

- Based on nonlinear feedback shift registers (NLFSR): KATAN-32/48/64
  1. 80-bit key
  2. 254 rounds
  3. Variants differ in register sizes and location of *taps*
- Linear key schedule

Attacks Summary and Comparison

Cipher	Rounds	Type	Time	Data	Ref
KATAN-32	117	SK Rectangle	$2^{79.3}$	$2^{27.3}$	(Chen, Teh, Liu, Su, Samsudin, and Xiang 20
	123	SK Diff.	$2^{75.80}$	2^{31}	This Paper
	187	RK Rectangle	$2^{78.4}$	$2^{31.8}$	(Chen, Teh, Liu, Su, Samsudin, and Xiang 20
	206	SK Multi-dim. MitM	2^{79}	3	(Rasoolzadeh and Raddum 2016)
KATAN-48	87	SK Rectangle	2^{78}	$2^{36.7}$	(Chen, Teh, Liu, Su, Samsudin, and Xiang 20
	130	SK Diff.	$2^{73.56}$	2^{45}	This Paper
	150	RK Rectangle	$2^{77.6}$	$2^{47.2}$	(Chen, Teh, Liu, Su, Samsudin, and Xiang 20
	148	SK Multi-dim. MitM	2^{79}	2	(Rasoolzadeh and Raddum 2016)
KATAN-64	72	SK Rectangle	2^{78}	$2^{55.1}$	(Chen, Teh, Liu, Su, Samsudin, and Xiang 20
	109	SK Diff.	$2^{73.65}$	2^{57}	This Paper
	133	RK Rectangle	$2^{78.5}$	$2^{58.4}$	(Chen, Teh, Liu, Su, Samsudin, and Xiang 20
	129	SK Multi-dim. MitM	2^{79}	2	(Rasoolzadeh and Raddum 2016)

Attacks Summary

- $\approx$ direct MiF application
- no plaintext structure (but free rounds)
- using multiple output differences to reduce data

Attacks Summary

- $\approx$ direct MiF application
- no plaintext structure (but free rounds)
- using multiple output differences to reduce data

Version	Subkey bits /round	Steps /round	Avg.Prob. (random)	Total Factor /round
KATAN-32	2	1	$2^{-1.76}$	$\times 2^{+0.24}$
KATAN-48	2	2	$2^{-3.52}$	$\times 2^{-1.52}$
KATAN-64	2	3	$2^{-5.28}$	$\times 2^{-3.28}$

Attacks Summary

- ≈ direct MiF application
- no plaintext structure (but free rounds)
- using multiple output differences to reduce data

Version	Subkey bits /round	Steps /round	Avg.Prob. (random)	Total Factor /round
KATAN-32	2	1	$2^{-1.76}$	$\times 2^{+0.24}$
KATAN-48	2	2	$2^{-3.52}$	$\times 2^{-1.52}$
KATAN-64	2	3	$2^{-5.28}$	$\times 2^{-3.28}$

- ⇒ better to directly guess "negative" rounds' subkeys
and decrypt ciphertexts before running MiF (2 subkey bits / round)

Plan

Conclusions

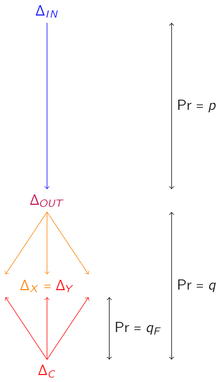
This work:

- simplified analysis of Meet-in-the-Filter (pen-and-paper)
- tools for analysis of trail distributions
- combining MiF with plaintext structures
- example applications: attacks on CHAM and KATAN

github.com/aa8a7b82/mif   ia.cr/2022/xxxx

Open problems:

- similar simplified theory for dynamic counting
- more applications



References I

Albrecht, Martin R. and Gregor Leander (2012). "An All-In-One Approach to Differential Cryptanalysis for Small Block Ciphers". In: *Selected Areas in Cryptography*. Vol. 7707. Lecture Notes in Computer Science. Springer, pp. 1–15.

Biham, Eli and Adi Shamir (1993). *Differential Cryptanalysis of the Data Encryption Standard*. Berlin, Heidelberg: Springer-Verlag. ISBN: 0387979301.

Biryukov, Alex, Luan Cardoso dos Santos, Je Sen Teh, Aleksei Udovenko, and Vesselin Velichkov (2022). *Meet-in-the-Filter and Dynamic Counting with Applications to Speck*. Cryptology ePrint Archive, Paper 2022/673. https://eprint.iacr.org/2022/673.

Chen, Jiageng, Jesen Teh, Zhe Liu, Chunhua Su, Azman Samsudin, and Yang Xiang (2017). "Towards Accurate Statistical Analysis of Security Margins: New Searching Strategies for Differential Attacks". In: *IEEE Trans. Computers* 66.10, pp. 1763–1777.

References II

Dinur, Itai (Aug. 2014). "Improved Differential Cryptanalysis of Round-Reduced Speck". In: *SAC 2014*. Ed. by Antoine Joux and Amr M. Youssef. Vol. 8781. LNCS. Springer, Heidelberg, pp. 147–164. DOI: 10.1007/978-3-319-13051-4_9.

Huang, Mingjiang and Liming Wang (2019). "Automatic Tool for Searching for Differential Characteristics in ARX Ciphers and Applications". In: *INDOCRYPT 2019*. Vol. 11898. LNCS. Springer, pp. 115–138.

Isobe, Takanori, Yu Sasaki, and Jiageng Chen (2013). "Related-Key Boomerang Attacks on KATAN32/48/64". In: *ACISP*. Vol. 7959. Lecture Notes in Computer Science. Springer, pp. 268–285.

Knellwolf, Simon, Willi Meier, and María Naya-Plasencia (2010). "Conditional Differential Cryptanalysis of NLFSR-Based Cryptosystems". In: *ASIACRYPT*. Vol. 6477. Lecture Notes in Computer Science. Springer, pp. 130–145.

References III

Knellwolf, Simon, Willi Meier, and María Naya-Plasencia (2011). "Conditional Differential Cryptanalysis of Trivium and KATAN". In: *Selected Areas in Cryptography*. Vol. 7118. Lecture Notes in Computer Science. Springer, pp. 200–212.

Rasoolzadeh, Shahram and Håvard Raddum (2016). "Multidimensional Meet in the Middle Cryptanalysis of KATAN". In: *IACR Cryptol. ePrint Arch.*, p. 77.

Rechberger, Christian, Hadi Soleimany, and Tyge Tiessen (2018). "Cryptanalysis of Low-Data Instances of Full LowMCv2". In: *IACR Trans. Symm. Cryptol.* 2018.3, pp. 163–181. ISSN: 2519-173X. DOI: 10.13154/tosc.v2018.i3.163-181.

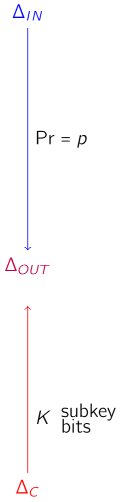
Roh, Dongyoung, Bonwook Koo, Younghoon Jung, Ilwoong Jeong, Donggeon Lee, Daesung Kwon, and Woo-Hwan Kim (2019). "Revised Version of Block Cipher CHAM". In: *ICISC*. Vol. 11975. Lecture Notes in Computer Science. Springer, pp. 1–19.

References IV

Xing, Zhaohui, Wenying Zhang, and Guoyong Han (2020). "Improved Conditional Differential Analysis on NLFSR-Based Block Cipher KATAN32 with MILP". In: *Wirel. Commun. Mob. Comput.* 2020, 8883557:1–8883557:14.

Signal/Noise Ratio (Biham and Shamir 1993)

- When is the differential attack meaningful?

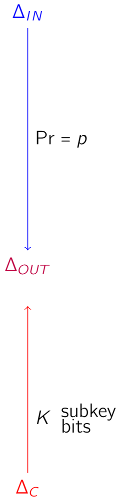


Signal/Noise Ratio (Biham and Shamir 1993)

- When is the differential attack meaningful?
- Signal/Noise ratio:

$$S/N = \frac{2^K p}{w}, \qquad \begin{aligned} p &= \Pr[\Delta_{IN} \to \Delta_{OUT}] \text{ (main differential)} \\ K &= \text{guessed subkeys size} \\ w &= \text{avg \# subkey candidates / pair} \end{aligned}$$

- Faster than K-bit exhaustive search by a factor (S/N)



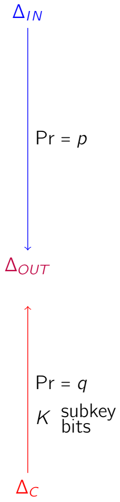
Signal/Noise Ratio (Biham and Shamir 1993)

- When is the differential attack meaningful?
- Signal/Noise ratio:

$$S/N = \frac{2^K p}{w}, \qquad \begin{aligned} p &= \Pr[\Delta_{IN} \to \Delta_{OUT}] \text{ (main differential)} \\ K &= \text{guessed subkeys size} \\ w &= \text{avg \# subkey candidates / pair} \end{aligned}$$

- Faster than K-bit exhaustive search by a factor (S/N)
- Consider observed difference Δ_C:

$$w = 2^K q, \text{ where } q = \Pr[\Delta_{OUT} \to \Delta_C] \quad \text{(MiF trail)}$$



Signal/Noise Ratio (Biham and Shamir 1993)

- When is the differential attack meaningful?
- Signal/Noise ratio:

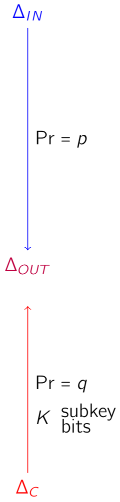
$$S/N = \frac{2^K p}{w},$$

$p = \Pr[\Delta_{IN} \to \Delta_{OUT}]$ (main differential)
$K =$ guessed subkeys size
$w =$ avg # subkey candidates / pair

- Faster than K-bit exhaustive search by a factor (S/N)
- Consider observed difference Δ_C:

$$w = 2^K q, \text{ where } q = \Pr[\Delta_{OUT} \to \Delta_C] \quad \text{(MiF trail)}$$

- Conclude $S/N = \frac{p}{q}$



Signal/Noise Ratio (Biham and Shamir 1993)

- When is the differential attack meaningful?
- Signal/Noise ratio:

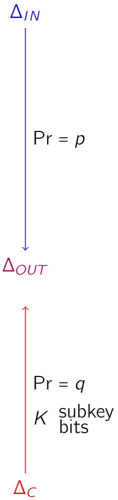
$$S/N = \frac{2^K p}{w},$$

$p = \Pr[\Delta_{IN} \to \Delta_{OUT}]$ (main differential)
$K =$ guessed subkeys size
$w =$ avg # subkey candidates / pair

- Faster than K-bit exhaustive search by a factor (S/N)
- Consider observed difference Δ_C:

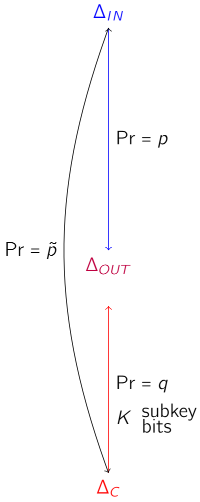
$$w = 2^K q, \text{ where } q = \Pr[\Delta_{OUT} \to \Delta_C] \quad \text{(MiF trail)}$$

- ~~Conclude $S/N = \frac{p}{q}$~~ INCORRECT



Gain

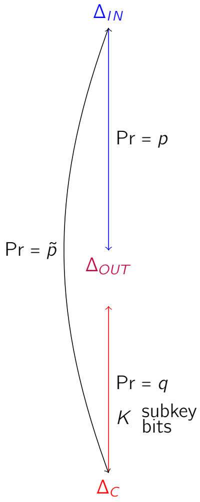
- define **gain** $g = \frac{\Pr[\text{a suggested key is the right one}]}{\Pr[\text{a random key is the right one}]}$



Gain

- define **gain** $g = \frac{\Pr[\text{a suggested key is the right one}]}{\Pr[\text{a random key is the right one}]}$

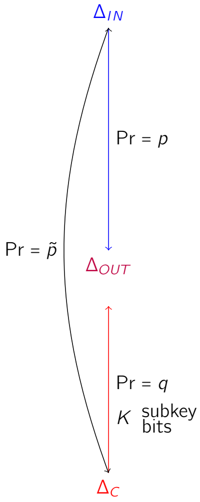
- we show that $g = \frac{p}{\tilde{p}} = \frac{\Pr[\Delta_{IN} \to \Delta_{OUT}]}{\Pr[\Delta_{IN} \to \Delta_{C}]} = S/N \cdot \frac{q}{\tilde{p}}$



Gain

- define **gain** $g = \dfrac{\Pr[\text{a suggested key is the right one}]}{\Pr[\text{a random key is the right one}]}$

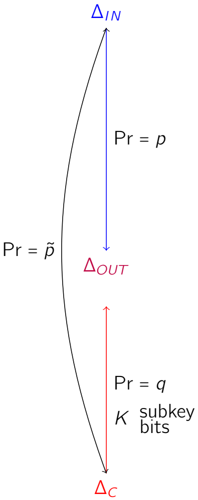
- we show that $g = \dfrac{p}{\tilde{p}} = \dfrac{\Pr[\Delta_{IN} \to \Delta_{OUT}]}{\Pr[\Delta_{IN} \to \Delta_C]} = S/N \cdot \dfrac{q}{\tilde{p}}$



Gain

- define **gain** $g = \frac{\text{Pr[a suggested key is the right one]}}{\text{Pr[a random key is the right one]}}$
- we show that $g = \frac{p}{\tilde{p}} = \frac{\Pr[\Delta_{IN} \to \Delta_{OUT}]}{\Pr[\Delta_{IN} \to \Delta_C]} = S/N \cdot \frac{q}{\tilde{p}}$
- ciphertext-randomization hypothesis:

$$\tilde{p} = 2^{-|C|} \quad \Rightarrow \quad g = 2^{|C|} p$$



Gain

- define **gain** $g = \frac{\Pr[\text{a suggested key is the right one}]}{\Pr[\text{a random key is the right one}]}$
- we show that $g = \frac{p}{\tilde{p}} = \frac{\Pr[\Delta_{IN} \rightarrow \Delta_{OUT}]}{\Pr[\Delta_{IN} \rightarrow \Delta_{C}]} = S/N \cdot \frac{q}{\tilde{p}}$
- ciphertext-randomization hypothesis:

$$\tilde{p} = 2^{-|C|} \quad \Rightarrow \quad g = 2^{|C|} p$$

- (general limit of differential key recovery)