The *Real* SHA-2,3,...

Pierre Karpman

$\aleph_0$ — France

pierre.karpman@$\aleph_0$.fr

CRYPTO 2015 Rump Session, Santa Barbara
2015–08–18

All hail SHA-3!

- NIST standardized SHA-3 this month (FIPS-202)
- 4th SHA, coming after SHA-0, SHA-1, SHA-2
- Winner of an *academic competition*
- Markedly different from SHA-2, SHA-1, SHA-0

Reminder: Initial NIST strategy

- SHA-0 := Some round function, Some message expansion
- SHA-1 := SHA-0's round function, (SHA-0's message expansion) $\circlearrowleft$ 1
- $\Uparrow$ "key" (message) rotation: very nice!

Reminder: Initial NIST strategy

- SHA-0 := Some round function, Some message expansion
- SHA-1 := SHA-0's round function, (SHA-0's message expansion) $\circlearrowleft$ 1
- $\Uparrow$ "key" (message) rotation: very nice!

Reminder: Initial NIST strategy

- SHA-0 := Some round function, Some message expansion
- SHA-1 := SHA-0's round function, (SHA-0's message expansion) $\circlearrowleft$ 1
- $\Uparrow$ "key" (message) rotation: very nice!

But then...

- SHA-2 := Complex round function, nothing to do with SHA-0's, Complex message expansion, nothing to do with SHA-0's
- And SHA-3 := Very complex round function (in 3D, need polarizing glasses to visualize), NO MESSAGE EXPANSION!

But then...

- SHA-2 := Complex round function, nothing to do with SHA-0's, Complex message expansion, nothing to do with SHA-0's
- And SHA-3 := Very complex round function (in 3D, need polarizing glasses to visualize), NO MESSAGE EXPANSION!

My point: KISS

⇒ Let's go back to NIST's initial strategy

- CAT-4, a SHA-4 proposal
- := SHA-0's round function, (SHA-0's message expansion) $\circlearrowleft$ 4

⇒ Let's go back to NIST's initial strategy

- CAT-4, a SHA-4 proposal
- := SHA-0's round function, (SHA-0's message expansion) $\circlearrowleft$ 4

CAT-4's advantages

- Easy to migrate from SHA-0 or SHA-1
- Mostly compatible with existing HW/Instruction sets
- Lightweight : state $\approx 320 + 512$ bits < 1000 gates
- Well understood security (most analysis on SHA-1 also applies)

CAT-4's advantages

- Easy to migrate from SHA-0 or SHA-1
- Mostly compatible with existing HW/Instruction sets
- Lightweight : state $\approx 320 + 512$ bits < 1000 gates
- Well understood security (most analysis on SHA-1 also applies)

CAT-4's advantages

- Easy to migrate from SHA-0 or SHA-1
- Mostly compatible with existing HW/Instruction sets
- Lightweight : state $\approx 320 + 512$ bits < 1000 gates
- Well understood security (most analysis on SHA-1 also applies)

CAT-4's advantages

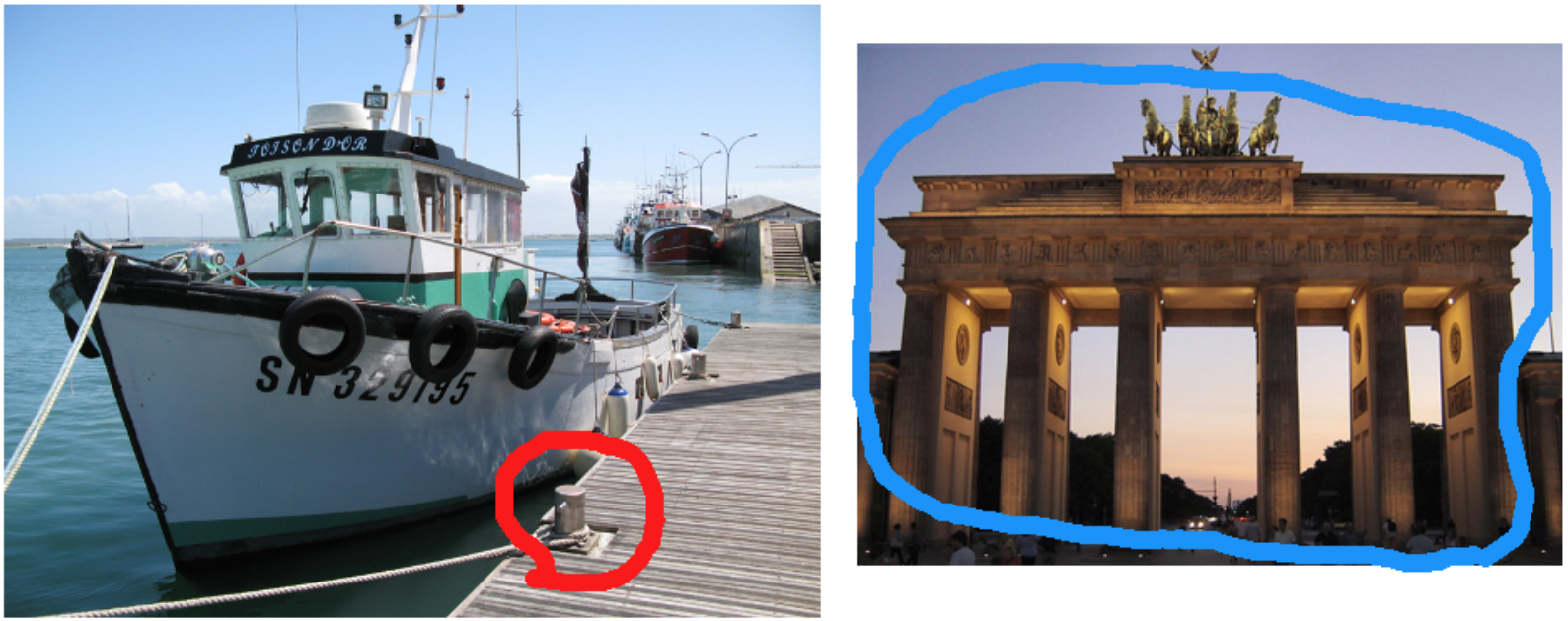

Figure : Fact: 1 bitte (French bit) « 1 German gate

CAT-4's advantages

- Easy to migrate from SHA-0 or SHA-1
- Mostly compatible with existing HW/Instruction sets
- Lightweight : state $\approx 320 + 512$ bits < 1000 gates
- Well understood security (most analysis on SHA-1 also applies)

Please contact me to make SHA-4 a reality!!

≈~≈⇒ pierre.karpman@$\aleph_0$.fr ⇐≈~≈