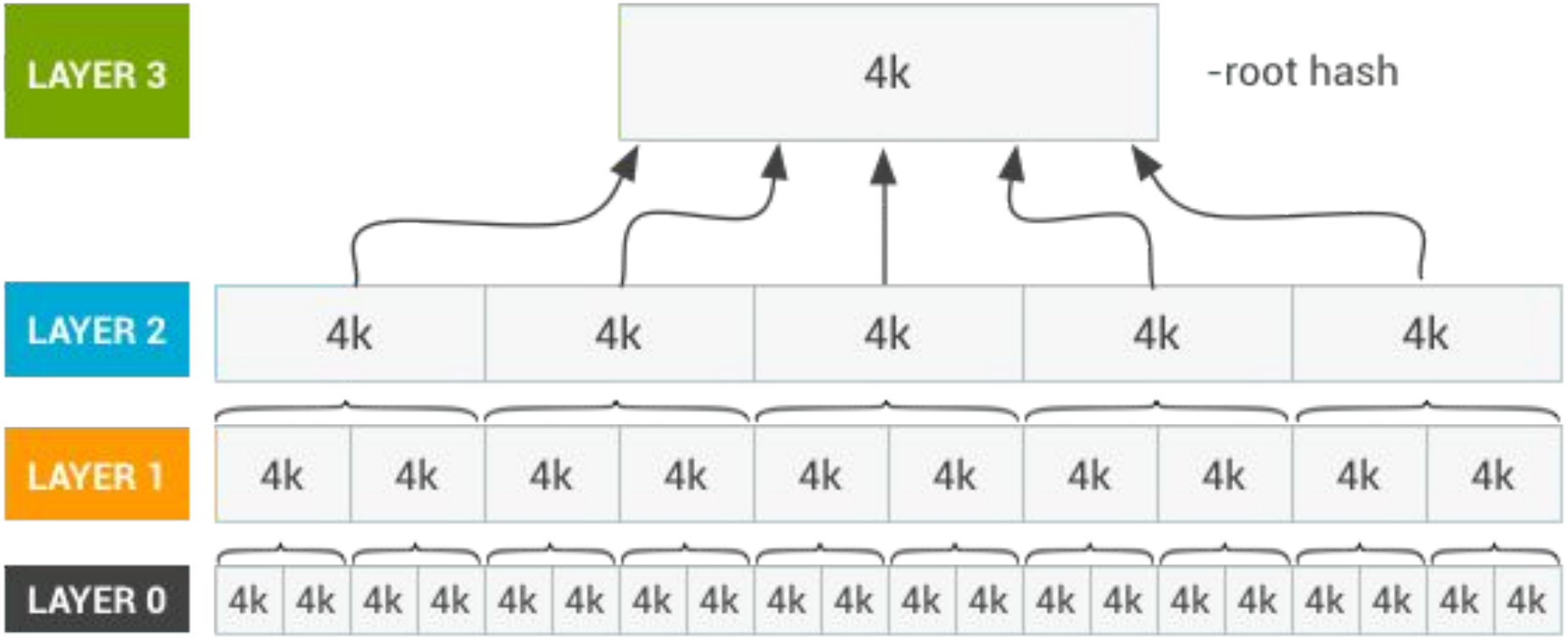
$1000 talk
Fast hashing with TCRs

Paul Crowley, Google LLC


LAYER 3
4k
-root hash
LAYER 2
4k
4k
4k
4k
4k
LAYER 1
4k
4k
4k
4k
4k
4k
4k
4k
4k
4k
LAYER 0
4k
4k
4k
4k
4k
4k
4k
4k
4k
4k
4k
4k
4k
4k
4k
4k
4k
4k
4k
4k

Hashing is too slow

900MHz Broadcom BCM2836 (2015):

- SHA-256: 28.9 cpb, 31.2 MB/s
- BLAKE2b: 15.3 cpb, 58.7 MB/s

Much slower than underlying hardware

Universal function

or almost universal

- Attacker chooses m
- Attacker chooses $m' \neq m$
- Attacker learns random key k
- Attacker wins if $H(k, m) = H(k, m')$

Not suitable for broadcast.

Hash function

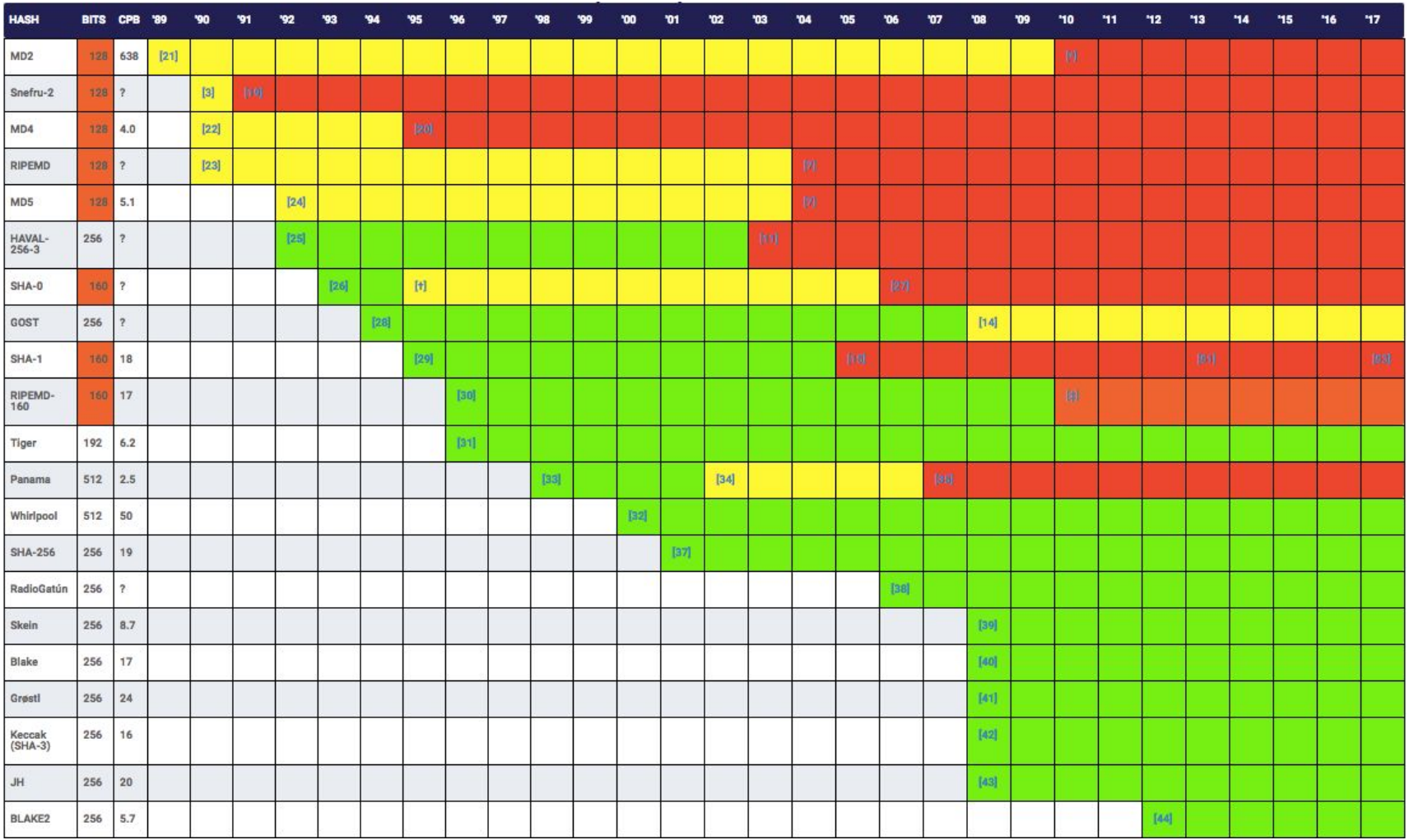
in one model of security

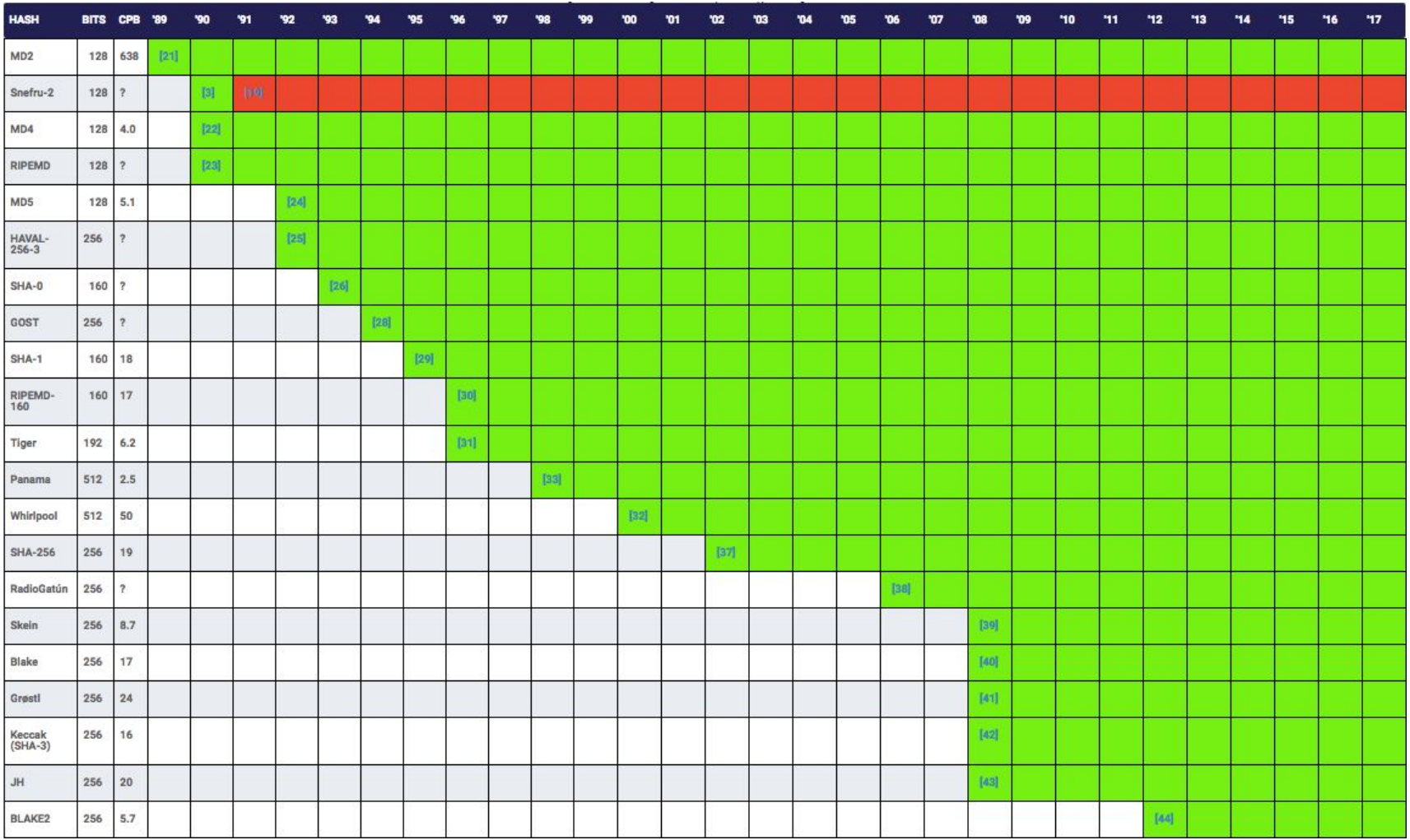
- Attacker learns random key k
- Attacker chooses m
- Attacker chooses $m' \neq m$
- Attacker wins if $H(k, m) = H(k, m')$

Too slow.

Target collision resistant function

- Attacker chooses message m
- Attacker learns random key k
- Attacker chooses $m' \neq m$
- Attacker wins if $H(k, m) = H(k, m')$


HASH
BITS
CPB
'89
'90
'91
'92
'93
'94
'95
'96
'97
'98
'99
'00
'01
'02
'03
'04
'05
'06
'07
'08
'09
'10
'11
'12
'13
'14
'15
'16
'17
MD2
128
638
[21]
[1]
Snefru-2
128
?
[3]
[19]
MD4
128
4.0
[22]
[20]
RIPEMD
128
?
[23]
[7]
MD5
128
5.1
[24]
[7]
HAVAL-256-3
256
?
[25]
[11]
SHA-0
160
?
[26]
[†]
[27]
GOST
256
?
[28]
[14]
SHA-1
160
18
[29]
[13]
[51]
[53]
RIPEMD-160
160
17
[30]
[3]
Tiger
192
6.2
[31]
Panama
512
2.5
[33]
[34]
[35]
Whirlpool
512
50
[32]
SHA-256
256
19
[37]
RadioGatún
256
?
[38]
Skein
256
8.7
[39]
Blake
256
17
[40]
Grøstl
256
24
[41]
Keccak (SHA-3)
256
16
[42]
JH
256
20
[43]
BLAKE2
256
5.7
[44]


HASH
BITS
CPB
'89
'90
'91
'92
'93
'94
'95
'96
'97
'98
'99
'00
'01
'02
'03
'04
'05
'06
'07
'08
'09
'10
'11
'12
'13
'14
'15
'16
'17
MD2 128 638 [21]
Snefru-2 128 ? [3] [19]
MD4 128 4.0 [22]
RIPEMD 128 ? [23]
MD5 128 5.1 [24]
HAVAL-256-3 256 ? [25]
SHA-0 160 ? [26]
GOST 256 ? [28]
SHA-1 160 18 [29]
RIPEMD-160 160 17 [30]
Tiger 192 6.2 [31]
Panama 512 2.5 [33]
Whirlpool 512 50 [32]
SHA-256 256 19 [37]
RadioGatún 256 ? [38]
Skein 256 8.7 [39]
Blake 256 17 [40]
Grøstl 256 24 [41]
Keccak (SHA-3) 256 16 [42]
JH 256 20 [43]
BLAKE2 256 5.7 [44]

$1000 prize

- for most interesting work
  - Attack my proposal
  - Propose TCRs
  - Consider multiple-target attacks
  - Consider quantum resistance
- Advance our understanding of faster-than-hash verification
- Deadline: 31 December 2019 (probably)
- Full presentation (WIP): https://is.gd/jLAEBO
  - fun stuff eg “tweakable TCRs” and more.
- Remember this presentation when judging “Le méta-prix Poincaré-Magritte-Couperin” - thank you!