Attacks against hash functions

CATALDO BASILE

< CATALDO.BASILE@ POLITO.IT >

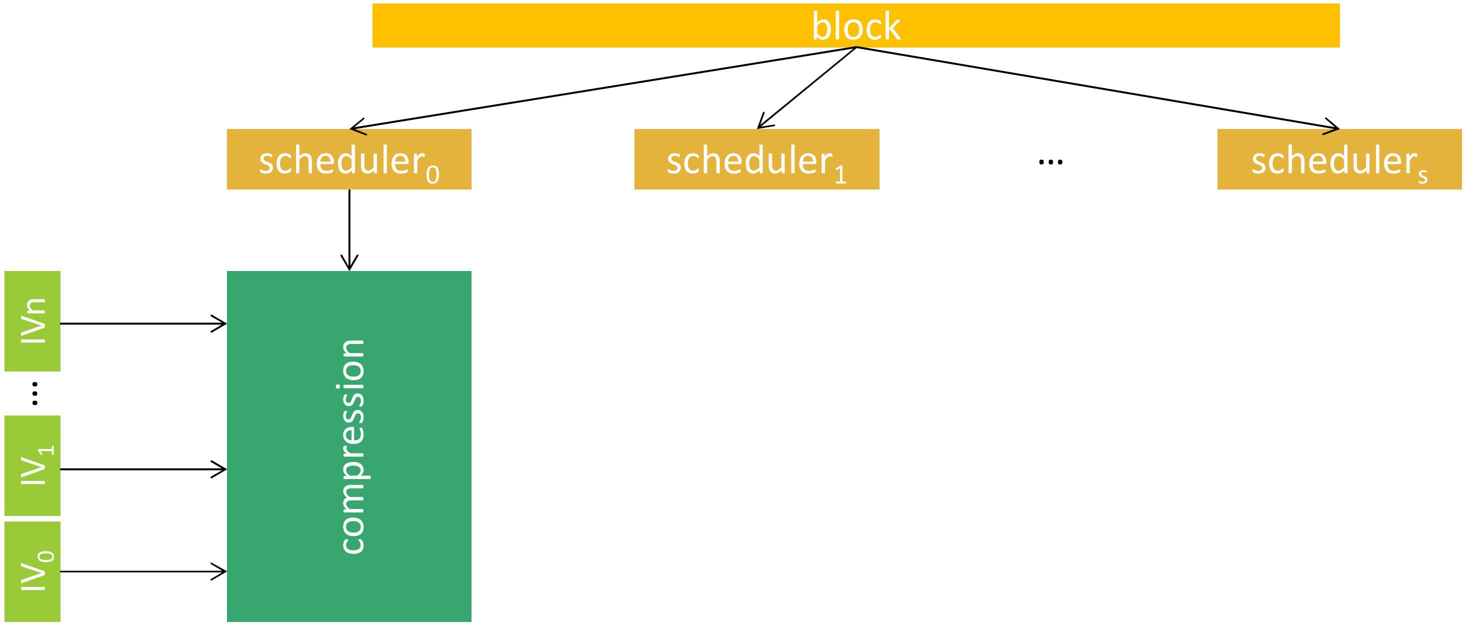
POLITECNICO DI TORINO

Agenda

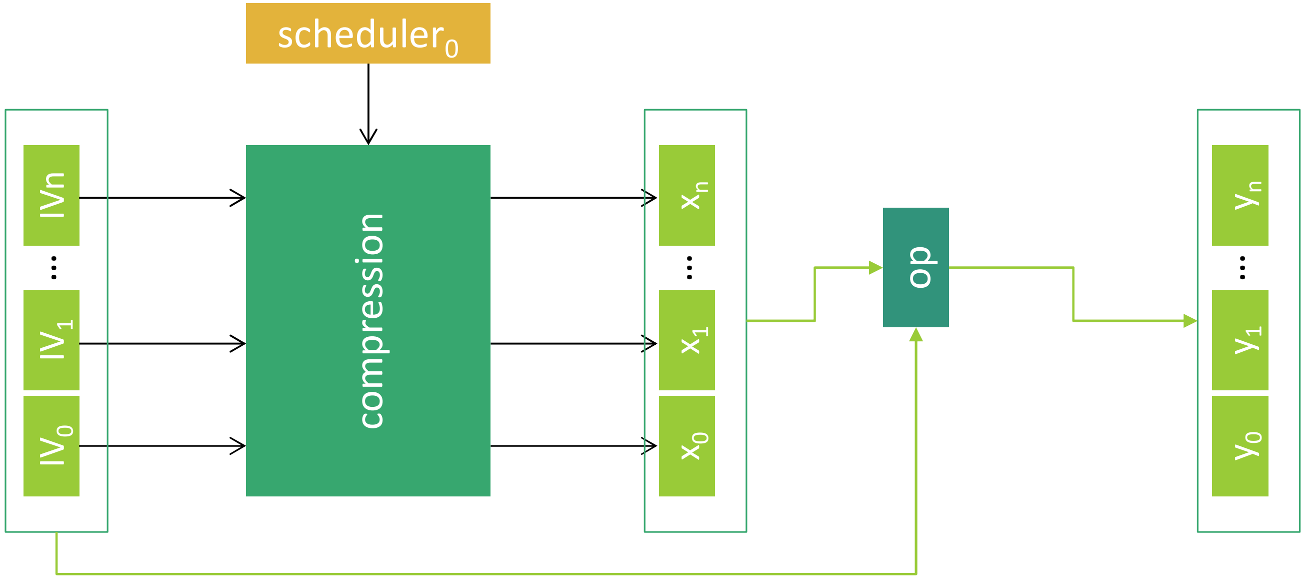
- learning objectives
  - weak hash algorithms you can easily find collisions
    - short digests do not help…
  - hash constructions may be intrinsically weak
    - Merkle-Damgard still resists but…

- topics
  - Merkle-Damgard construction
    - seen from an attacker perspective
  - length extension attacks
  - Wang attack against MD4

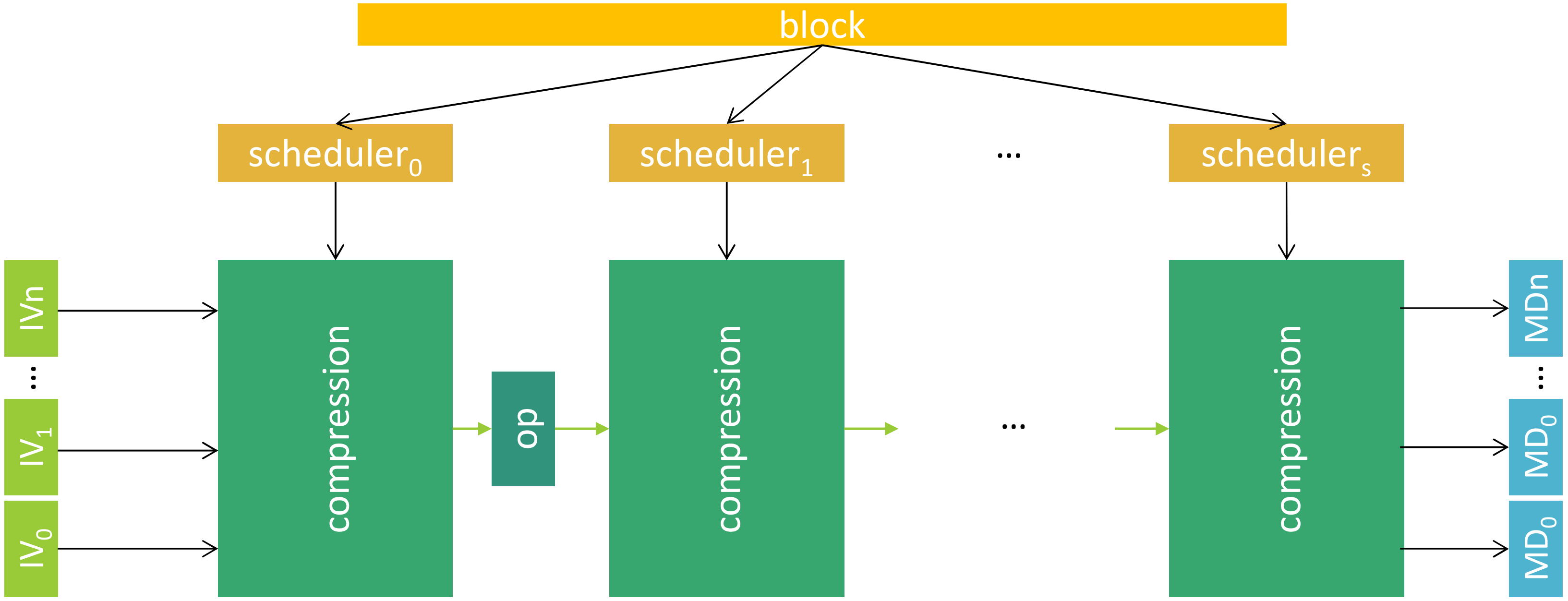
Merkle-Damgard architecture: 1 block



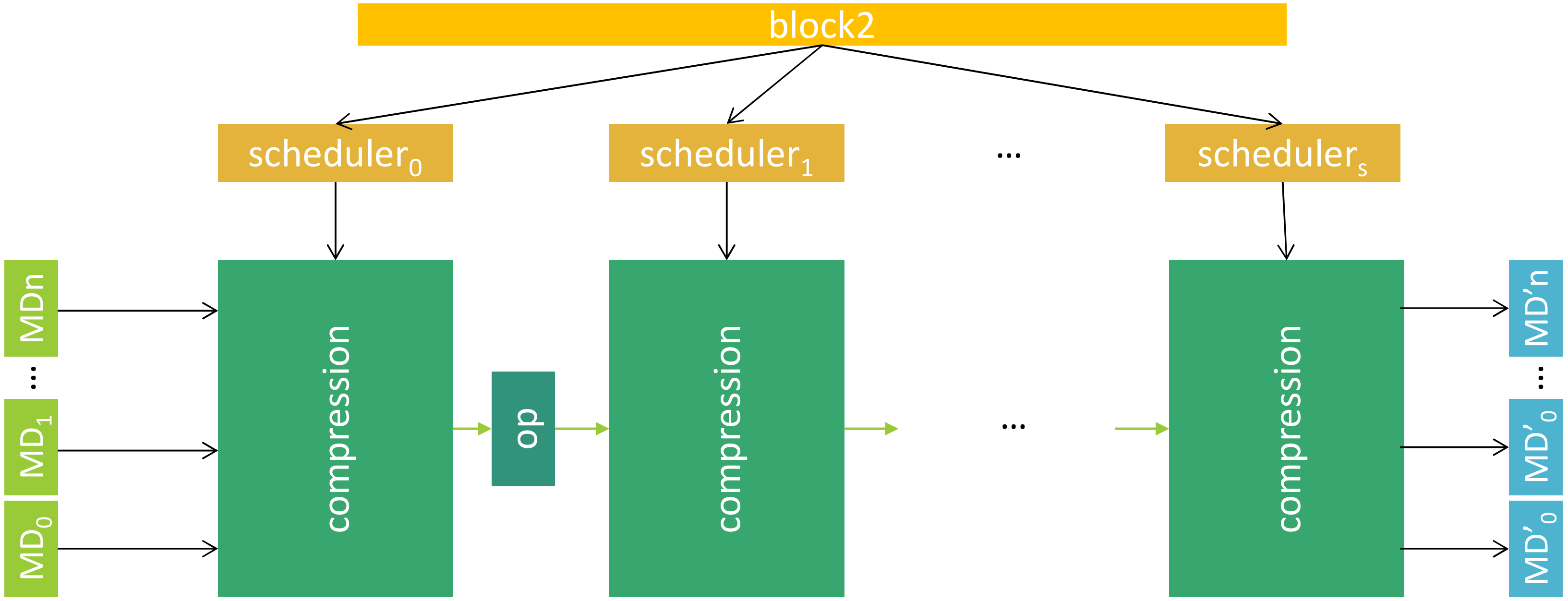
Compression



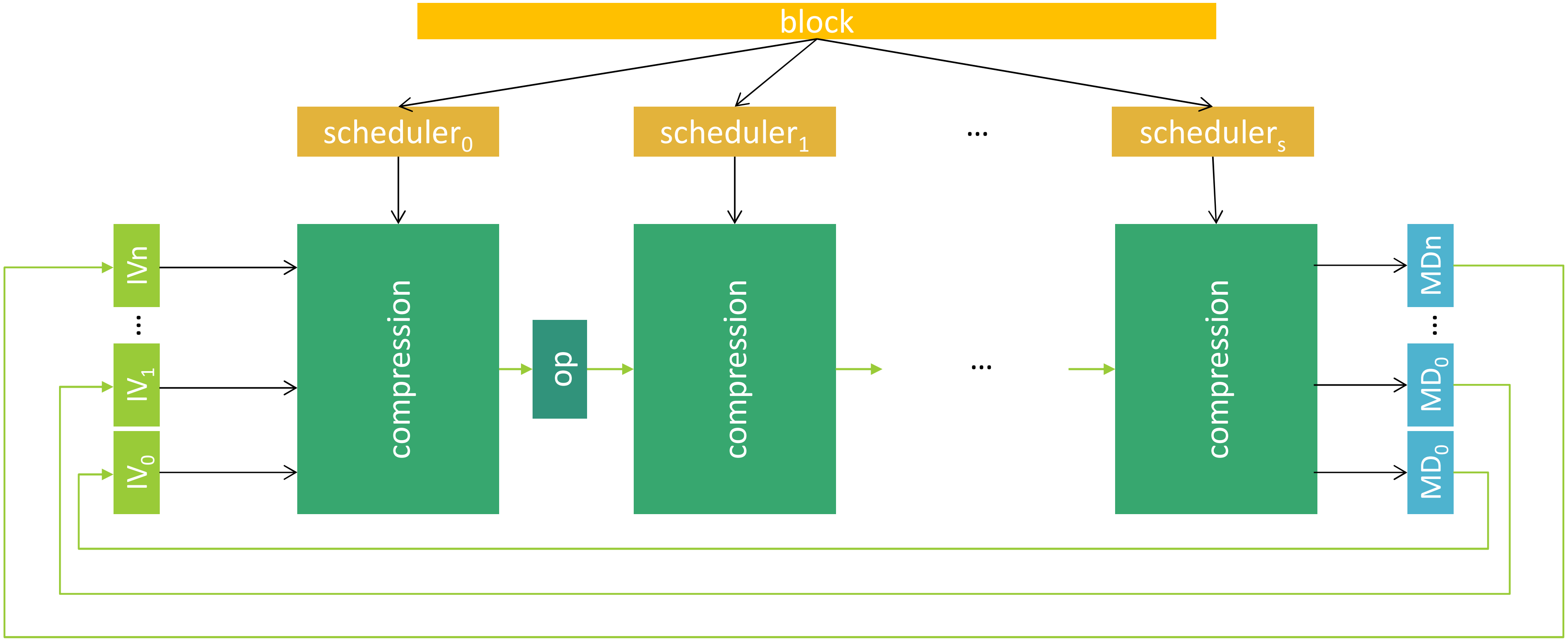
Merkle-Damgard architecture: 1 block



Merkle-Damgard architecture: block 2



Merkle-Damgard architecture



Attacks against the Merkle-Damgard construction

prone to multi-collision attacks

- many messages with the same hash
- i.e., once you find a collision it’s computationally easy to generate additional collisions

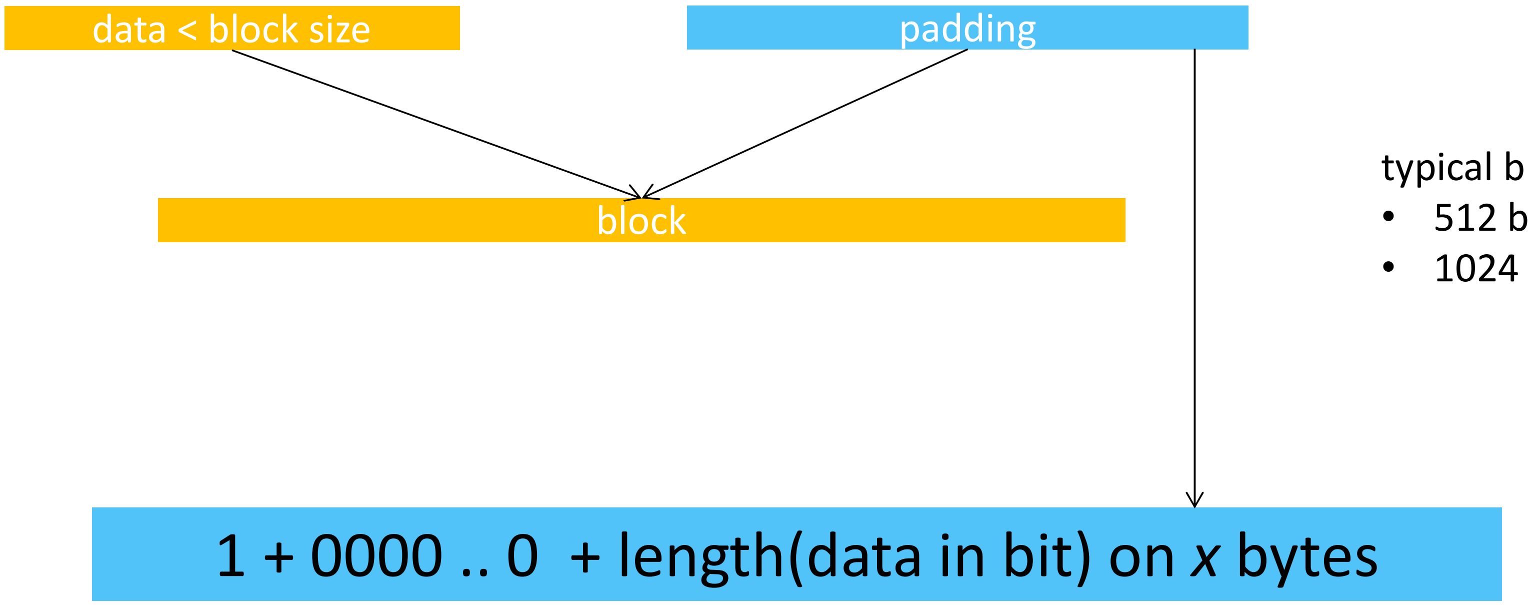
Herding attacks = chosen-prefix collisions

- to find useful collisions in less-than-ideal case
- https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=150629

length extension

- digest of the *n*-th block computed based on the digest of the previous n-1 blocks
  - may break wrongly designed keyed-digests
- worked against commercial web message authentication schemes

Length extension attack



data < block size

padding

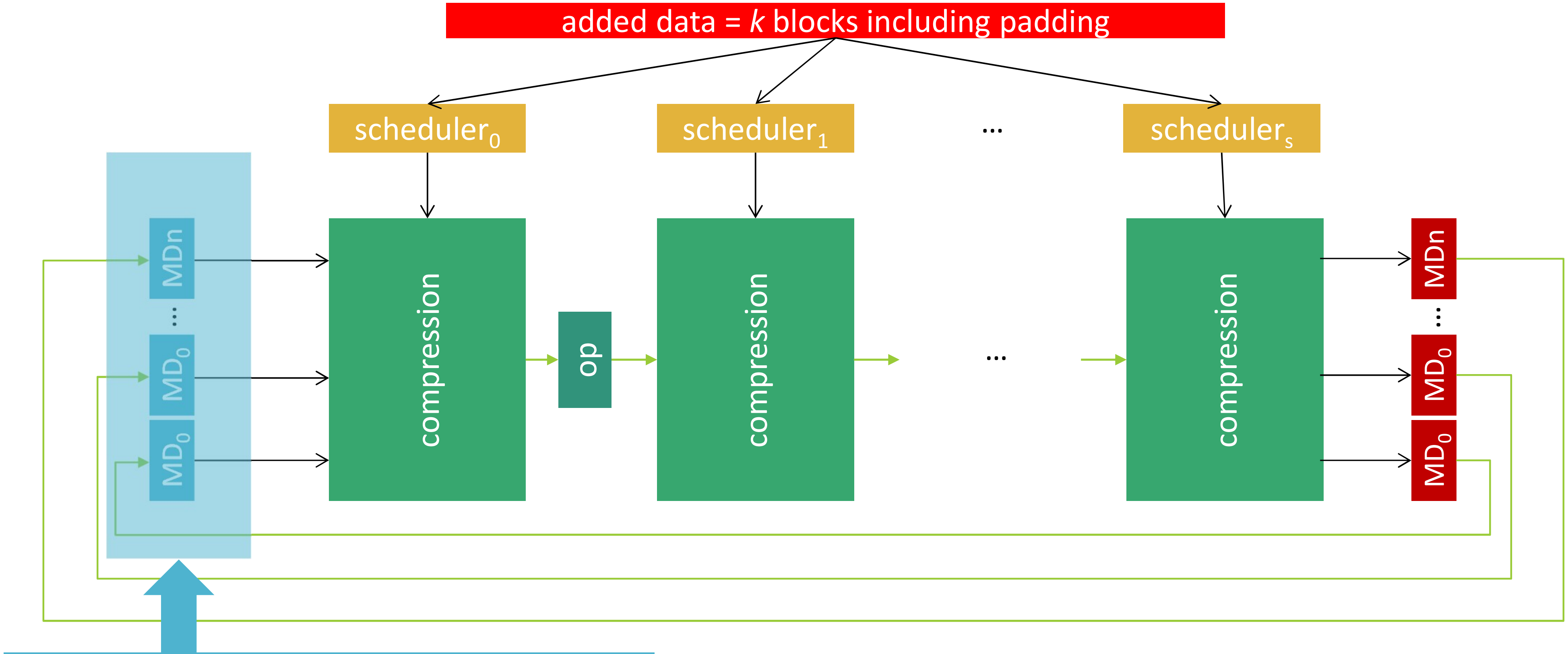
block

1 + 0000 .. 0 + length(data in bit) on *x* bytes

typical block size

- 512 bit
- 1024 bit

Merkle-Damgard: length extension



this is the (keyed-)hash sniffed by the attacks

A general purpose tool

HashPump automatically implements the attack for several algorithms

- implemented in C++
- https://github.com/bwall/HashPump

Collision attacks

against MD4 based on a paper of Wang

- https://link.springer.com/chapter/10.1007/978-3-642-25243-3_19
- https://eprint.iacr.org/2005/151.pdf
- implementation of the attack is here
  - https://github.com/HMY626/MD4-Collision

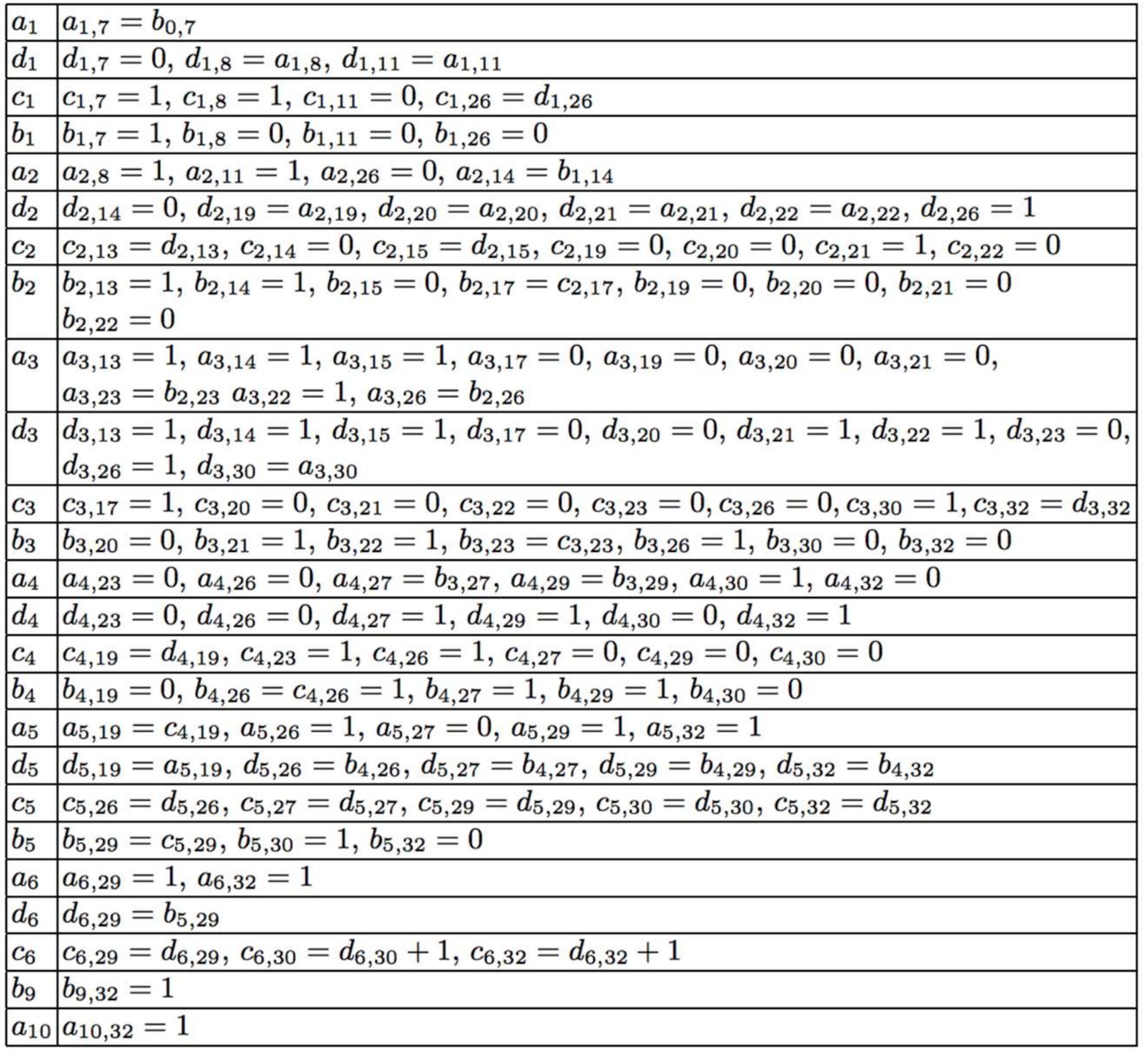
another interesting reading (SHAttered, against SHA-1)

- https://shattered.io/static/shattered.pdf

visualization of MD5 collisions

- https://www.links.org/?p=6

Table 6. A Set of Sufficient Conditions for Collisions of MD4



a_1	$a_{1,7} = b_{0,7}$
d_1	$d_{1,7} = 0,\ d_{1,8} = a_{1,8},\ d_{1,11} = a_{1,11}$
c_1	$c_{1,7} = 1,\ c_{1,8} = 1,\ c_{1,11} = 0,\ c_{1,26} = d_{1,26}$
b_1	$b_{1,7} = 1,\ b_{1,8} = 0,\ b_{1,11} = 0,\ b_{1,26} = 0$
a_2	$a_{2,8} = 1,\ a_{2,11} = 1,\ a_{2,26} = 0,\ a_{2,14} = b_{1,14}$
d_2	$d_{2,14} = 0,\ d_{2,19} = a_{2,19},\ d_{2,20} = a_{2,20},\ d_{2,21} = a_{2,21},\ d_{2,22} = a_{2,22},\ d_{2,26} = 1$
c_2	$c_{2,13} = d_{2,13},\ c_{2,14} = 0,\ c_{2,15} = d_{2,15},\ c_{2,19} = 0,\ c_{2,20} = 0,\ c_{2,21} = 1,\ c_{2,22} = 0$
b_2	$b_{2,13} = 1,\ b_{2,14} = 1,\ b_{2,15} = 0,\ b_{2,17} = c_{2,17},\ b_{2,19} = 0,\ b_{2,20} = 0,\ b_{2,21} = 0$ $b_{2,22} = 0$
a_3	$a_{3,13} = 1,\ a_{3,14} = 1,\ a_{3,15} = 1,\ a_{3,17} = 0,\ a_{3,19} = 0,\ a_{3,20} = 0,\ a_{3,21} = 0,$ $a_{3,23} = b_{2,23}\ a_{3,22} = 1,\ a_{3,26} = b_{2,26}$
d_3	$d_{3,13} = 1,\ d_{3,14} = 1,\ d_{3,15} = 1,\ d_{3,17} = 0,\ d_{3,20} = 0,\ d_{3,21} = 1,\ d_{3,22} = 1,\ d_{3,23} = 0,$ $d_{3,26} = 1,\ d_{3,30} = a_{3,30}$
c_3	$c_{3,17} = 1,\ c_{3,20} = 0,\ c_{3,21} = 0,\ c_{3,22} = 0,\ c_{3,23} = 0, c_{3,26} = 0, c_{3,30} = 1, c_{3,32} = d_{3,32}$
b_3	$b_{3,20} = 0,\ b_{3,21} = 1,\ b_{3,22} = 1,\ b_{3,23} = c_{3,23},\ b_{3,26} = 1,\ b_{3,30} = 0,\ b_{3,32} = 0$
a_4	$a_{4,23} = 0,\ a_{4,26} = 0,\ a_{4,27} = b_{3,27},\ a_{4,29} = b_{3,29},\ a_{4,30} = 1,\ a_{4,32} = 0$
d_4	$d_{4,23} = 0,\ d_{4,26} = 0,\ d_{4,27} = 1,\ d_{4,29} = 1,\ d_{4,30} = 0,\ d_{4,32} = 1$
c_4	$c_{4,19} = d_{4,19},\ c_{4,23} = 1,\ c_{4,26} = 1,\ c_{4,27} = 0,\ c_{4,29} = 0,\ c_{4,30} = 0$
b_4	$b_{4,19} = 0,\ b_{4,26} = c_{4,26} = 1,\ b_{4,27} = 1,\ b_{4,29} = 1,\ b_{4,30} = 0$
a_5	$a_{5,19} = c_{4,19},\ a_{5,26} = 1,\ a_{5,27} = 0,\ a_{5,29} = 1,\ a_{5,32} = 1$
d_5	$d_{5,19} = a_{5,19},\ d_{5,26} = b_{4,26},\ d_{5,27} = b_{4,27},\ d_{5,29} = b_{4,29},\ d_{5,32} = b_{4,32}$
c_5	$c_{5,26} = d_{5,26},\ c_{5,27} = d_{5,27},\ c_{5,29} = d_{5,29},\ c_{5,30} = d_{5,30},\ c_{5,32} = d_{5,32}$
b_5	$b_{5,29} = c_{5,29},\ b_{5,30} = 1,\ b_{5,32} = 0$
a_6	$a_{6,29} = 1,\ a_{6,32} = 1$
d_6	$d_{6,29} = b_{5,29}$
c_6	$c_{6,29} = d_{6,29},\ c_{6,30} = d_{6,30} + 1,\ c_{6,32} = d_{6,32} + 1$
b_9	$b_{9,32} = 1$
a_{10}	$a_{10,32} = 1$