Too much crypto™ II

JP Aumasson

TAURUS

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Energie: Massnahmen für den Fall einer Strommangellage gehen in Vernehmlassung

Bern, 23.11.2022 - Der Bundesrat hat an seiner Sitzung vom 23. November 2022 die Bewirtschaftungsmassnahmen für den Fall einer schweren Strommangellage zur Kenntnis genommen. Die Verordnungsentwürfe, die Verwendungsbeschränkungen und Verbote, Sofortkontingentierung, Kontingentierung sowie Netzabschaltungen regeln, gehen bis zum 12. Dezember 2022 in eine verkürzte Vernehmlassung.

Énergie : mise en consultation des mesures prévues en cas de pénurie d'électricité

Berne, 23.11.2022 - Lors de sa séance du 23 novembre 2022, le Conseil fédéral a pris connaissance des mesures de gestion réglementée prévues en cas de pénurie grave d'électricité. Les projets d'ordonnance réglant les restrictions et interdictions d'utilisation, le contingentement immédiat et le contingentement ainsi que les délestages font l'objet d'une consultation raccourcie jusqu'au 12 décembre 2022.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Wenn der Strom knapp wird

Mögliche Massnahmen bei einer Strom-Mangellage

Stand: 23. November 2022

Je nach Strommenge, die eingespart werden muss, werden die Massnahmen einzeln oder kombiniert eingesetzt

Sparappelle (Aufruf zum Sparen)

Entscheidung: Delegierter der Wirtschaftlichen Landesversorgung (WL)
Betroffen: alle Verbraucher

Einschränkung oder Verbote nicht zwingend benötigter Geräte und Anlagen

Entscheidung: Bundesrat
Betroffen: je nach Situation sind folgende Schritte möglich:

- **1. Schritt:** z.B. Maximale Temperatur für Waschmaschinen in privaten Haushalten, Beleuchtungen zu Werbezwecken zwischen 23:00 und 05:00 Uhr verboten
- **2. Schritt:** z.B. Maximale Heiztemperatur für öffentlich zugängliche Räume, Verbot von Beleuchtungen zu Werbezwecken
- **3. Schritt:** z.B. Ladenöffnungszeiten reduzieren, Verbot von Waschanlagen für Fahrzeuge

Kontingentierung

max
Entscheidung: Bundesrat
Vollzug: OSTRAL*
Betroffen: Grossverbraucher

- **4. Schritt:** z.B. Verbot des Betriebs von Sportanlagen, Verbot von Kulturveranstaltungen sofern elektrisch betrieben

Netzabschaltungen für einige Stunden

ultima ratio
Entscheidung: Bundesrat, Vollzug: OSTRAL*
Betroffen: alle Verbraucher

Quand l'électricité vient à manquer

Les mesures potentielles en cas de pénurie d'électricité

État au 23 novembre 2022

En fonction de la quantité d'électricité à économiser, les mesures peuvent être déployées de manière individuelle ou combinée

Appels à réduire la consommation

Décision : délégué à l'approvisionnement économique du pays
Acteurs visés : tous les consommateurs

Limitations ou interdictions frappant les appareils et installations non essentiels

Décision : Conseil fédéral
Activités visées : en fonction de la pénurie, les paliers suivants sont envisageables :

- **1er palier :** limitation de la température de lavage maximale des lave-linge dans les ménages privés, interdiction des éclairages publicitaires entre 23 heures et 5 heures, p. ex.
- **2e palier :** limitation de la température de chauffage maximale dans les pièces accessibles au public, interdiction d'éclairage à des fins publicitaires, p. ex.
- **3e palier :** réduction des horaires d'ouverture des magasins, interdiction d'utiliser les stations de lavage pour les véhicules, p. ex.

Contingentement

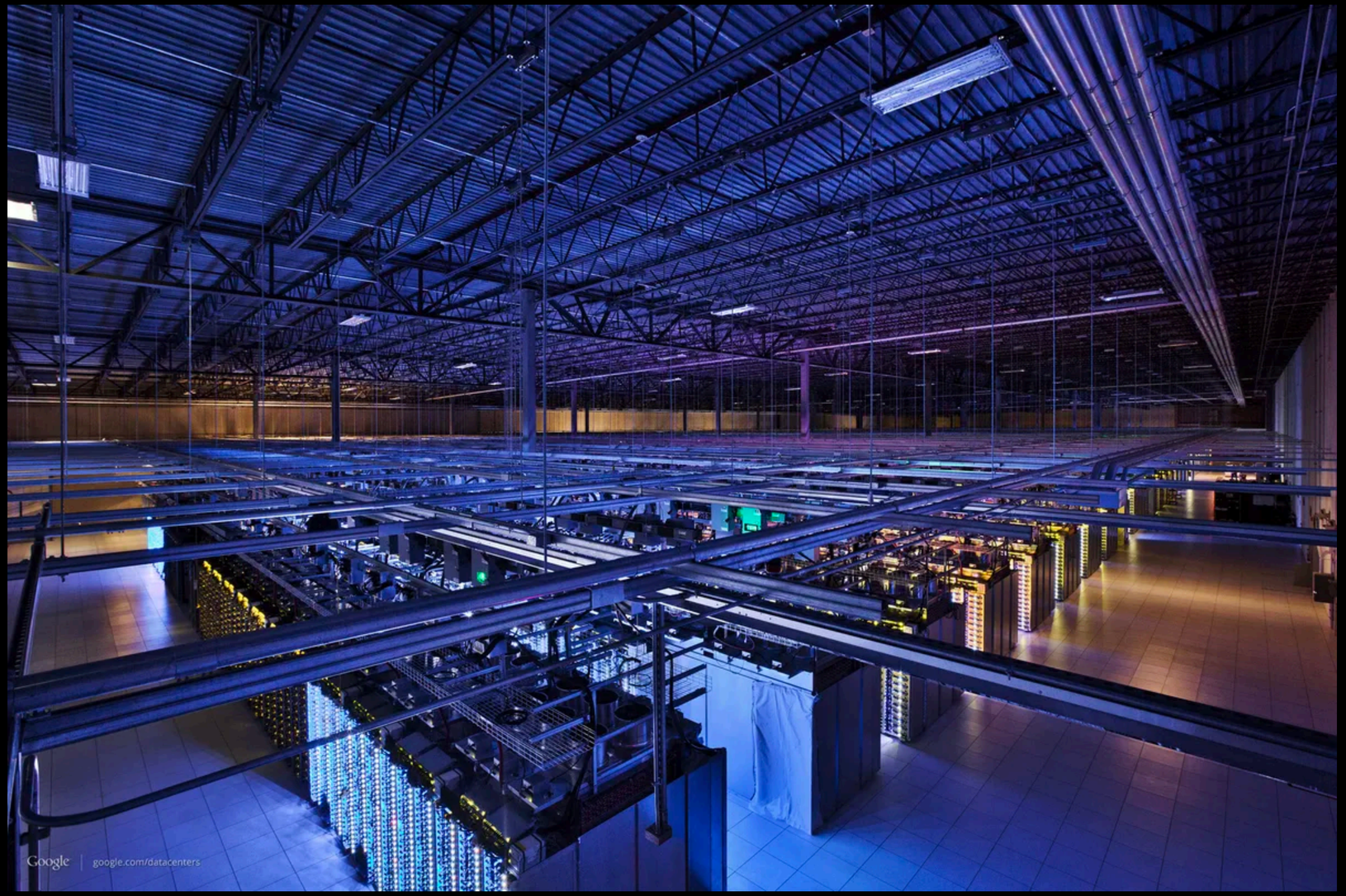
max
Décision : Conseil fédéral
Exécution : OSTRAL*
Acteurs visés : gros consommateurs

- **4e palier :** interdiction d'exploiter des installations sportives ou de réaliser des manifestations culturelles si elles utilisent de l'électricité, p. ex.

Délestages pour quelques heures

En dernier recours
Décision : Conseil fédéral, Exécution : OSTRAL*
Acteurs visés : tous les consommateurs


ПРЧ-2.46
11
125


Google | google.com/datacenters

Real World Crypto 2020, NYC

Too Much Crypto

Jean-Philippe Aumasson

Taurus, Switzerland

Abstract. We show that many symmetric cryptography primitives would not be less safe with significantly fewer rounds. To support this claim, we review the cryptanalysis progress in the last 20 years, examine the reasons behind the current number of rounds, and analyze the risk of doing fewer rounds. Advocating a rational and scientific approach to round numbers selection, we propose revised number of rounds for AES, BLAKE2, ChaCha, and SHA-3, which offer more consistent security margins across primitives and make them much faster, without increasing the security risk.

Symmetric cryptography does too much computation

It could achieve the same security with way fewer operations and less energy

Symmetric cryptography does too much computation

It could achieve the same security with way fewer operations and less energy

Because algorithms are overdesigned

Round numbers are initially set to a high number, precautionarily, but are never adjusted after we realise that fewer rounds would be sufficient

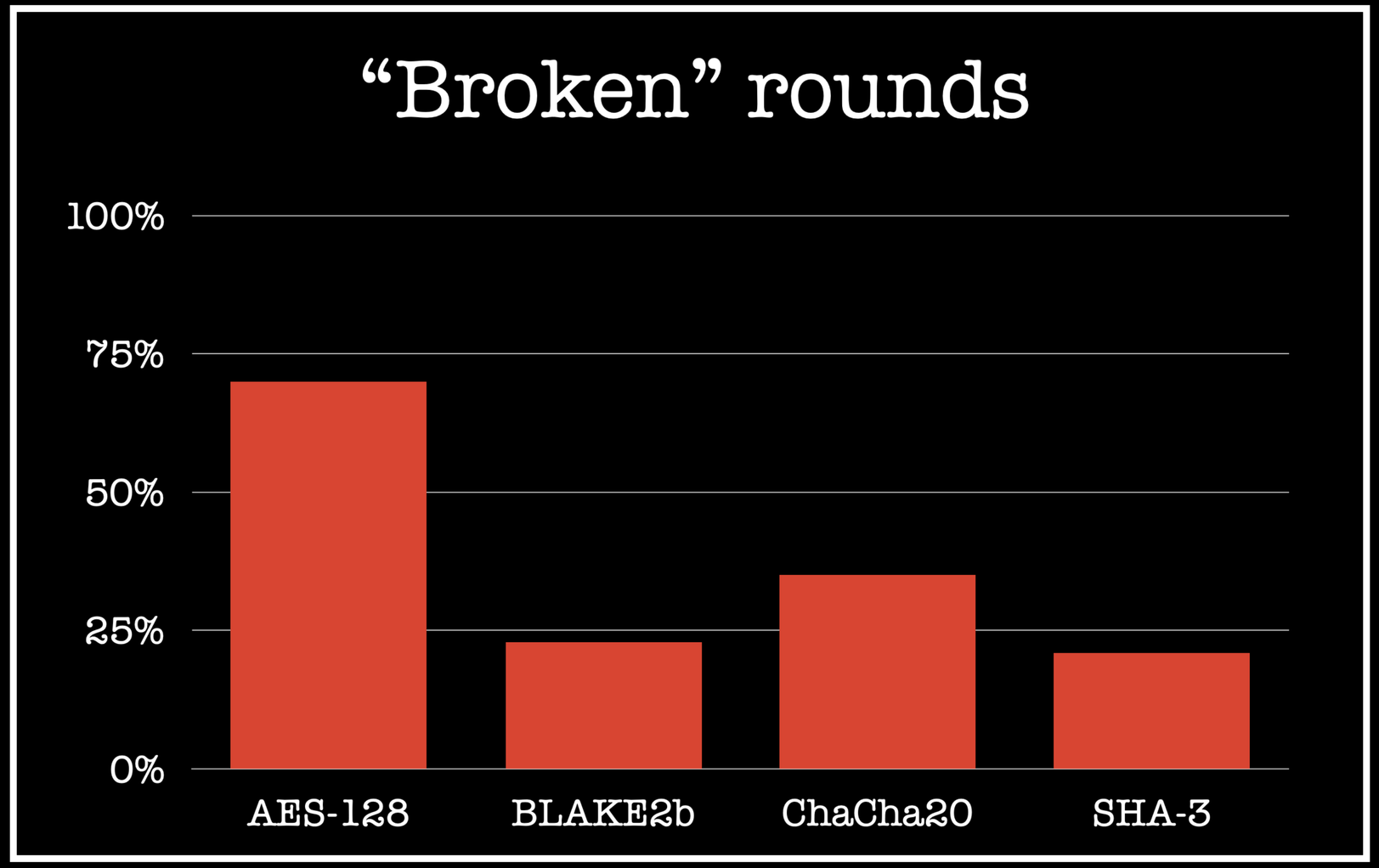
Symmetric cryptography does too much computation

It could achieve the same security with way fewer operations and less energy

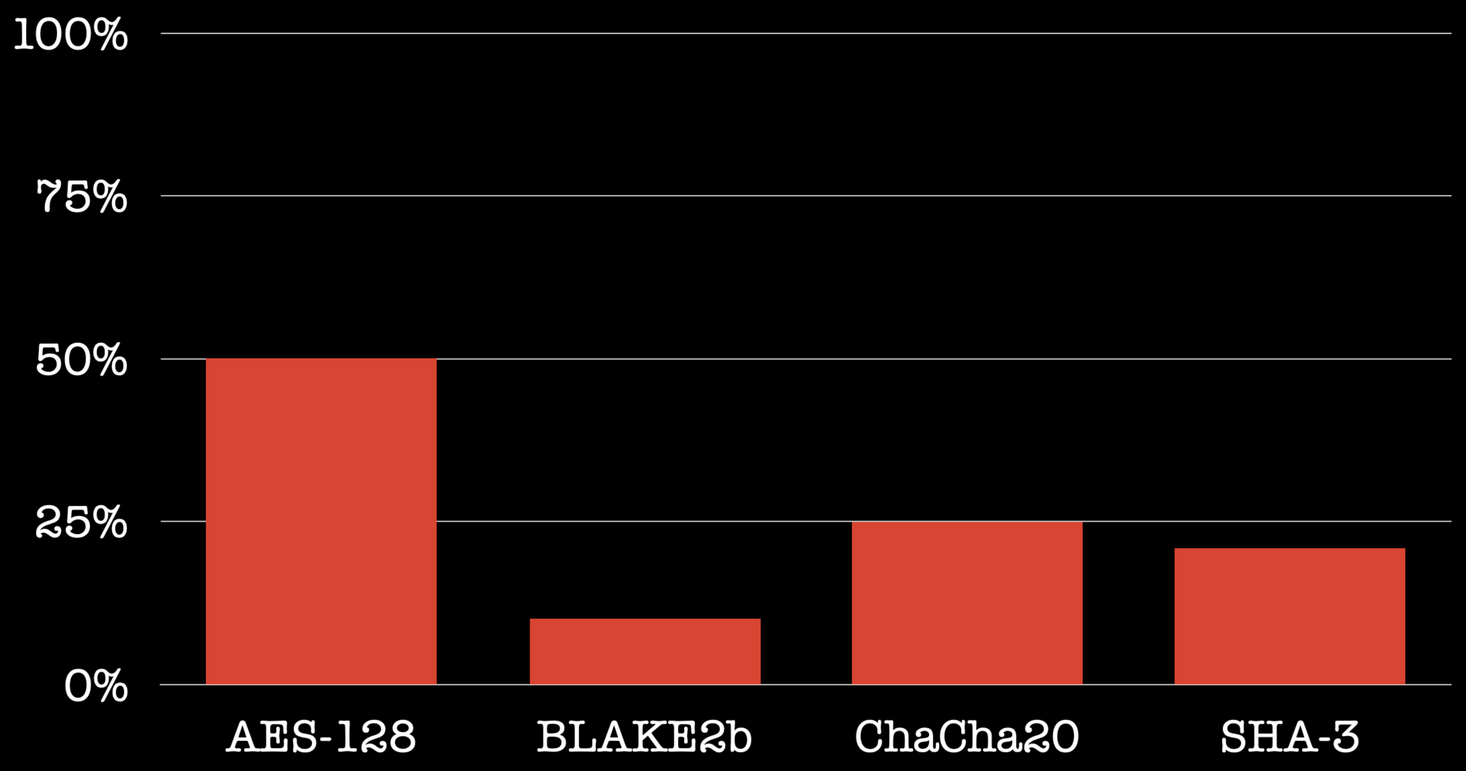
Because algorithms are overdesigned

Round numbers are initially set to a high number, precautionarily, but are never adjusted after we realise that fewer rounds would be sufficient

Due to imperfect selection processes, deployment costs, poor risk thinking


“Broken” rounds
100%
75%
50%
25%
0%
AES-128
BLAKE2b
ChaCha20
SHA-3

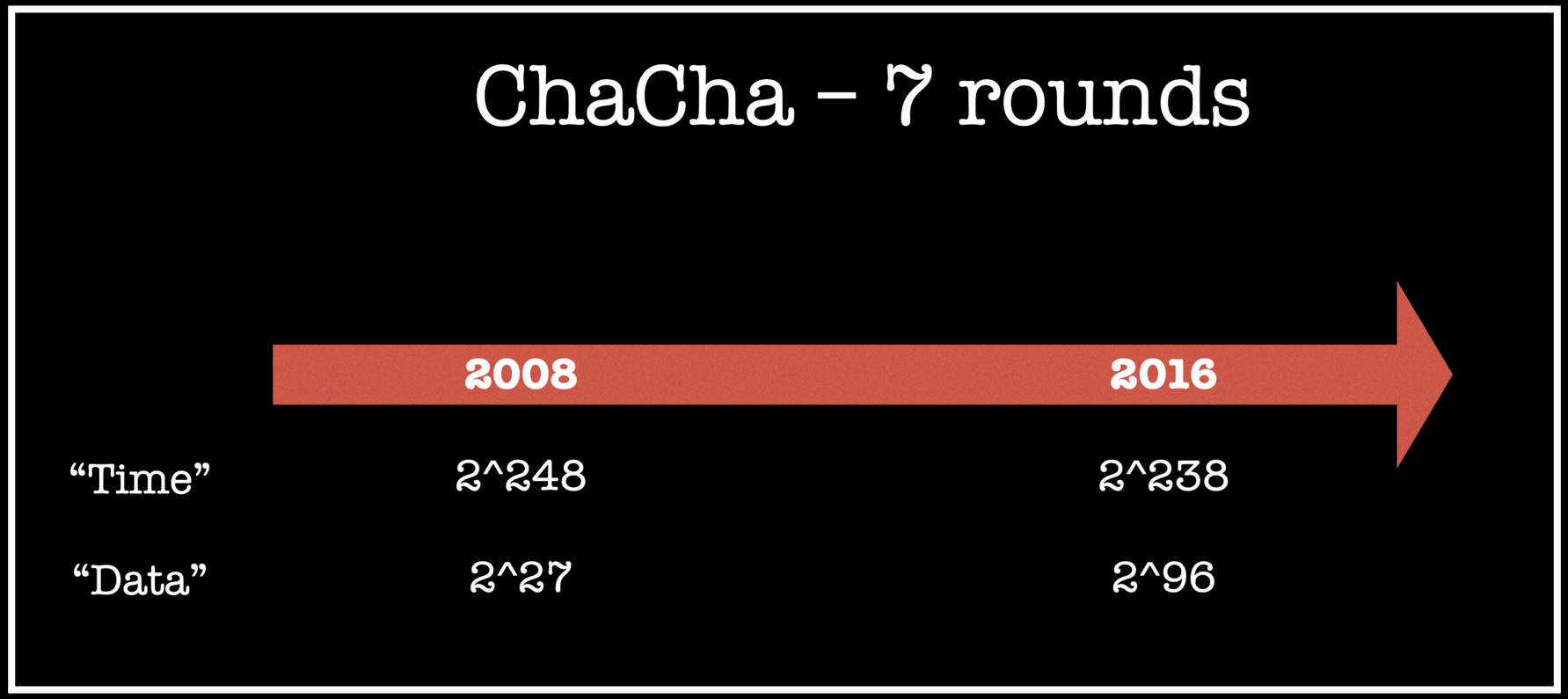
Practically broken rounds



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



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

In the real world, 128-bit security is enough, even 100 bits

Economic argument:

With the power/capability/time/means/budget to run a 2^{100} attack, you can do other, more effective things to compromise a system than break its crypto

My 2020 proposal:

Faster and less energy-hungry crypto

- **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

My 2020 proposal:

Faster and less energy-hungry crypto

Q4 2022 status:

No new attacks

Proposal still stands

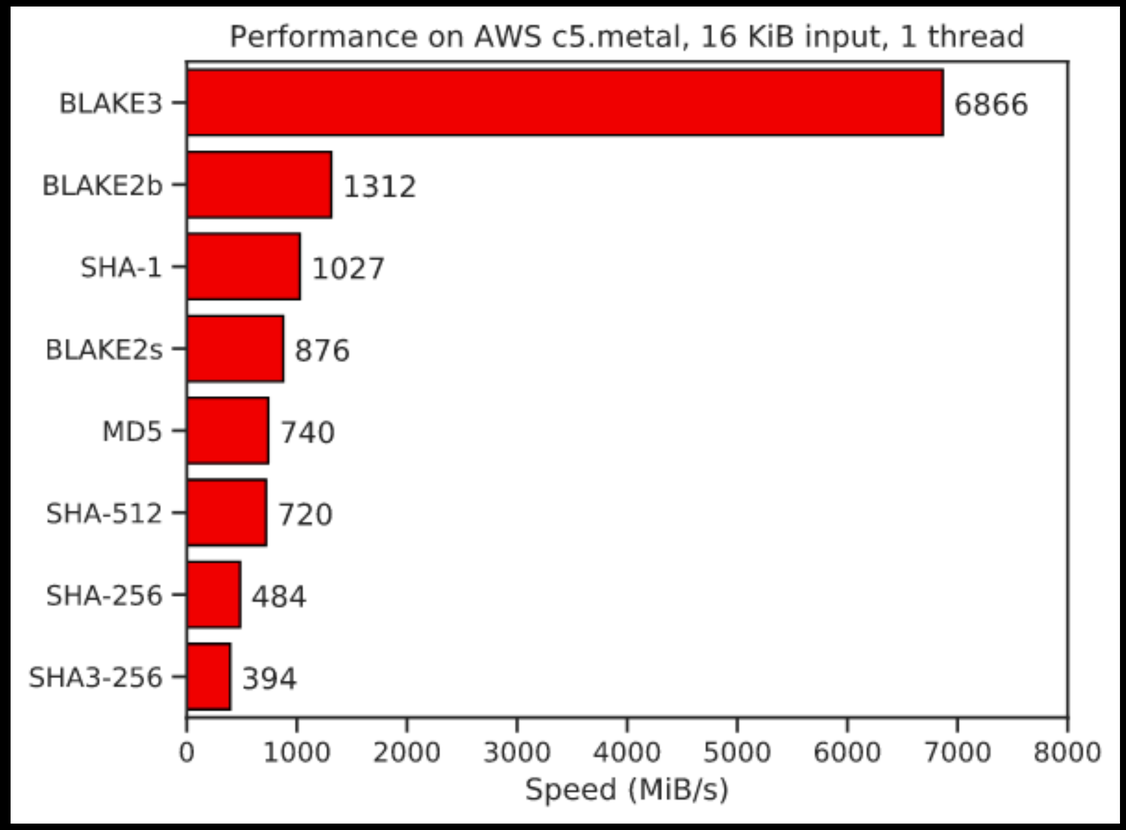
ChaCha8 gained popularity

- **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

The BLAKE3 hash/PRF/KDF

Based on 7-round BLAKE2

blake3.io



Too much ~~cryptocomputation~~ in blockchains

Proof of work

Too much ~~crypto~~computation in blockchains

Every program is recomputed multiple times

Hampers scalability, solved by "rollups"...

Too much crypto in ZK proof systems?

When general-purpose primitives are as arithmetic circuits (SHA2, BLAKE2, etc.)

-> Use ZK-friendly hash functions, like Poseidon

When a general-purpose crypto hash is superfluous

-> Use universal hash if sufficient

Too much crypto in ZK friendly hash functions?

Small changes can have a major speed/energy impact, because

-> Circuit transformation amplifies performance gains losses

-> Hashing is everywhere in ZKPs: Merkle trees, commitment schemes, Fiat-Shamir transforms, encryption, signature, etc.

Too much crypto in ZK friendly hash functions?

Small changes can have a major speed/energy impact, if we

-> Eliminate padding

-> Support only known-length input

-> Use an all-in-one primitive for hashing, encryption, randomness

safe-hash.dev

Upcoming: security proof

SAFE (Sponge API for Field Elements) – A Toolbox for ZK Hash Applications

Dmitry Khovratovich – *Ethereum Foundation and Dusk Network*
JP Aumasson – *Taurus and Inference*
Porçu Quine – *Lurk Lab and Protocol Labs*

We define a unified Sponge API for Field Elements (SAFE), which provides ZK proof systems designers with a secure and efficient framework for hashing, encryption, and applications thereof (commitment schemes, Fiat-Shamir transforms, AEAD, and so on). We do not restrict the permutation algorithm nor the field type, thus SAFE can be instantiated with established constructions.

SAFE is implemented by Filecoin's Neptune, which is our reference implementation (in Rust).

Don't Spill a Drop – SAFE Sponges in ZK Proofsystems

JP Aumasson[1], Dmitry Khovratovich[2], Bart Mennink[3], and Porçu Quine[4]

[1]Taurus SA and Inference AG
[2]Ethereum Foundation and Dusk Network
[3]Radboud University
[4]Lurk Lab and Protocol Labs

Too much conclusion

- Crypto standards will most likely keep doing way too much crypto
- More toomuchcrypto in Salsa/ChaCha-based TLS/SSH than in AES-based
- If you don't need a standard, ChaCha8 and BLAKE3 are fine
- ZKPs have more incentives (circuits cost & gas) to reduce crypto and are not stuck with standards and interoperability constraints yet

Much thanks!

JP

TAURUS