Update on SHA-256

Florian Mendel, Tomislav Nad, Martin Schläffer

florian.mendel@iaik.tugraz.at

Previous Results

- All collisions attacks so far are of practical complexity
- All attacks are based on the same basic idea: extending a local collision to more steps

attack setting	steps	example	reference
collision	18	✓	FSE 2006
	21	✓	FSE 2008
	24	✓	SAC 2008
	24	✓	Indocrypt 2008
	27	✓	Asiacrypt 2011

Finding Differential Characteristics

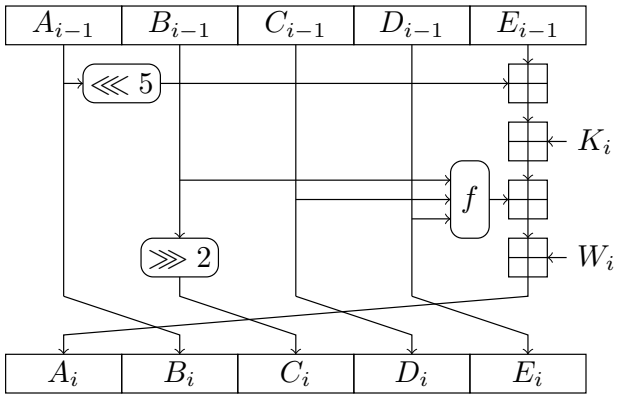
- These characteristics can not be constructed manually
- Use a sophisticated automatic search tool to construct these characteristics
- Extend the approach of De Cannière and Rechberger for SHA-1

(x_i, x_i^*)	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
?	✓	✓	✓	✓
-	✓	-	-	✓
x	-	✓	✓	-
0	✓	-	-	-
u	-	✓	-	-
n	-	-	✓	-
1	-	-	-	✓
#	-	-	-	-

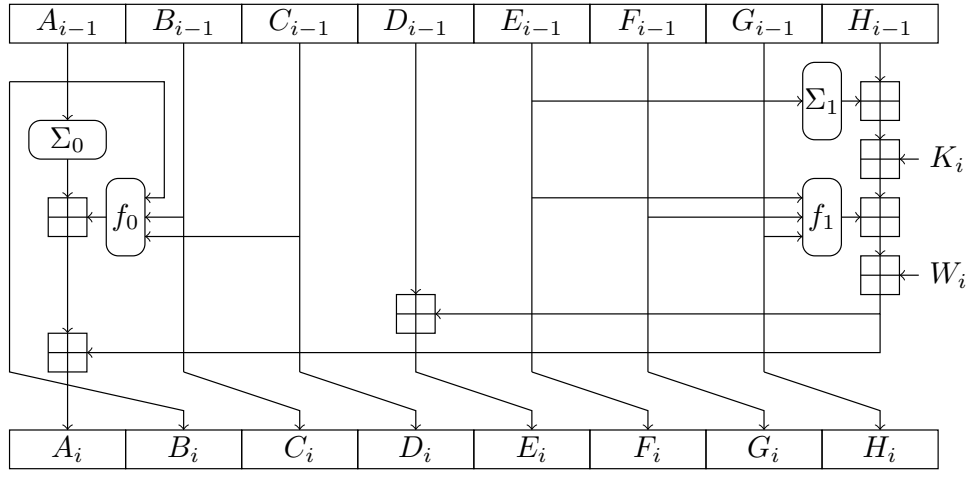
(x_i, x_i^*)	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
3	✓	✓	-	-
5	✓	-	✓	-
7	✓	✓	✓	-
A	-	✓	-	✓
B	✓	✓	-	✓
C	-	-	✓	✓
D	✓	-	✓	✓
E	-	✓	✓	✓

Increased Complexity of SHA-2

SHA-1



SHA-2

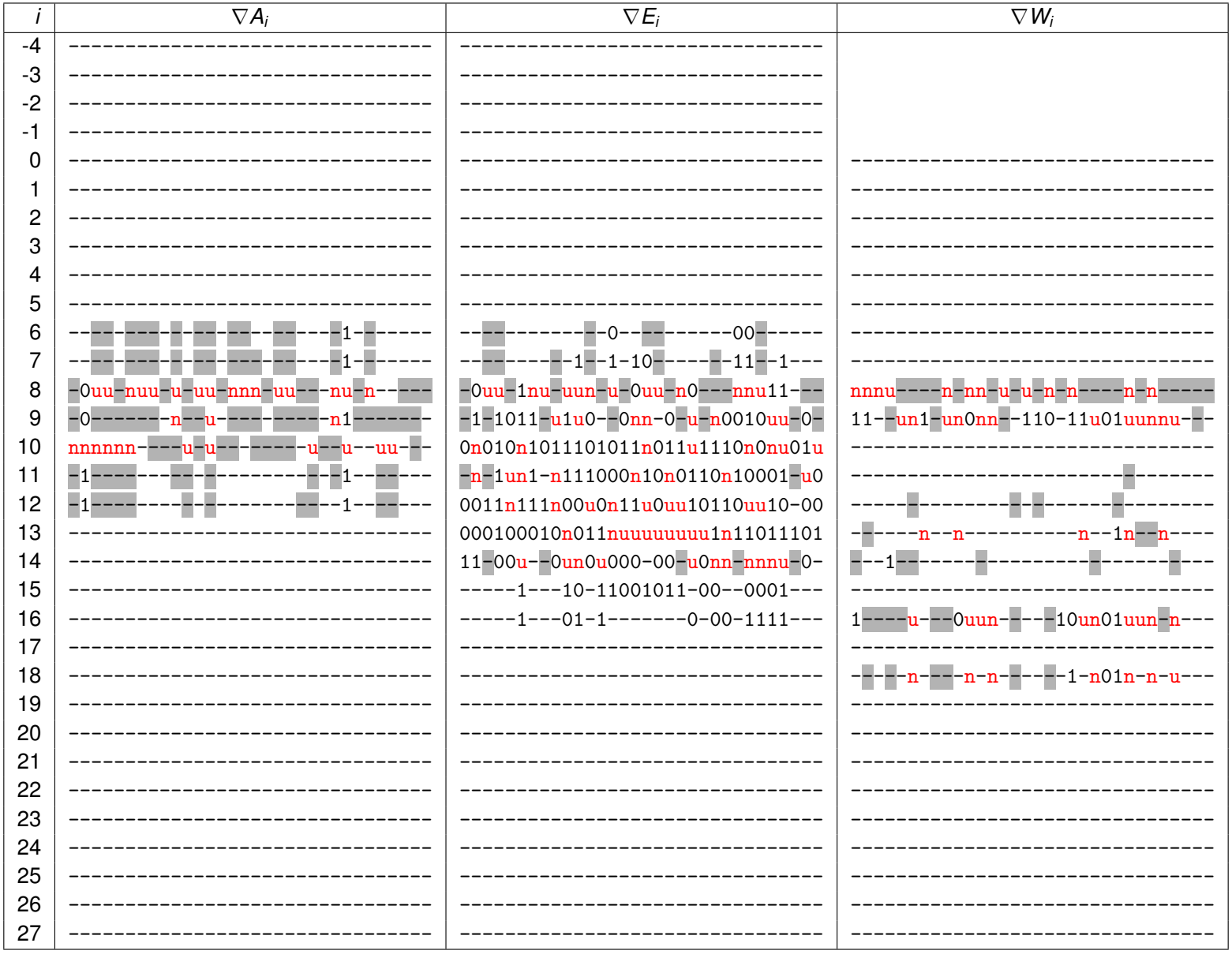


Design Complexity

Improved Results

attack setting	steps	example	reference
collision	18	✓	FSE 2006
	21	✓	FSE 2008
	24	✓	SAC 2008
	24	✓	Indocrypt 2008
	27	✓	Asiacrypt 2011
	28	✓	**new**
	31	–	**new**

Collisions for 28 Steps



Collisions for 28 Steps

h_0	6a09e667	bb67ae85	3c6ef372	a54ff53a
	510e527f	9b05688c	1f83d9ab	5be0cd19
m_0	14c48440	b3c3277f	ad69812d	c3d4dffa
	7eae690b	7f9fe027	832aece8	9a489458
	1607a45c	db81bdc8	8786e031	d8f22801
	72b6be5e	45a2652f	f3fbb17a	2ce70f52
m_0^*	14c48440	b3c3277f	ad69812d	c3d4dffa
	7eae690b	7f9fe027	832aece8	9a489458
	e6b2f4fc	d759b930	8786e031	d8f22801
	72b6be5e	47e26dbf	f3fbb17a	2ce70f52
Δm_0	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000
	f0b550a0	0cd804f8	00000000	00000000
	00000000	02400890	00000000	00000000
h_1	01470131	cd0062bc	7e8f8c21	98938652
	3d49075a	327f38e8	11f0d36d	58601725

What about Collisions for the Compression Function?

attack setting	steps	example	reference
free-start collision	52	–	FSE 2012
semi-free-start collision	23	✓	FSE 2008
	32	✓	Asiacrypt 2011
	38	✓	**new**
collision	18	✓	FSE 2006
	21	✓	FSE 2008
	24	✓	SAC 2008
	24	✓	Indocrypt 2008
	27	✓	Asiacrypt 2011
	28	✓	**new**
	31	–	**new**

Semi-free-start Collision for 38 Steps

h_0	ba75b4ac	c3c9fd45	fce04f3a	6d620fdb
	42559d01	b0a0cd10	729ca9bc	b284a572
m_0	4f5267f8	8f8ec13b	22371c61	56836f2b
	459501d1	8078899e	98947e61	4015ef31
	06e98ffc	4babda4a	27809447	3bf9f3be
	7b3b74e1	065f711d	6c6ead5e	a1781d54
m_0^*	4f5267f8	8f8ec13b	22371c61	56836f2b
	459501d1	8078899e	98947e61	7e73f1f1
	06e99000	4babda4a	277f1447	3bf9f3be
	7b3b74e1	065f711d	6c6ead5e	a1781d50
Δm_0	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	3e661ec0
	00001ffc	00000000	00ff8000	00000000
	00000000	00000000	00000000	00000004
h_1	baa8df17	9f9f64dd	d57d5c2c	7b232c81
	1f3916e6	7a03a2be	7afb1d86	6b0eced6

Discussion

- ARX-based designs are hard to analyze
- Dedicated tools are needed
- Developing these tools take a lot of time
- . . .

Thank you for your attention!