# Too Much Crypto

Jean-Philippe Aumasson

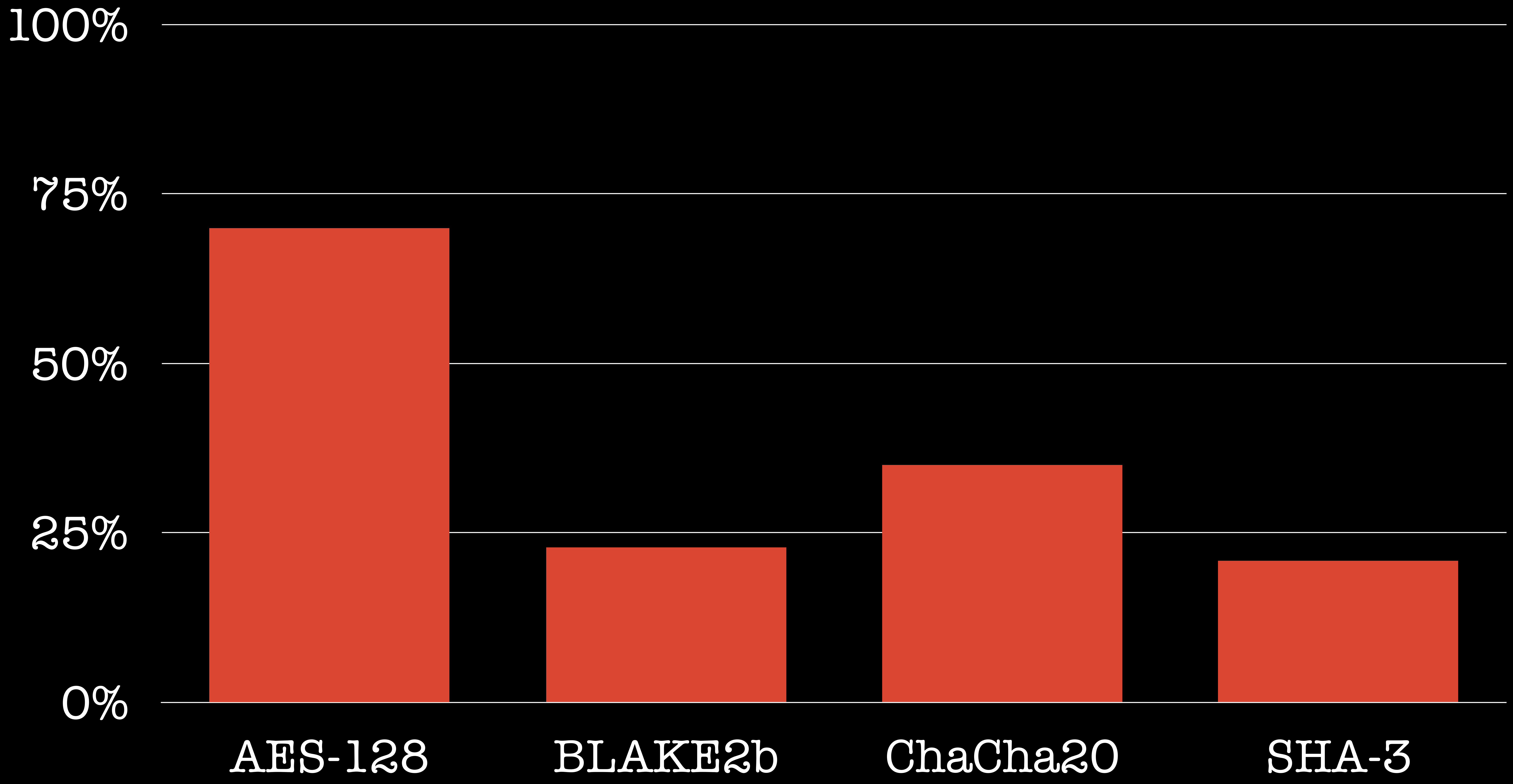
Teserakt

# Three acts

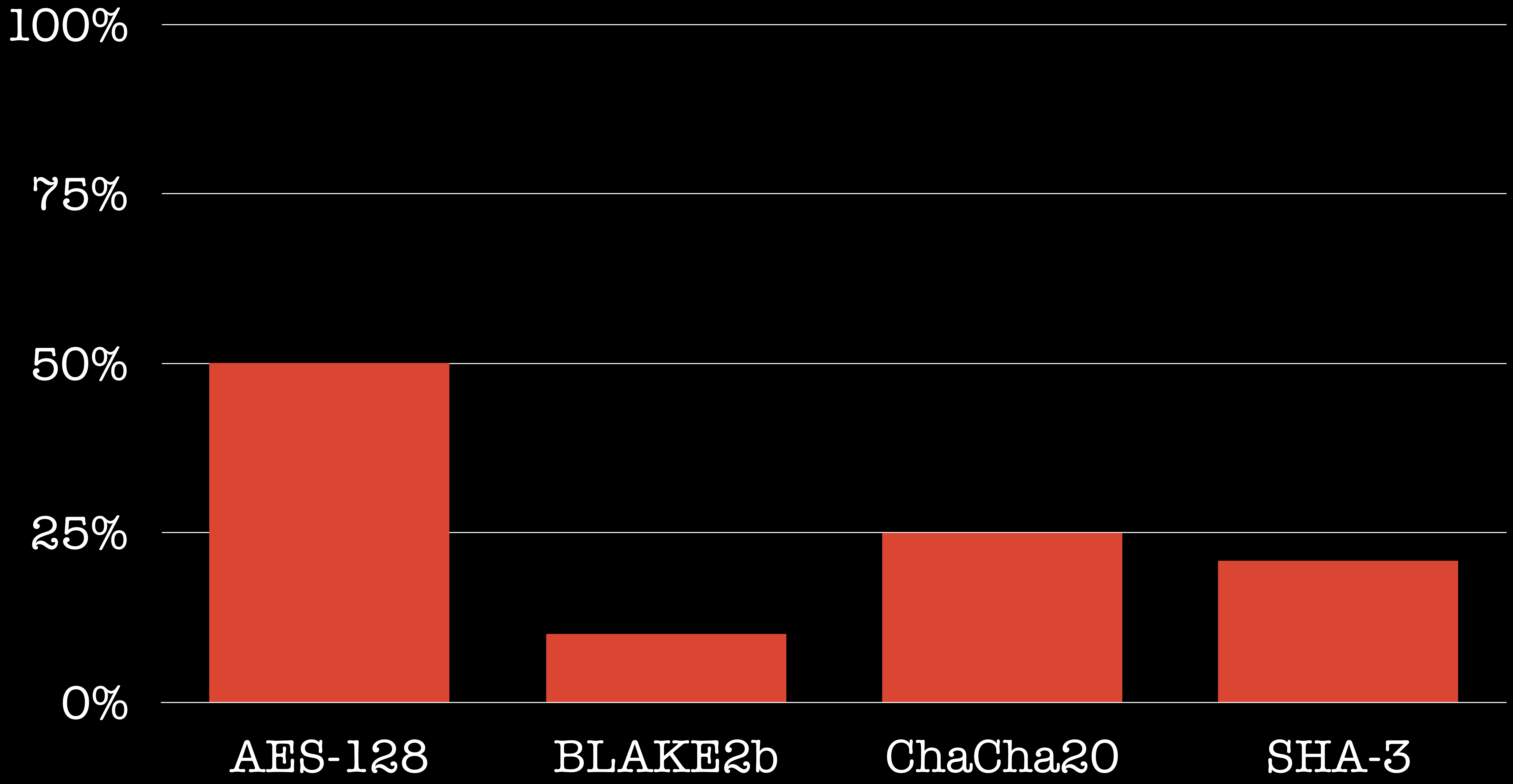
1. Problem exposition
2. Explanation attempts
3. Resolution proposals

1/3

# “Broken” rounds



# Practically broken rounds



# Inconsistent security margins

# AES – 5 rounds

|  | 1998 | 2000 | 2018 | 2019 |
|---|---|---|---|---|
| “Time” | 2^45 | 2^35 | 2^24 | 2^16 |
| “Data” | 2^11 | 2^33 | 2^24 | 2^15 |

# AES – 6 rounds

|  | 1998 | 2000 | 2018 |
|---|---|---|---|
| “Time” | 2^72 | 2^44 | 2^80 |
| “Data” | 2^34 | 2^35 | 2^26 |

# AES – 7 rounds

| | 2000 | 2013 | 2018 |
|---|---|---|---|
| “Time” | 2^155 | 2^99 | 2^146 |
| “Data” | 2^36 | 2^97 | 2^26 |
| “Memory” | 2^32 | 2^100 | 2^40 |

# ChaCha – 7 rounds

| | 2008 | 2016 |
|---|---|---|
| “Time” | 2^248 | 2^238 |
| “Data” | 2^27 | 2^96 |

# Attacks don’t really get better

# A mature research field

Symmetric cryptanalysis well-explored territory:

- Mostly variants of differential or linear cryptanalysis
- Thousands of papers, stagnating results and techniques
- Even DES and GOST are not convincingly broken

# AES – 7 rounds

| | 2000 | 2013 | 2018 |
|---|---|---|---|
| “Time" | 2^155 | 2^99 | 2^146 |
| “Data" | 2^36 | 2^97 | 2^26 |
| “Memory" | 2^32 | 2^100 | 2^40 |

# What do these numbers mean?

# Real-world

Orders of magnitude reminder:

- 2^**61** ≈ SHA-1 chosen-prefix collision
- 2^**76** ≈ current per-block Bitcoin effort
- 2^**88** ≈ nanoseconds since the Big Bang
- 2^**200** ≈ Earth volume physical information capacity

# Impossible is impossible

“The difference between 80 bits and 128 bits of key search is like the difference between a mission to Mars and a mission to Alpha Centauri. (...) no meaningful difference between 192-bit and 256-bit keys in terms of practical bruteforce attacks; impossible is impossible.”
—John Kelsey

“any primitive at or above the 128-bit security level is equally matched today, because they are all effectively infinitely strong”
—Adam Langley

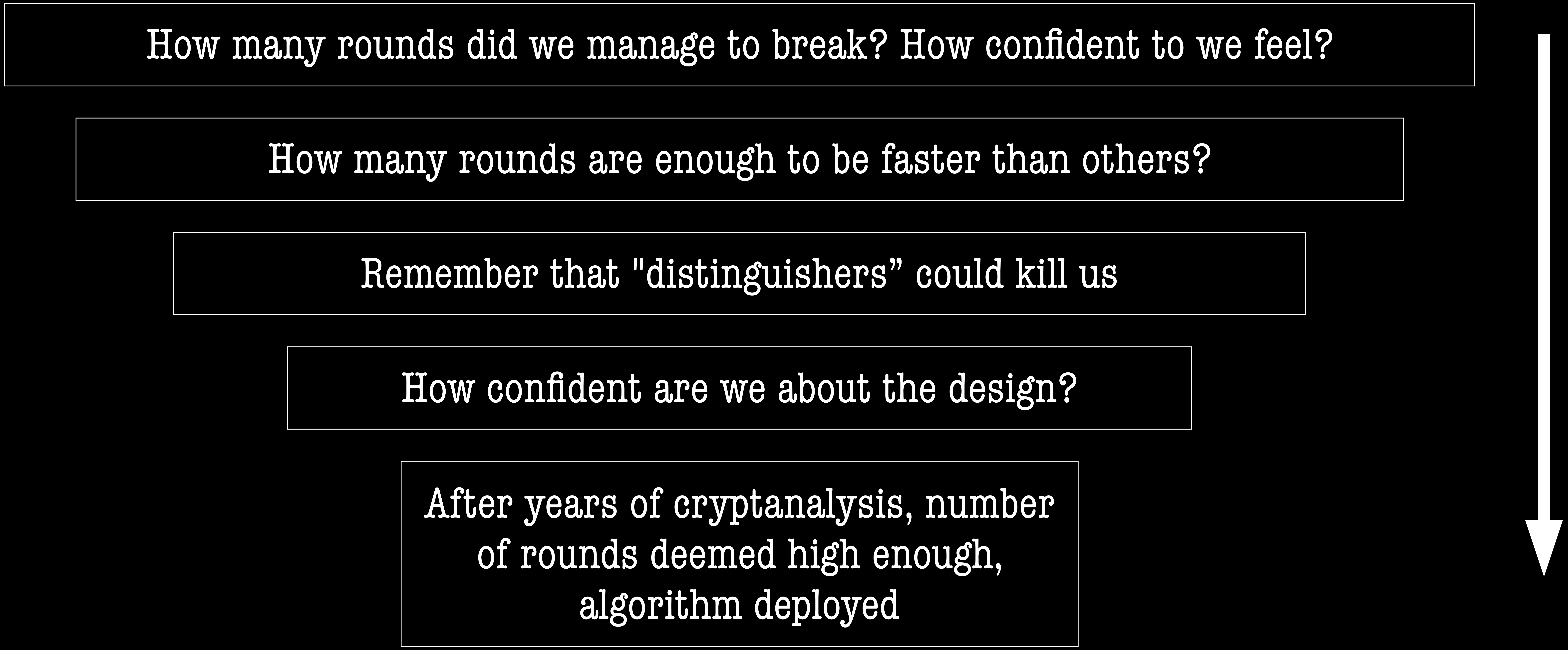
# Impossibility theorem

No attack requiring **2^N-{time | data |memory}** where N ≥128 will ever be completed before the human species goes extinct.

(Caveat: quantum speed-ups when applicable, as there’s a thin chance that a scalable QC be built)

How do we choose round numbers?

# Round selection process



How many rounds did we manage to break? How confident to we feel?

How many rounds are enough to be faster than others?

Remember that "distinguishers” could kill us

How confident are we about the design?

After years of cryptanalysis, number of rounds deemed high enough, algorithm deployed

In large part arbitrary, dependent on context and risk appetite

# Rare opportunities for correction

# Too many/few rounds?

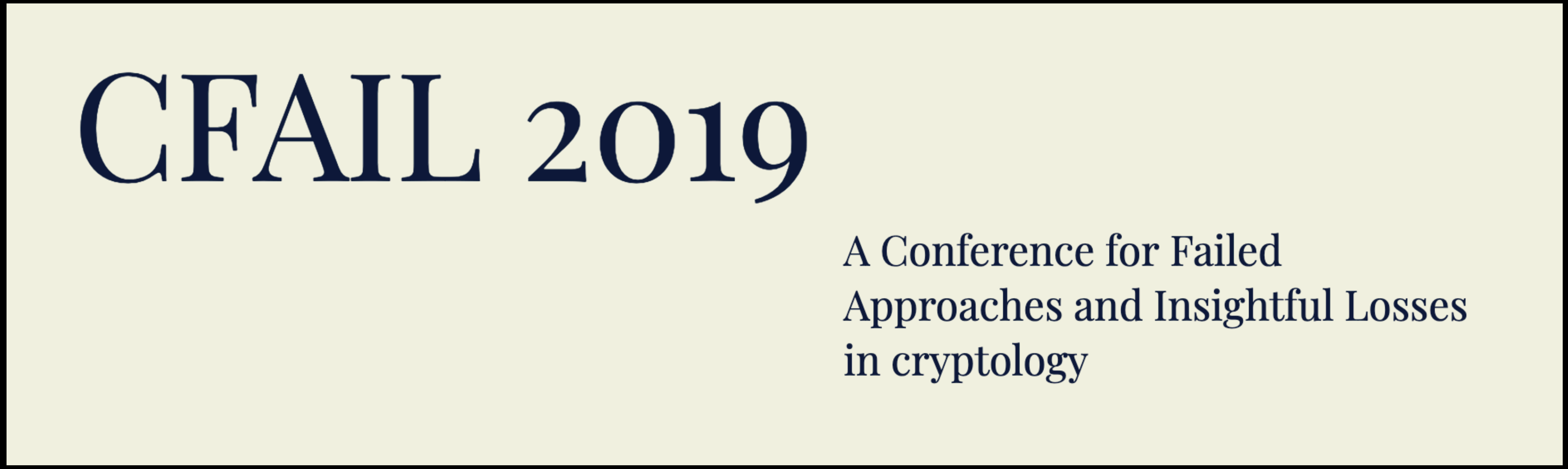
2/3

# Attacks as negative results

Most attacks published are **failures** to attack the full primitive, and help us understand what makes a primitive secure, by targeting weakened versions:

- Weaker **internals**, e.g. SHI1's linearized SHA1
- Weaker **models**, e.g. related-key models
- Weaker **goals**, e.g.  distinguishers

# Negative results matter



CFAIL 2019

A Conference for Failed
Approaches and Insightful Losses
in cryptology

“we are founding a new conference: a place for papers that describe instructive failures or not-yet-successes, as they may prefer to be called.”

We need more negative results (see CFAIL 2020)

# Reading negative results

The 2^238 attack on 7 of ChaCha's 20 rounds can be read as:

A. **ChaCha7 is broken**, because it fails to be 256-bit secure

B. **ChaCha7 is risky**, because the attack might be improved and be practical

C. **ChaCha7 is safe**, because the best attack found is highly impractical

# Reading negative results

The 2^238 attack on 7 of ChaCha's 20 rounds can be read as:

A. **ChaCha7 is broken**, because it fails to be 256-bit secure

B. **ChaCha7 is risky**, because the attack might be improved and be practical

C. **ChaCha7 is safe**, because the best attack found is highly impractical

Answer A is only valid for definitions of "broken" irrelevant to security and real-world considerations.

# Reading negative results

The 2^238 attack on 7 of ChaCha's 20 rounds can be read as:

A. **ChaCha7 is broken**, because it fails to be 256-bit secure

B. **ChaCha7 is risky**, because the attack might be improved and be practical

C. **ChaCha7 is safe**, because the best attack found is highly impractical

Answers B and C are about **risk** assessment.

# Risk

“Risk means more things can happen than will happen.”
—Elroy Dimson

Cryptographers’ job is to create secure algorithms, not to worry about assurance–performance trade-offs

Choosing round numbers is a **risk assessment**, which is a different job than identifying a good enough number

# Bad risk thinking

Real-world objections, some from crypto researchers:

“**What if** a practical attack is found on AES?”

“There’s no AES security proof, so it **could be** insecure”

“I don't **believe** that ARX algorithms are secure”

“We need N+k rounds **in case** N rounds are broken"

“**4000-bit** symmetric keys are safer than 256-bit keys”

# Bad risk thinking

**What if** we live in a simulation?

# Attacks always get better™

**Attack cost** inescapably gets lower over time (Moore, etc.)

Rare major improvements, from new techniques discovery

Incremental improvements of an attack (e.g. for SHA-1)

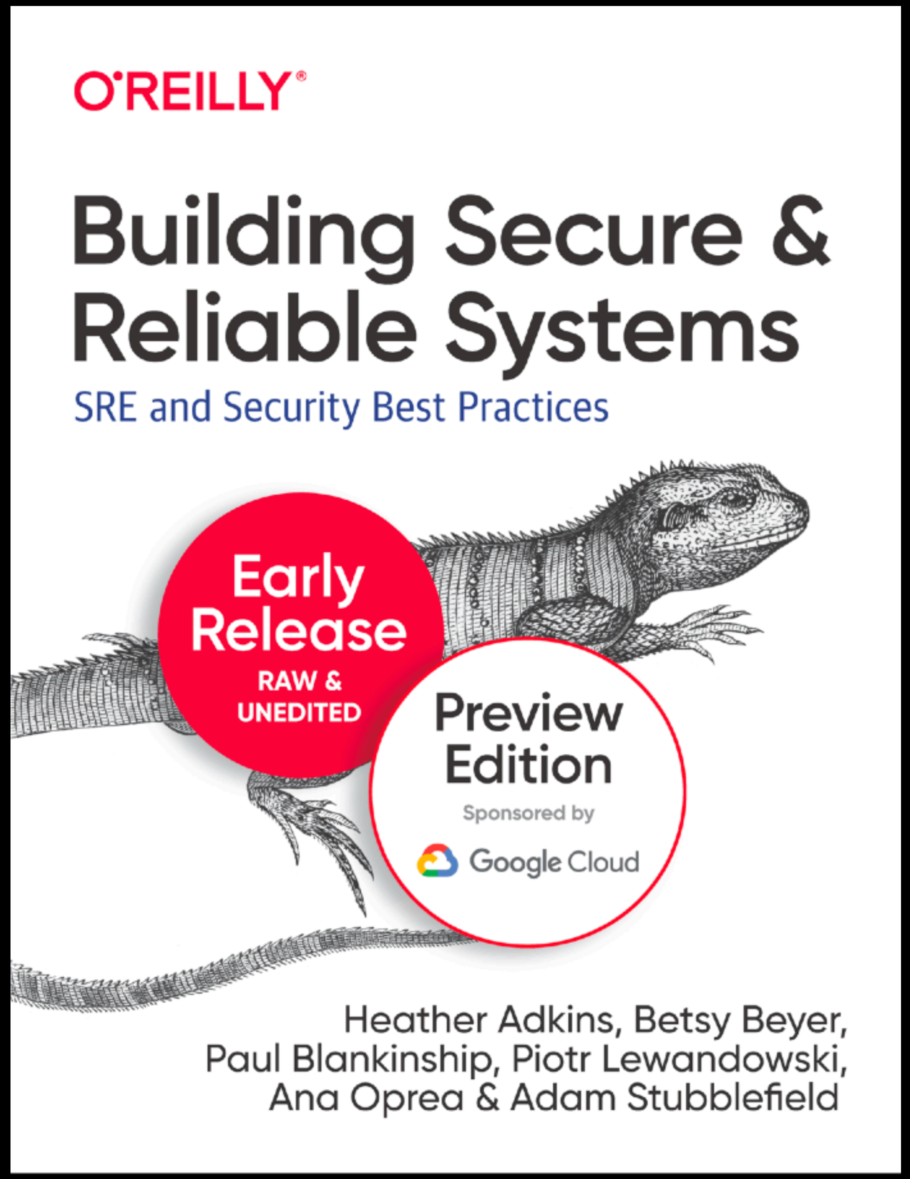
- Better implementations (SHAttered)
- Refined analysis (post-Wang papers)
- Extension (next talk)

# Crypto is never an island

The cost of compromising the system around cryptography is much lower than that of running a **2^80 time** attack, be it by attacking the software, hardware, processes, or people

Red teamers, military CNA/CNE, and cybercriminals don’t need to break the crypto to get your secret keys

# Crypto is never an island



O'REILLY

Building Secure & Reliable Systems

SRE and Security Best Practices

Early Release

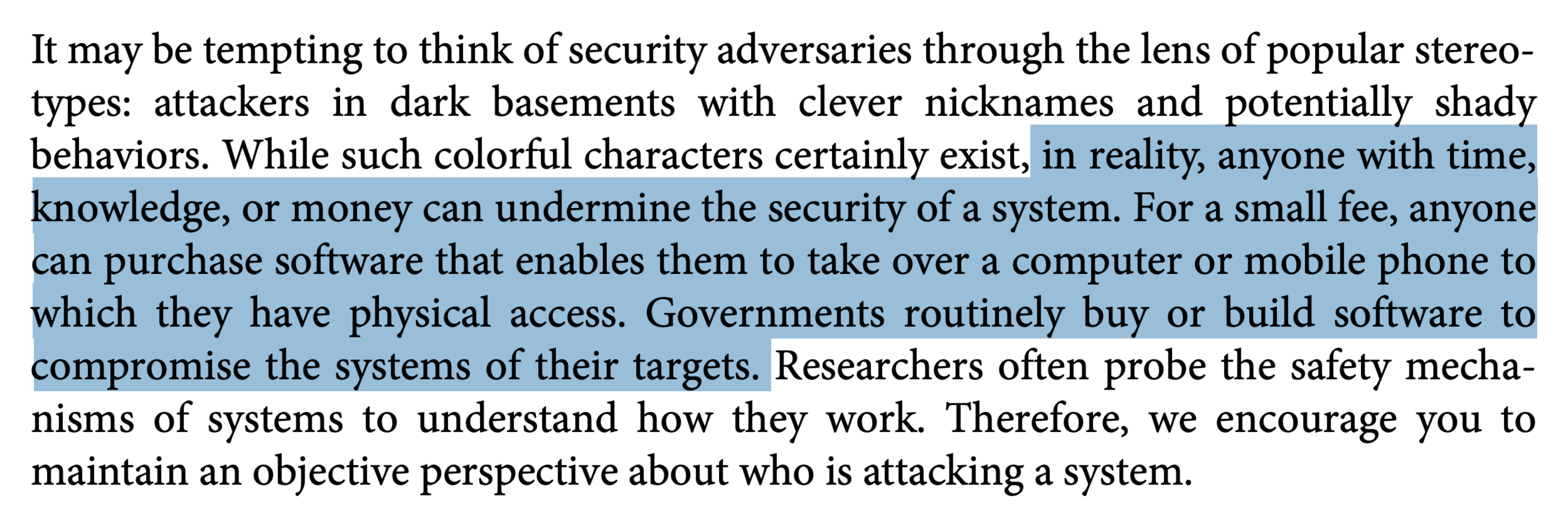
RAW & UNEDITED

Preview Edition

Sponsored by

Google Cloud

Heather Adkins, Betsy Beyer,
Paul Blankinship, Piotr Lewandowski,
Ana Oprea & Adam Stubblefield



It may be tempting to think of security adversaries through the lens of popular stereotypes: attackers in dark basements with clever nicknames and potentially shady behaviors. While such colorful characters certainly exist, in reality, anyone with time, knowledge, or money can undermine the security of a system. For a small fee, anyone can purchase software that enables them to take over a computer or mobile phone to which they have physical access. Governments routinely buy or build software to compromise the systems of their targets. Researchers often probe the safety mechanisms of systems to understand how they work. Therefore, we encourage you to maintain an objective perspective about who is attacking a system.

https://landing.google.com/sre/resources/foundationsandprinciples/srs-book/

3/3

# What we want

- More scientific and rational approach to choosing round numbers, tolerance for corrections
- More consistent security margins across primitives
- Better terminology for a better understanding

# Attack taxonomy proposal

- **Analyzed**: Less efficient than generic attacks both numerically and practically (e.g. 2^100 time & memory)
- **Attacked**: More efficient numerically yet practically impossible (e.g. 2^220 time)
- **Wounded**: Incremental improvements could lead to practical attack (e.g. 2^100)
- **Broken**: Doable now or in the near future (e.g. 2^80)

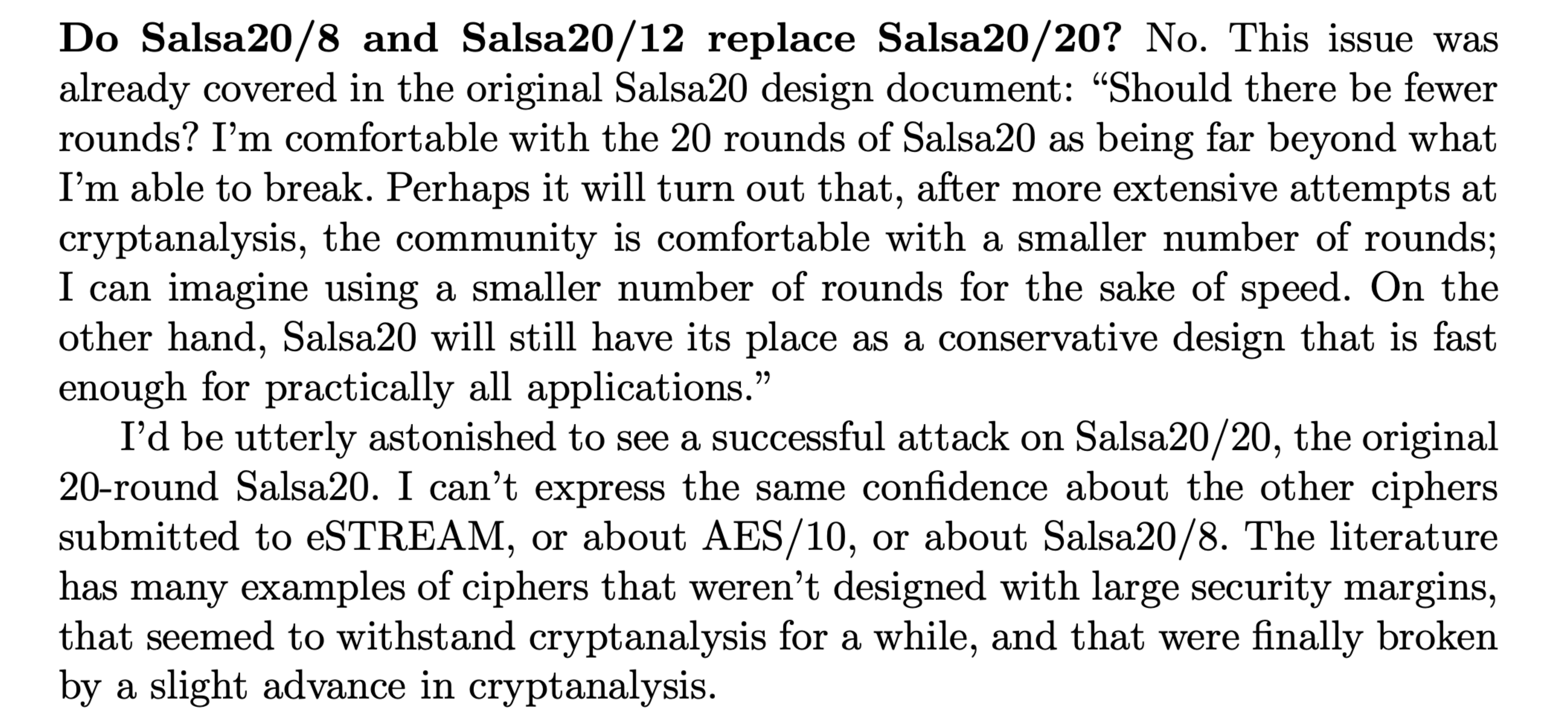
(Not perfect, numbers-free on purpose, just a model.)

# Correcting rounds

Few examples:

- Keccak’s **18** -> **24** (after 2^1000 “distinguisher”)
- Keccak: Kangaroo**12**, Marsupilami**14**, Kravatte (**6**,**4**)
- Salsa20/**12** (blessed by eSTREAM)

# How prudent should we be?



**Do Salsa20/8 and Salsa20/12 replace Salsa20/20?** No. This issue was already covered in the original Salsa20 design document: “Should there be fewer rounds? I’m comfortable with the 20 rounds of Salsa20 as being far beyond what I’m able to break. Perhaps it will turn out that, after more extensive attempts at cryptanalysis, the community is comfortable with a smaller number of rounds; I can imagine using a smaller number of rounds for the sake of speed. On the other hand, Salsa20 will still have its place as a conservative design that is fast enough for practically all applications.”

I’d be utterly astonished to see a successful attack on Salsa20/20, the original 20-round Salsa20. I can’t express the same confidence about the other ciphers submitted to eSTREAM, or about AES/10, or about Salsa20/8. The literature has many examples of ciphers that weren’t designed with large security margins, that seemed to withstand cryptanalysis for a while, and that were finally broken by a slight advance in cryptanalysis.

https://cr.yp.to/snuffle/812.pdf (2006)

# Our round correction proposal

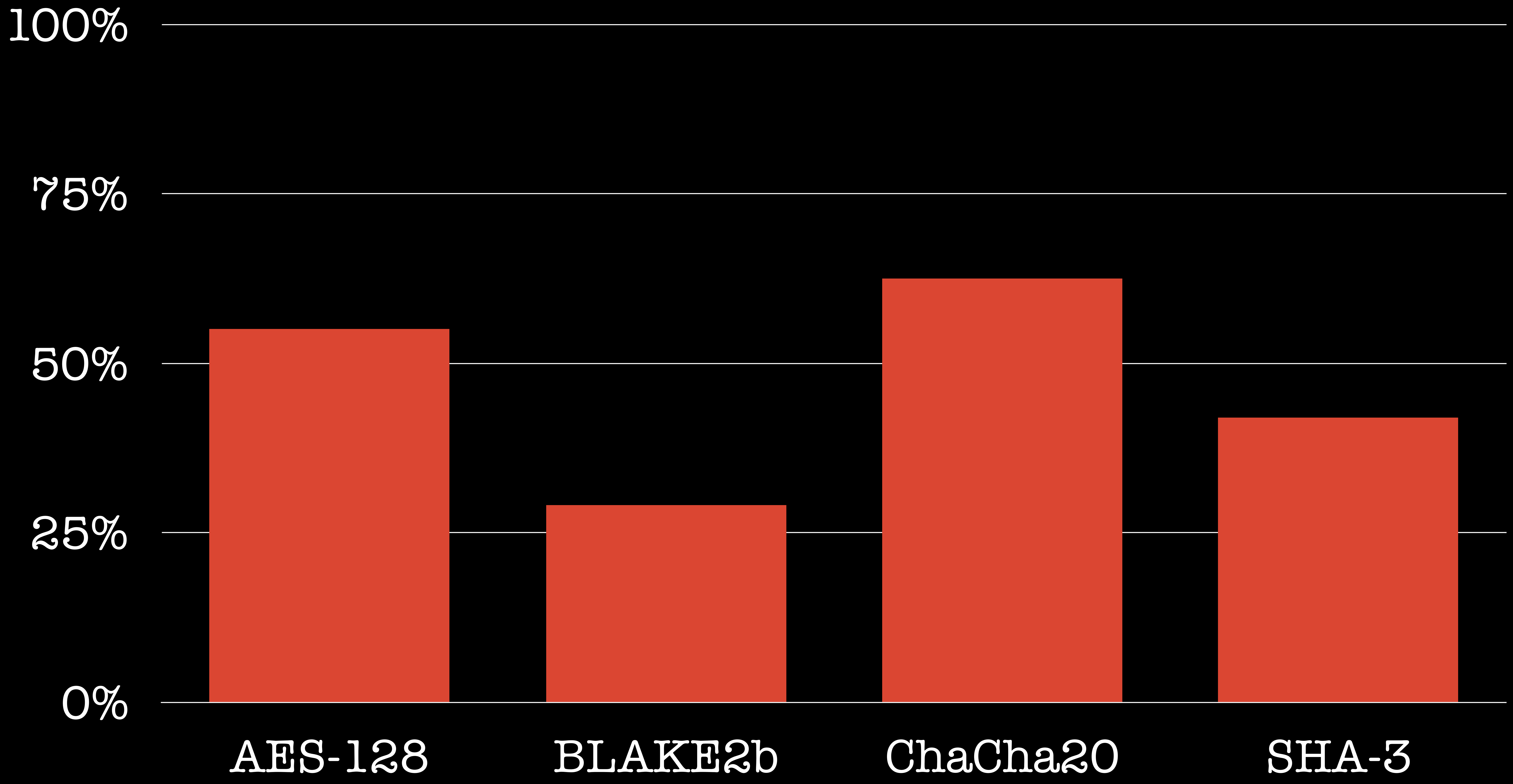
- **AES**: 9/10/11 instead of 10/12/14
  **1.1×, 1.2×, 1.3× speed-up**

- **BLAKE2**: 7/8 instead of 10/12
  **1.4×, 1.5× speed-up**

- **ChaCha**: 8 instead of 20
  **2.5× speed-up**

- **SHA-3**: 10 instead of 24
  **2.4× speed-up**

# Practically broken rounds with corrected round



4/3

# Objections (1/2)

**What if better attacks are found? Dangerous!**

Whatifs and FUD is not risk thinking, instead we should rely on data. Same argument holds for any number rounds. And what about attacks working for any number of rounds? :)

**Had we reduced the security margin of cipher XYZ 20 years ago, it would have been broken afterwards!**

I'm talking about AES, B2, ChaCha, SHA-3 in 2019, or the algorithms that were the most cryptanalyzed over about 20 years, with stagnating results despite sustained cryptanalysis. SHA-3 is more recent but its core is about as old as AES.

# Objections (2/2)

**Attacks do get better! Look, SHA-1 now!**

The collision and its recent refinements are incremental progresses of the 2004 attack (when SHA-1 was already on thin ice, despite attention focused on block ciphers late 90s).

**See the effort/time it took to make such refinements? If there exists better attacks, it'll be even harder to find them**

That's a possibility, but empirical data suggests this won't happen

**Your proposed rounds correction isn't sound because (…)**

You may be right, happy to see counter-proposals!

# Conclusions

Fewer rounds wouldn't be less safe, according to reasonable risk metrics, calling for:

- New/revised standards
- Round correction in crypto competitions
- Implementations supporting faster versions

Lower energy consumption as a by-product 🌱

More in the paper @ https://eprint.iacr.org

Thanks to Samuel Neves and other listed reviewers