Meet-in-the-Middle Attacks on SHA-3 Candidates

Dmitry Khovratovich, Ivica Nikolić, Ralf-P. Weinmann

University of Luxembourg

Workshop on Fast Software Encryption 2009
Leuven, 2009-02-24

Outline

1. Preimages using meet-in-the-middle techniques
   - Principles
   - Reducing state size
   - Memoryless MITM
2. Attacked functions
   - Boole
   - Edon-R
   - EnRUPT
   - Sarmal

MITM attacks on hash functions

- find preimage $m = m_1||m_2$ for $h = H(m)$ with h fixed
- alternative view: $H(m) = G(F(IV, m_1), m_2)$
- inversion of g for 2nd component fixed: G^{-1}
- idea: compute many values

$$c_i = F(IV, m_{1,i}) \quad \text{and} \quad d_i = G^{-1}(H(m), m_{2,i})$$

and for random $m_{1,i},\ m_{2,i}$ and test for $c_i = d_i$

Reducing the “birthday space”

- trivial: birthday space = state space S
- idea: “cheaply” generate intermediate states such that they are from a smaller subspace $T \subset S$
- “cheaply”: must not be more computationally expensive than computing F or G respectively
- example: words of state fixed to zero

Memoryless MITM

- CRYPTO 1991 paper by Morita, Ohta and Miyaguchi
- idea: use Floyd cycle finding with switching function

$$r : D \rightarrow \{0,1\}$$

- F : function in forward, G : function in backward direction
- define step function:

$$s : D \rightarrow D, \quad x \mapsto \begin{cases} F(x) & \text{if } r(x) = 0 \\ G(x) & \text{if } r(x) = 1 \end{cases}$$

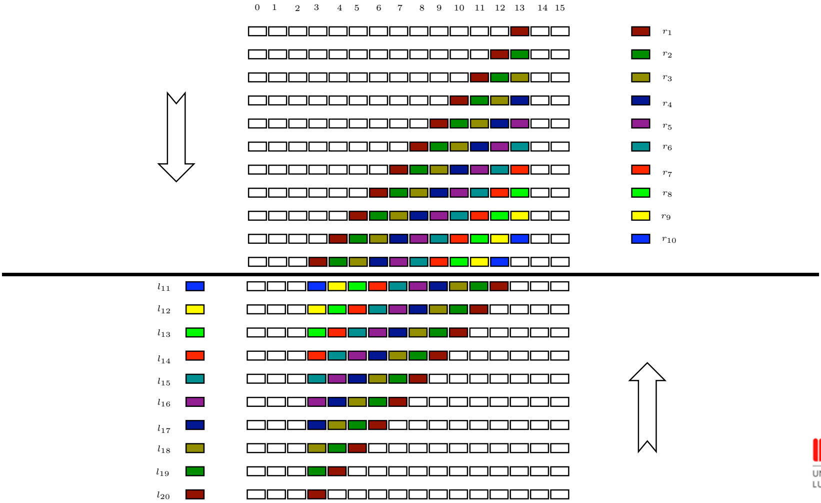
A closer look at memoryless MITM

- when finding cycle in *s*, must check whether MITM or cycle in *F* or *G* occurred
- restart when cycle in *F* or *G* [Pr(restart) = 0.5]
- assumption: output of switching function *r* equi-distributed
- if *G* is relative costly to compute (computationally) compared to *F* or vice versa, *r* not equi-distributed
- a high ratio here kill memoryless MITM

Boole

- attacked function: Boole-384/512 [stream based hash]
- size of internal state: 1216 bits (16 + 3 words)
- birthday space: 576 bits (9 words)
- computational complexity: 2^{288} operations
- memory requirements: 2^{64} blocks
- function *withdrawn* from competition because of attack

Boole MITM


0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
r_1
r_2
r_3
r_4
r_5
r_6
r_7
r_8
r_9
r_{10}
l_{11}
l_{12}
l_{13}
l_{14}
l_{15}
l_{16}
l_{17}
l_{18}
l_{19}
l_{20}

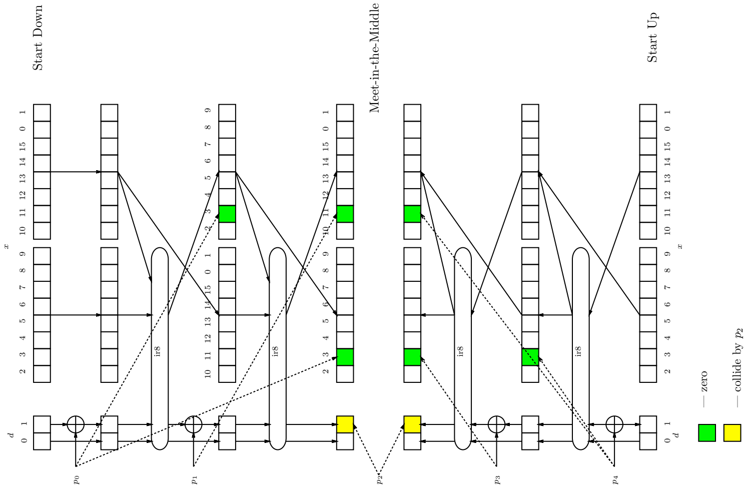
Edon-R

- attacked function: Edon-R-n [Merkle-Damgård]
- size of internal state: $2n$ bits
- computational complexity: $\max(2^{n-s}, 2^{n/2+s})$
- memory requirements: 2^s blocks
- function *not withdrawn*

EnRUPT

- attacked function: EnRUPT-512 [stream based hash]
- size of internal state: 1152 bits
- computational complexity: 2^{480}
- memory requirements: 2^{384} blocks, needs large look-up tables
- Practical collision attack in next talk!

EnRUPT MITM


Start Down
Meet-in-the-Middle
Start Up
x
d
ir8
p0
p1
p2
p3
p4
— zero
— collide by p2

Sarmal

- attacked function: Sarmal-512 [HAIFA design]
- size of internal state: 512 bits (just chaining value)
- computational complexity: $\max(2^{512-s}, 2^{256+s})$
- memory requirements: 2^s blocks
- status: designers consider it a weakness, but not an "attack"

Q & A

Questions?

Q & A

Questions? Please... ?