Keyak v2

Leakage-robust authenticated encryption

Guido Bertoni[1] Joan Daemen[1,2]
Michaël Peeters[1] Gilles Van Assche[1] Ronny Van Keer[1]

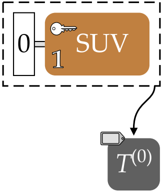
[1]STMicroelectronics

[2]Radboud University

CHES rump session
September 15, 2015

What is Keyak?

An authenticated-encryption scheme submitted to CAESAR
→ based on Keccak ←

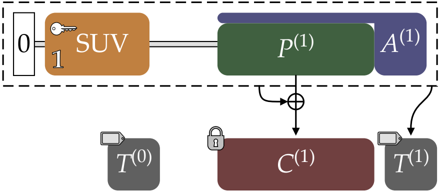


- SUV = Secret and Unique Value
- Works in *sessions*

What is Keyak?

An authenticated-encryption scheme submitted to CAESAR

→ based on Keccak ←

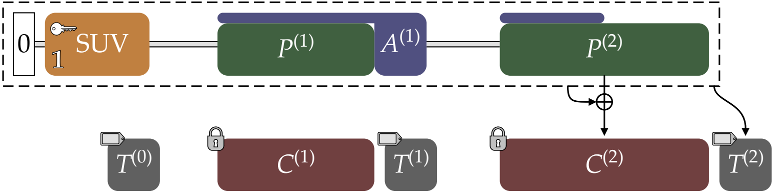


- SUV = Secret and Unique Value
- Works in *sessions*

What is Keyak?

An authenticated-encryption scheme submitted to CAESAR

→ based on Keccak ←

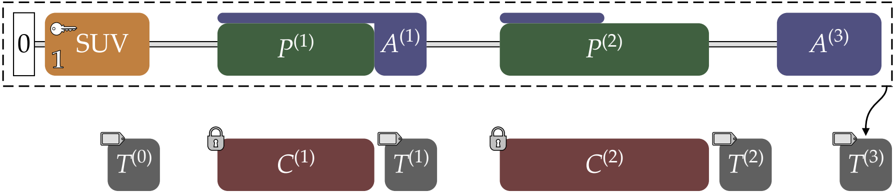


- SUV = Secret and Unique Value
- Works in *sessions*

What is Keyak?

An authenticated-encryption scheme submitted to CAESAR

→ based on Keccak ←



- SUV = Secret and Unique Value
- Works in *sessions*

What is new in Keyak v2?

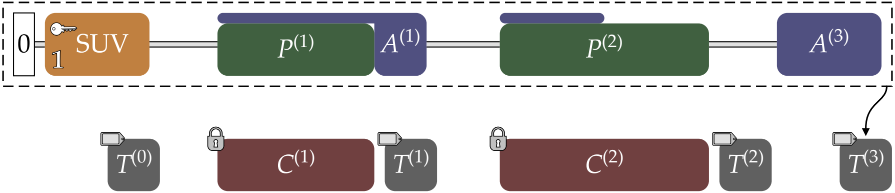
Full-state absorbing! [Mennink, Reyhanitabar and Vizár, 2015]

- More efficient for long messages
    - $\approx 2.25\times$ faster than SHAKE128 [FIPS 202]

Combined output usage (tag/keystream)

- More efficient for short messages
    - 12 rounds of Keccak-*f* per message

Why leakage robustness?



- Provided that **uniqueness** is enforced
- then ...
  - the secret state is a *moving target* [Taha, Schaumont, HOST 2014]

Where to find more information?

http://keyak.noekeon.org/