Nonrandomness of the 33-round MD6

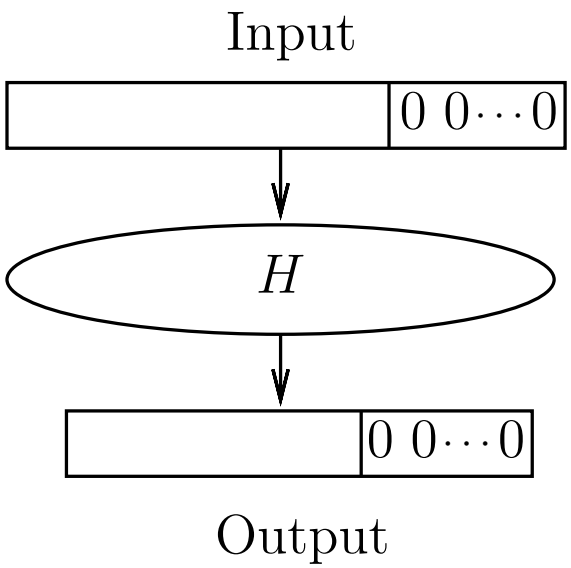
Dmitry Khovratovich

University of Luxembourg

FSE 2009

Differentiability from the random oracle

Fix n bits of input and n bits of output.



- To find a solution for a random oracle one needs 2^n trials;
- For some compression functions we can generate solutions with cost 1.

MD6 compression function

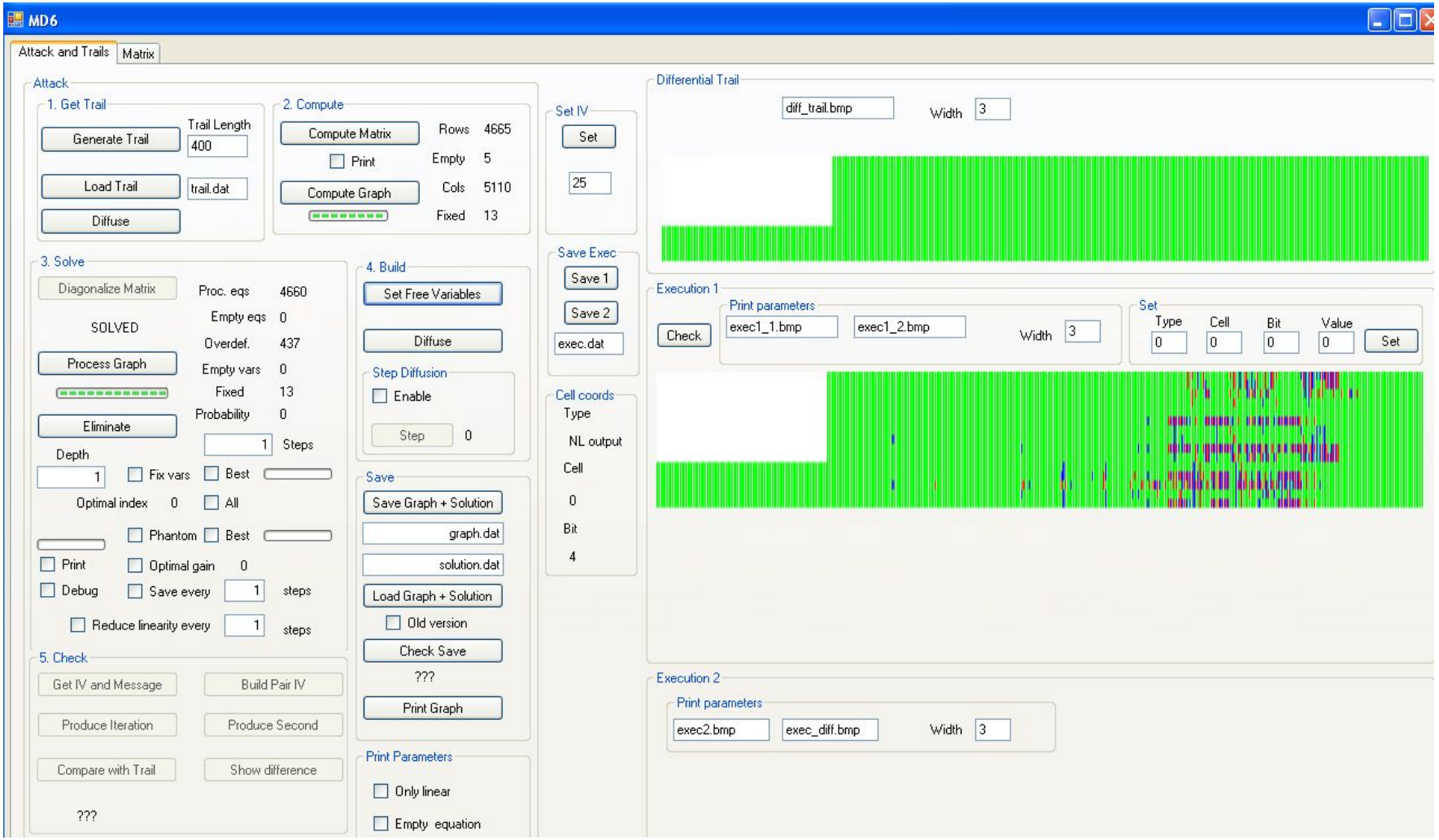
- H: 89 words $\longrightarrow$ 16 words.
- Write down bit equations for the compression function:
  - Nonlinear: $x^j_{i-89} + x^j_{i-31}x^j_{i-67} + x^j_{i-18}x^j_{i-21} + x^j_{i-17} + x^j_i = 0$.
  - 2$\times$ Linear: $y^j_i = x^j_i + x^{j+l_i}_i$.
- $1664 \times 3 \times 64 \approx 300000$ equations for MD6-256.
- Set some variables to constants.
- Solve a system with a Gaussian-like process.
- Generate many solutions.

Results

We fix several bits in the input and the output of the compression function — and show how to derive the others.

Rounds	Fixed bits		Speed	
	input	output	32-bit	64-bit
18	Aumasson et al.		11	5
22	> 9	> 9	14	6
26	6	6	17	7
30	2	2	20	8
32	2	2	21	9
33	1	1	22	9
80	MD6-160		52	22
96	MD6-224		63	26
104	MD6-256		68	28

Tool


MD6
Attack and Trails
Matrix
Attack
1. Get Trail
Generate Trail
Trail Length
400
Load Trail
trail.dat
Diffuse
2. Compute
Compute Matrix
Print
Compute Graph
Rows 4665
Empty 5
Cols 5110
Fixed 13
Set IV
Set
25
Save Exec
Save 1
Save 2
exec.dat
Cell coords
Type
NL output
Cell
0
Bit
4
Differential Trail
diff_trail.bmp
Width 3
Execution 1
Print parameters
Check
exec1_1.bmp
exec1_2.bmp
Width 3
Set
Type Cell Bit Value
0 0 0 0
Set
3. Solve
Diagonalize Matrix
Proc. eqs 4660
SOLVED
Empty eqs 0
Overdef. 437
Process Graph
Empty vars 0
Fixed 13
Probability 0
Eliminate
1 Steps
Depth
1
Fix vars
Best
Optimal index 0
All
Phantom
Best
Print
Optimal gain 0
Debug
Save every 1 steps
Reduce linearity every 1 steps
4. Build
Set Free Variables
Diffuse
Step Diffusion
Enable
Step 0
Save
Save Graph + Solution
graph.dat
solution.dat
Load Graph + Solution
Old version
Check Save
???
Print Graph
Print Parameters
Only linear
Empty equation
5. Check
Get IV and Message
Build Pair IV
Produce Iteration
Produce Second
Compare with Trail
Show difference
???
Execution 2
Print parameters
exec2.bmp
exec_diff.bmp
Width 3