Differential Fault Analysis on Minalpher

Avik Chakraborti, Mridul Nandi

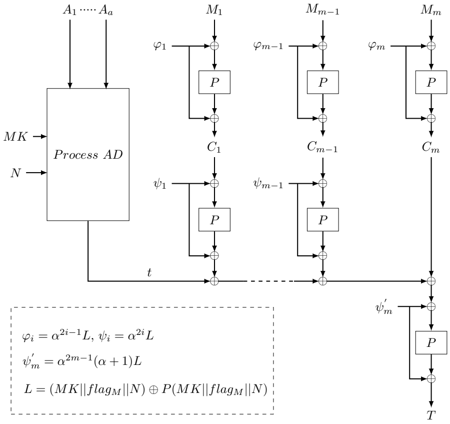
September 28, 2015

Outline of the talk

1. Introduction.
2. Differential Fault Analysis on Minalpher with a Single Random Fault
3. Differential Fault Analysis on Minalpher with Two Random Faults
4. Attack Complexities
5. Conclusions and Future Works

1. Introduction
2. DFA with a Single Random Fault
3. DFA with Two Random Faults
4. Attack Complexities
5. Conclusions and Future Works

Minalpher AE Scheme



- AEAD - Enc : $(M, K, N, A) \mapsto (C, T)$
  - AEAD - CGen : $(M, K, N, A) \mapsto C$
  - AEAD - TGen : $(C, K, N, A) \mapsto T$

- P - SPN structure.

- $MK \rightarrow L \rightarrow \varphi_i, \psi_i, \psi'_m$

P Permutation

- 256-bit input and 256-bit output (Two 128-bit state A and B)
- 17.5 round functions
- Each Round - $SN(S) \rightarrow SR(T) \rightarrow MC(M)$
- Last Round - $SN(S) \rightarrow SR(T)$

S Function

- $(A_{in}||B_{in}) \mapsto (A_{out}||B_{out})$

- Replaces x by $s(x)$, $\forall$ 4-bit nibbles x in $(A_{in}||B_{in})$

Table : s Function

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
s(x)	B	3	4	1	2	8	C	F	5	D	E	0	6	9	A	7

T Function

- $(A_{in}||B_{in}) \mapsto (A_{out}||B_{out})$

- $A_{out} = SR^2(B^{in}),\ B^{out} = SR^1(A^{in}) \oplus SR^2(B^{in})$

0,0	0,1	0,2	0,3	0,4	0,5	0,6	0,7
1,0	1,1	1,2	1,3	1,4	1,5	1,6	1,7
2,0	2,1	2,2	2,3	2,4	2,5	2,6	2,7
3,0	3,1	3,2	3,3	3,4	3,5	3,6	3,7

$\downarrow SR^1$

0,6	0,7	0,1	0,0	0,2	0,3	0,4	0,5
1,4	1,5	1,0	1,1	1,7	1,6	1,2	1,3
2,3	2,2	2,4	2,5	2,6	2,7	2,0	2,1
3,2	3,3	3,6	3,7	3,0	3,1	3,5	3,4

0,0	0,1	0,2	0,3	0,4	0,5	0,6	0,7
1,0	1,1	1,2	1,3	1,4	1,5	1,6	1,7
2,0	2,1	2,2	2,3	2,4	2,5	2,6	2,7
3,0	3,1	3,2	3,3	3,4	3,5	3,6	3,7

$\downarrow SR^2$

0,3	0,2	0,4	0,5	0,6	0,7	0,0	0,1
1,2	1,3	1,6	1,7	1,0	1,1	1,5	1,4
2,6	2,7	2,1	2,0	2,2	2,3	2,4	2,5
3,4	3,5	3,0	3,1	3,7	3,6	3,2	3,3

Figure : SR^1 AND SR^2

M Function

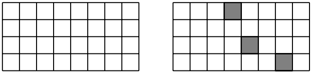
- $(A_{in}||B_{in}) \mapsto (A_{out}||B_{out})$

- Multiplies each columns of $(A_{in}||B_{in})$ by M

$$M = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

Single Fault Injection Position

$A^{16,S}$



$B^{16,S}$

Figure : Fault Positions

- $A^{i,op}$, $B^{i,op}$: A and B after op operation at the i^{th} round.
- Optimized Random fault (gray nibbles) after S (16^{th} round)
- 1 enc query + 1 faulty enc query

Fault Propagation

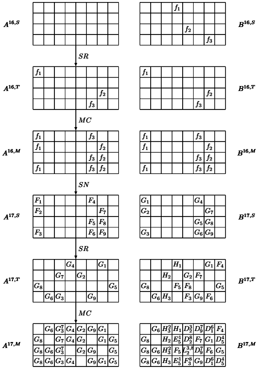


Figure : Fault Propagation

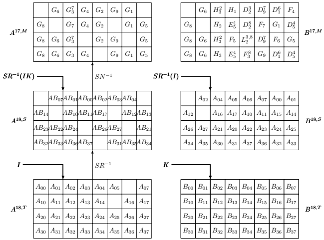


Figure : Backward Key Propagation

- $A \oplus B \rightarrow AB$, $I \oplus K \rightarrow IK$

Form First Set of 30 Eqns

$B^{17,M}$

	G_6	H_3^2	H_1	D_2^3	D_9^7	D_1^6	F_4
G_8		H_2	E_5^1	D_2^8	F_7	G_1	D_5^4
G_8	G_6	H_3^2	F_5	$L_2^{3,8}$	D_9^7	F_6	G_5
G_8	G_6	H_3	E_5^1	F_3^8	G_9	D_1^6	D_5^4

- Each equation corresponds to an active nibble in $B^{17,M}$

- Filter out invalid I values

- Time comp : 2^{12}, Reduced key space for I : $2^{128} \rightarrow 2^{68}$

Form Second Set of 25 Eqns

$A^{17,M}$

	G_6	G_3^7	G_4	G_2	G_9	G_1	
G_8		G_7	G_4	G_2		G_1	G_5
G_8	G_6	G_3^7		G_2	G_9		G_5
G_8	G_6	G_3	G_4		G_9	G_1	G_5

- Each equation corresponds to an active nibble in $A^{17,M}$
- Filter out invalid $IK = I \oplus K$ values
- Time comp : 2^8, Reduced key space for IK : $2^{128} \rightarrow 2^{64}$

Form Third Set of 9 Eqns

$B^{16,M}$

f_1					f_3		
f_1						f_2	
					f_3	f_2	
f_1					f_3	f_2	

- Each equation corresponds to an active nibble in $B^{16,M}$
- Further filter out invalid IK values
- Time comp : 2^8, Reduced key space for IK : $2^{64} \rightarrow 2^{40}$

Form Fourth Set of 10 Eqns (By Equalities)

Equality on G_8 difference

$A^{17,M}$

	G_6	G_3^7	G_4	G_2	G_9	G_1	
G_8		G_7	G_4	G_2		G_1	G_5
G_8	G_6	G_3^7		G_2	G_9		G_5
G_8	G_6	G_3	G_4		G_9	G_1	G_5

$B^{17,M}$

	G_6	H_3^2	H_1	D_2^3	D_9^7	D_1^6	F_4
G_8		H_2	E_5^1	D_2^8	F_7	G_1	D_5^4
G_8	G_6	H_3^2	F_5	$L_2^{3,8}$	D_9^7	F_6	G_5
G_8	G_6	H_3	E_5^1	F_3^8	G_9	D_1^6	D_5^4

- Compares between $A^{17,M}$ and $B^{17,M}$
- Filter out joint keyspace for invalid I, IK values
- Time comp : 2^{108}, Reduced key space for (I, IK) : $2^{108} \to 2^{68}$

Form Fifth Set of 9 Eqns

$A^{16,M}$

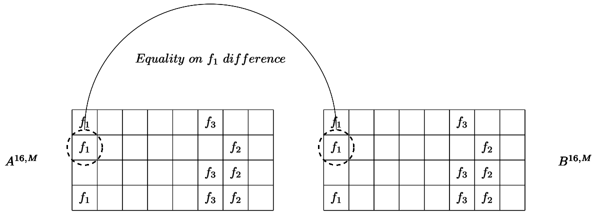
f_1					f_3		
f_1						f_2	
					f_3	f_2	
f_1					f_3	f_2	

- Corresponds to $A^{16,M}$

- Further filter out joint keyspace for invalid I, IK values

- Time comp : 2^{68}, Reduced key space for (I, IK) : $2^{68} \rightarrow 2^{44}$

Form Sixth Set of Eqns (By Equalities)



- Compares between $A^{16,M}$ and $B^{16,M}$
- Further filter out joint keyspace for invalid I, IK values
- Time comp : 2^{44}, Reduced key space for (I, IK) : $2^{44} \rightarrow 2^8$

Finally...

- Compute 2^8, I and K values
- Compute L for each of the 2^8, φ_1 values
- Total Time Complexity : 2^{108}
- Can forge (C, T) for any M and AD but with same N

1. Introduction
2. DFA with a Single Random Fault
3. DFA with Two Random Faults
4. Attack Complexities
5. Conclusions and Future Works

Two Random Fault Injection

- Injects another fault in the same position
- Form two 6 sets of equations parallely
- Filter out more invalid φ_1 values (find unique φ_1)
- compute unique $L = \alpha^{-1}.L$ from φ_1
- Reduces time complexity significantly (From the fourth equation set possible (I, IK) values will be only 2^{16} but not 2^{108})

Attack Complexities

# Faults	Reduced Key Space Size	Time Complexity	# Forging Attempts
1	2^8	2^{108}	2^8
2	1	2^{16}	1

Conclusions and Future Works

- Retrieve *Intermediate Key* (More easily with 2 faults)

- Forge (C, T) pair for *any* M with *any* AD but with *same* N

- Future Work
  - Retrieve *master* key MK from L (W / W.O extra fault) .

Thank you