Shaking up Authenticated Encryption

Joan Daemen[1] Seth Hoffert Silvia Mella[1] Gilles Van Assche[2] Ronny Van Keer[2]

[1]Radboud University [2]STMicroelectronics

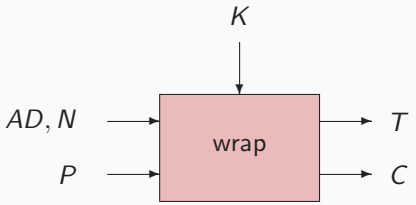
RWC 2025, Sofia, Bulgaria, March 26–28, 2025

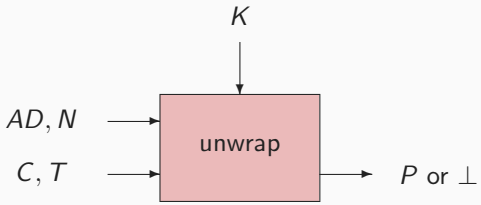
Radboud University

life.augmented

What?

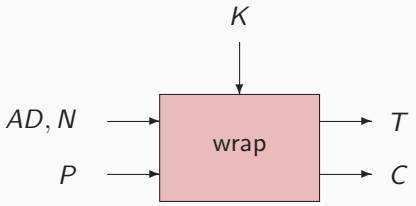
Authenticated encryption...

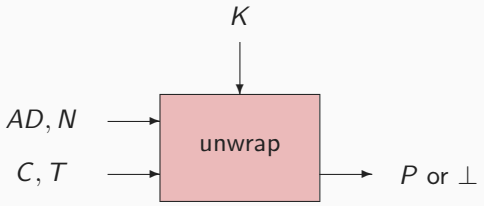




- wrap takes (K, N, AD, P) and returns C, T
- unwrap takes (K, N, AD, C, T) and returns P or error $\perp$

Authenticated encryption...



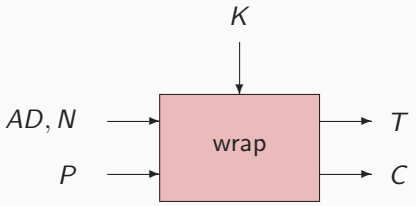


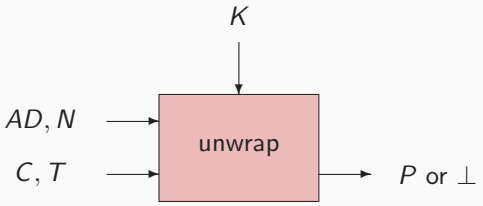
- wrap takes (K, N, AD, P) and returns C, T
- unwrap takes (K, N, AD, C, T) and returns P or error $\perp$

Ideally

- C looks random for each input
- unwrap of invalid ciphertext fails

Authenticated encryption...





- wrap takes (K, N, AD, P) and returns C, T
- unwrap takes (K, N, AD, C, T) and returns P or error $\perp$

Ideally

- C looks random for each input
- unwrap of invalid ciphertext fails

Examples

- AES-GCM, AES-CCM, Ascon-AEAD128, ChaCha20-Poly1305, and others

...on top of SHAKE and TurboSHAKE

...on top of SHAKE and TurboSHAKE

SHAKE128 and SHAKE256 [FIPS 202]

FIPS PUB 202

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions

CATEGORY: COMPUTER SECURITY SUBCATEGORY: CRYPTOGRAPHY

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.FIPS.202

August 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

...on top of SHAKE and TurboSHAKE

SHAKE128 and SHAKE256 [FIPS 202]

FIPS PUB 202

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions

CATEGORY: COMPUTER SECURITY SUBCATEGORY: CRYPTOGRAPHY

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.FIPS.202

August 2015

DEPARTMENT OF COMMERCE
UNITED STATES OF AMERICA

U.S. Department of Commerce
Penny Pritzker, Secretary

...on top of SHAKE and TurboSHAKE

SHAKE128 and SHAKE256 [FIPS 202]

- Sponge with KECCAK-p[**24 rounds**] [Bertoni et al., EUROCRYPT 2008]
- 15 years of public scrutiny $\Rightarrow$ 12 rounds give comfortable safety margin


FEDERAL INFORMATION PROCESSING STANDARDS

SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions

CATEGORY: COMPUTER SECURITY SUBCATEGORY: CRYPTOGRAPHY

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.FIPS.202

August 2015

DEPARTMENT OF COMMERCE
UNITED STATES OF AMERICA

U.S. Department of Commerce
Penny Pritzker, Secretary

...on top of SHAKE and TurboSHAKE

SHAKE128 and SHAKE256 [FIPS 202]

- Sponge with KECCAK-p[**24 rounds**] [Bertoni et al., EUROCRYPT 2008]
- 15 years of public scrutiny ⇒ 12 rounds give comfortable safety margin

TurboSHAKE128 and TurboSHAKE256

- Sponge with KECCAK-p[**12 rounds**] [Bertoni et al., ePrint 2023/342] + [RFC draft in the pipe]
- Same public scrutiny applies as all cryptanalysis is on reduced-round versions

...on top of SHAKE and TurboSHAKE

SHAKE128 and SHAKE256 [FIPS 202]

- Sponge with KECCAK-p[**24 rounds**] [Bertoni et al., EUROCRYPT 2008]
- 15 years of public scrutiny $\Rightarrow$ 12 rounds give comfortable safety margin

TurboSHAKE128 and TurboSHAKE256

- Sponge with KECCAK-p[**12 rounds**] [Bertoni et al., ePrint 2023/342] + [RFC draft in the pipe]
- Same public scrutiny applies as all cryptanalysis is on reduced-round versions

Security of (Turbo)SHAKE

- Unkeyed: flat sponge claim with security strength 128/256

...on top of SHAKE and TurboSHAKE

SHAKE128 and SHAKE256 [FIPS 202]

- Sponge with KECCAK-p[**24 rounds**] [Bertoni et al., EUROCRYPT 2008]
- 15 years of public scrutiny $\Rightarrow$ 12 rounds give comfortable safety margin

TurboSHAKE128 and TurboSHAKE256

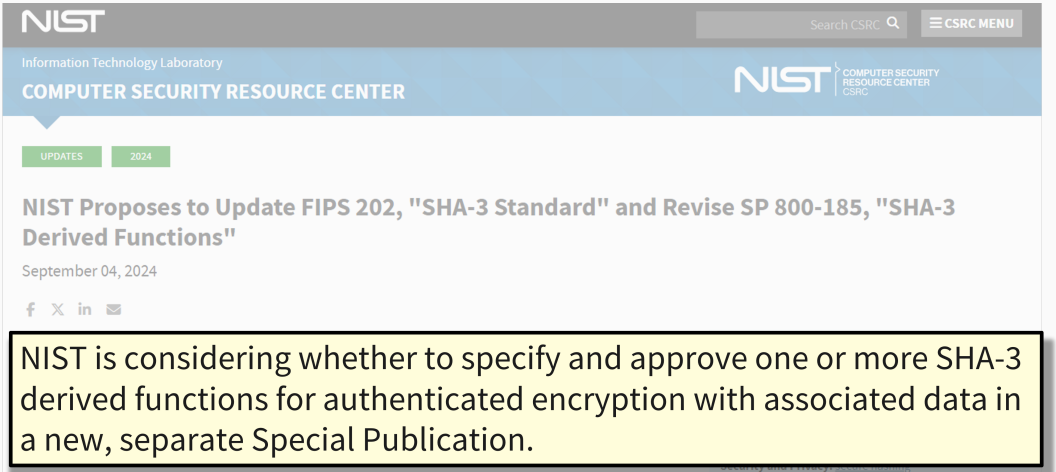
- Sponge with KECCAK-p[**12 rounds**] [Bertoni et al., ePrint 2023/342] + [RFC draft in the pipe]
- Same public scrutiny applies as all cryptanalysis is on reduced-round versions

Security of (Turbo)SHAKE

- Unkeyed: flat sponge claim with security strength 128/256
- Keyed:
  - When input to (Turbo)SHAKE is prefixed with a secret key K ...
  - ... it is hard to distinguish from a random oracle

Why?

NIST Publication Review Initiative



NIST

Search CSRC

CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

UPDATES 2024

NIST Proposes to Update FIPS 202, "SHA-3 Standard" and Revise SP 800-185, "SHA-3 Derived Functions"

September 04, 2024

NIST is considering whether to specify and approve one or more SHA-3 derived functions for authenticated encryption with associated data in a new, separate Special Publication.

NIST proposes to update FIPS 202 to improve its editorial quality. For example, text about SHA-1 and Triple DES will be edited to reflect the withdrawal of those techniques, as suggested in the public comments.

NIST proposes to revise SP 800-185 to provide "streaming" specifications of the two extendable output functions (XOFs) SHAKE128 and SHAKE256, to support implementations in which the length of the data output and the complete data input are not necessarily available before the XOF is called.

The public comments included suggestions that NIST specify and approve several other SHA-3 derived functions. NIST is considering

Activities and Products: standards development

RELATED PAGES

News Item: NIST Requests Public Comments on FIPS 202 and SP 800-185

News Item: Decision to Update FIPS 202 and Revise SP 800-

Public Comments

From https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/decision-proposal-comments/fips202-sp800-185-decision-proposal-comments-2024.pdf

Public Comments

From https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/decision-proposal-comments/fips202-sp800-185-decision-proposal-comments-2024.pdf

> We support NIST's plans to specify and approve additional SHA-3 derived functions, including those for authenticated encryption with associated data.

Public Comments

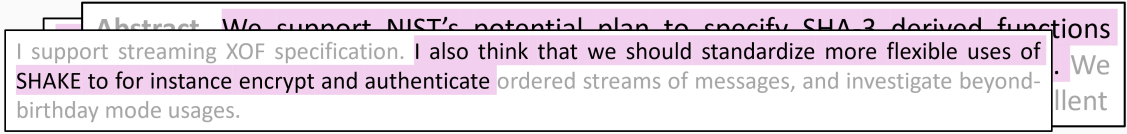
From https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/decision-proposal-comments/fips202-sp800-185-decision-proposal-comments-2024.pdf

W
th

Abstract. We support NIST's potential plan to specify SHA-3 derived functions ("Keccak Modes") for Authenticated Encryption with Associated Data (AEAD). We offer security and performance arguments for a Keccak-based AEAD as an excellent

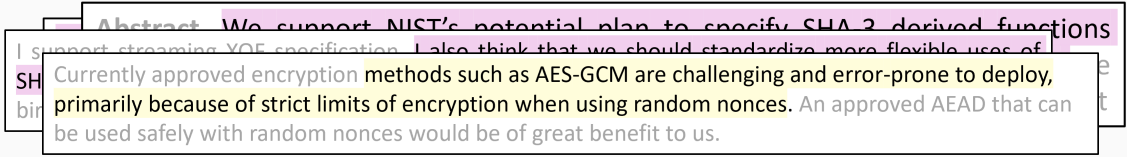
Public Comments

From https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/decision-proposal-comments/fips202-sp800-185-decision-proposal-comments-2024.pdf



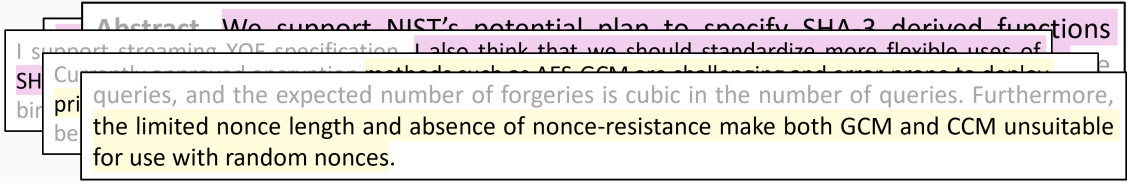
Public Comments

From https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/decision-proposal-comments/fips202-sp800-185-decision-proposal-comments-2024.pdf



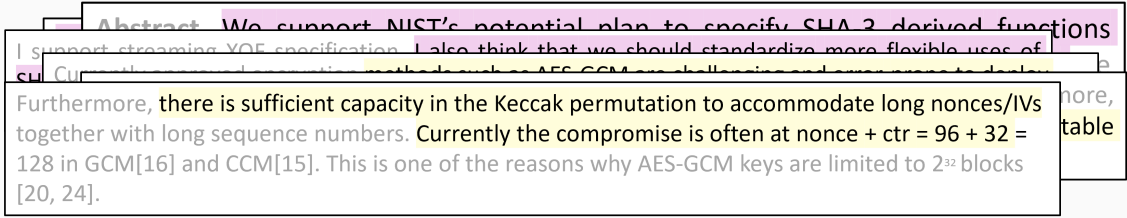
Public Comments

From https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/decision-proposal-comments/fips202-sp800-185-decision-proposal-comments-2024.pdf



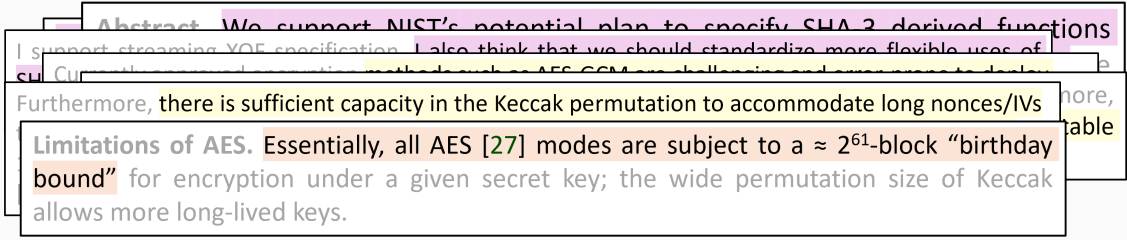
Public Comments

From https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/decision-proposal-comments/fips202-sp800-185-decision-proposal-comments-2024.pdf



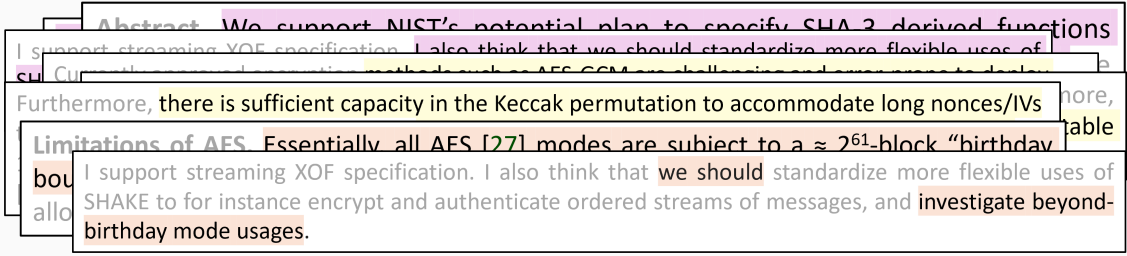
Public Comments

From https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/decision-proposal-comments/fips202-sp800-185-decision-proposal-comments-2024.pdf



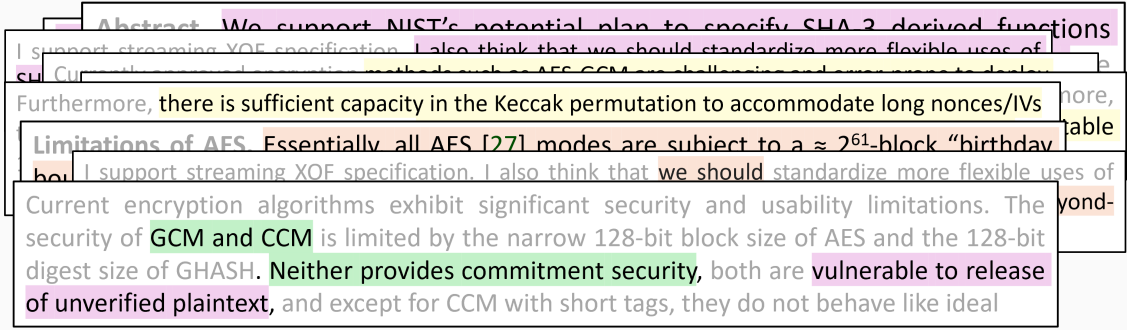
Public Comments

From https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/decision-proposal-comments/fips202-sp800-185-decision-proposal-comments-2024.pdf



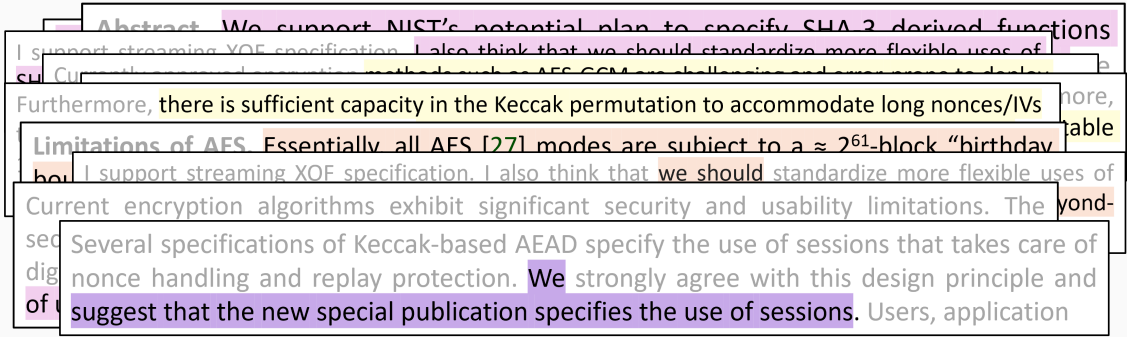
Public Comments

From https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/decision-proposal-comments-2024.pdf



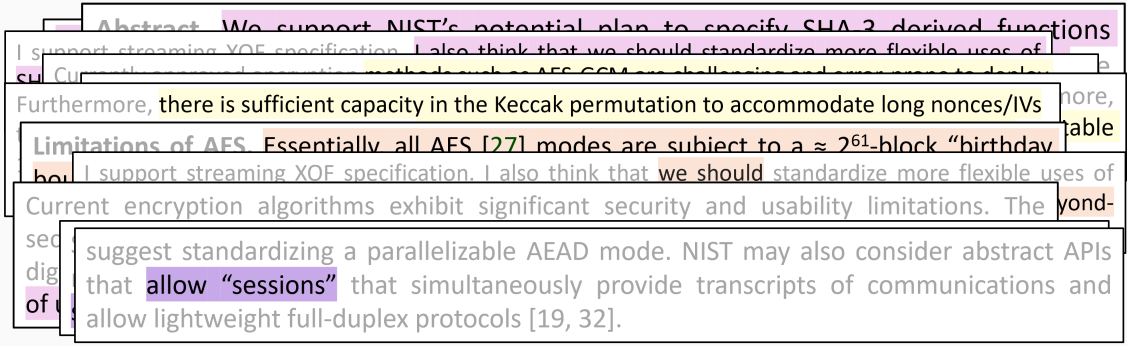
Public Comments

From https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/decision-proposal-comments-2024.pdf



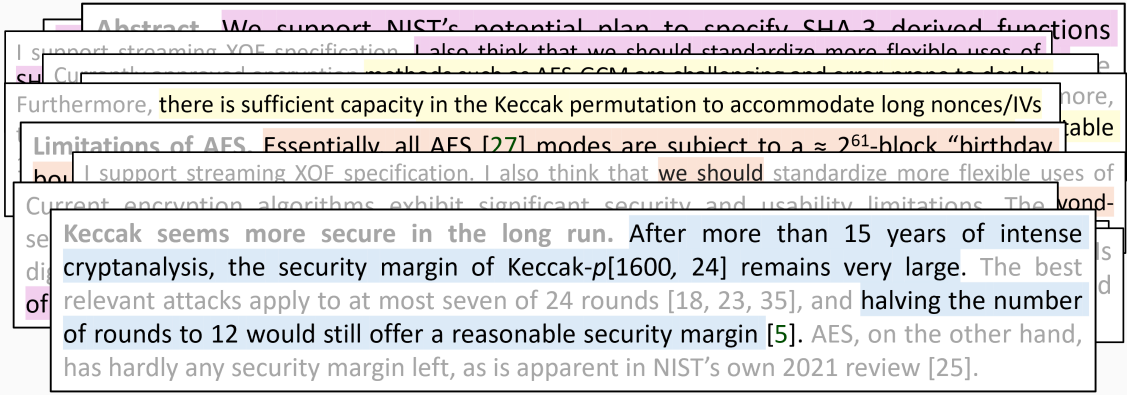
Public Comments

From https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/decision-proposal-comments-2024.pdf



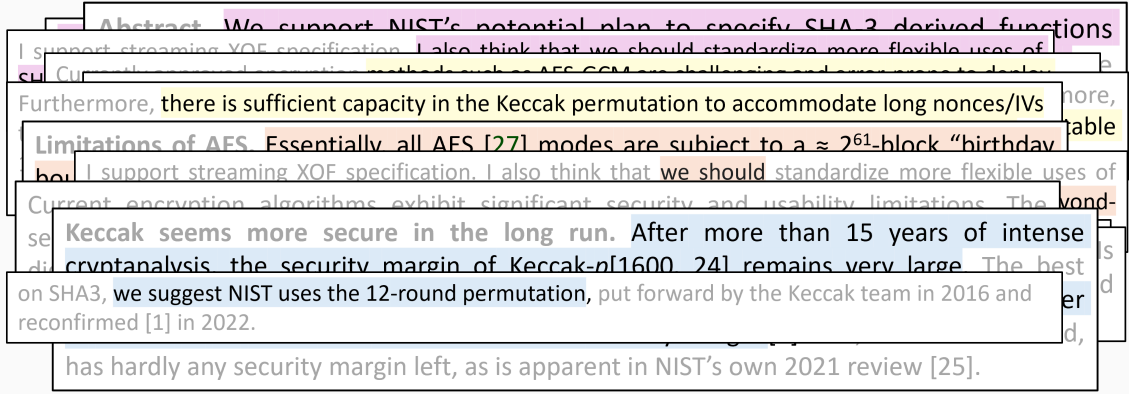
Public Comments

From https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/decision-proposal-comments/fips202-sp800-185-decision-proposal-comments-2024.pdf



Public Comments

From https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/decision-proposal-comments/fips202-sp800-185-decision-proposal-comments-2024.pdf



Public Comments

From https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/decision-proposal-comments/fips202-sp800-185-decision-proposal-comments-2024.pdf

Abstract. We support NIST's potential plan to specify SHA-3 derived functions

I support streaming XOF specification. I also think that we should standardize more flexible uses of

Furthermore, there is sufficient capacity in the Keccak permutation to accommodate long nonces/IVs

Limitations of AES. Essentially, all AES [27] modes are subject to a $\approx 2^{61}$-block "birthday

I support streaming XOF specification. I also think that we should standardize more flexible uses of

Current encryption algorithms exhibit significant security and usability limitations. The

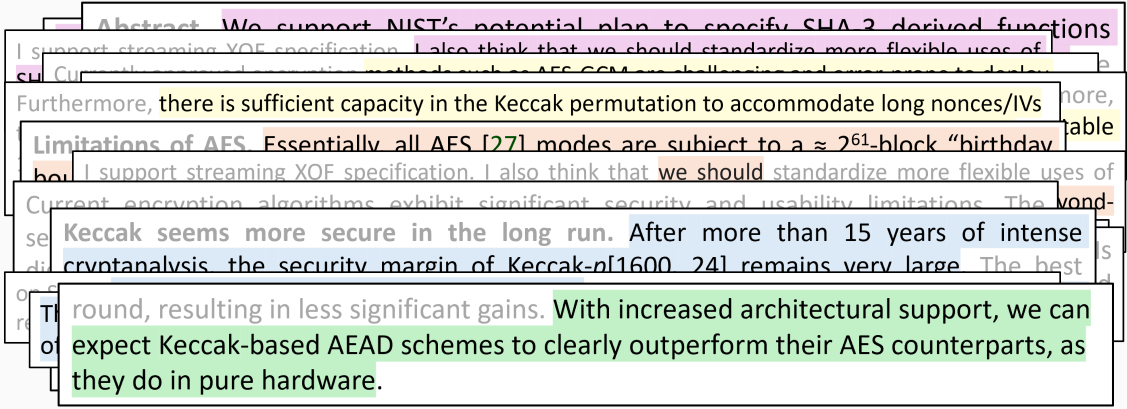
Keccak seems more secure in the long run. After more than 15 years of intense cryptanalysis, the security margin of Keccak-*p*[1600, 24] remains very large. The best

There is broad agreement that the number of rounds in FIPS 202 is too high by at least a factor of two. (1 2).

has hardly any security margin left, as is apparent in NIST's own 2021 review [23].

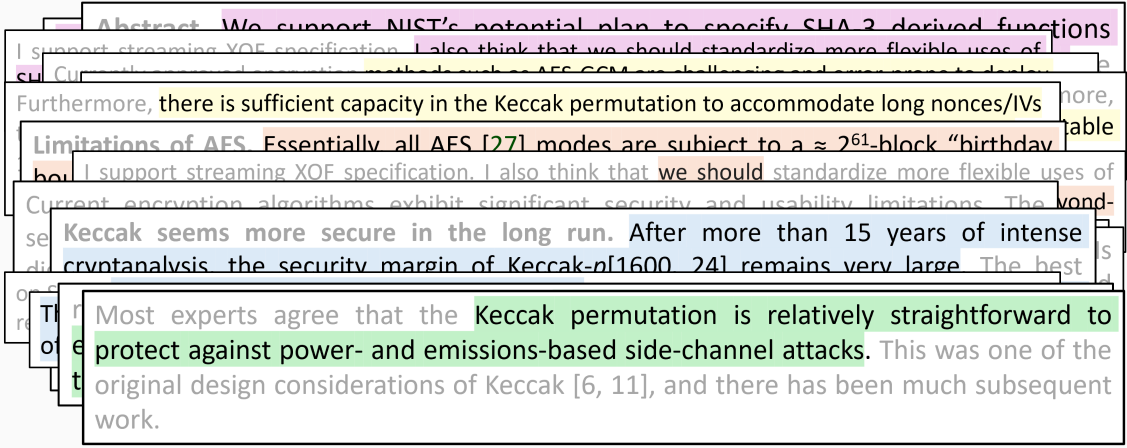
Public Comments

From https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/decision-proposal-comments/fips202-sp800-185-decision-proposal-comments-2024.pdf



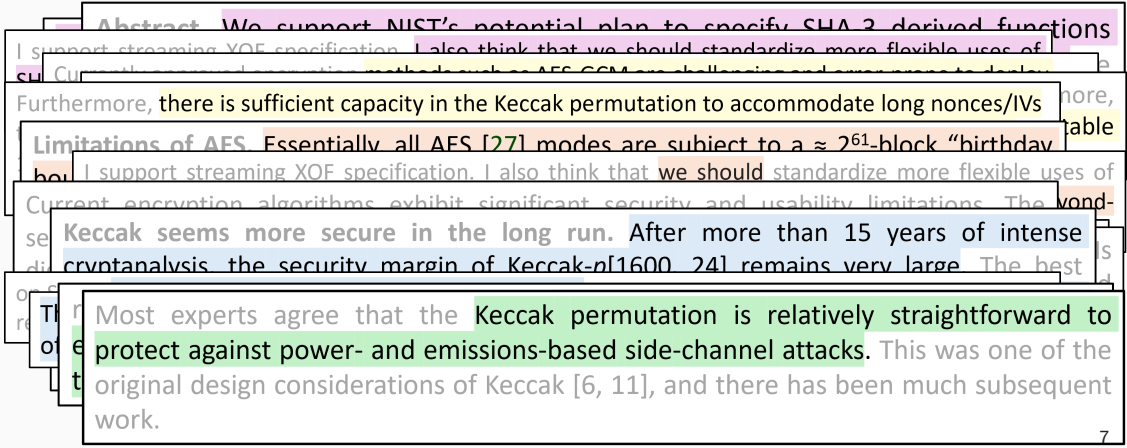
Public Comments

From https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/decision-proposal-comments/fips202-sp800-185-decision-proposal-comments-2024.pdf



Public Comments

From https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/decision-proposal-comments/fips202-sp800-185-decision-proposal-comments-2024.pdf



Summary of desired properties

Summary of desired properties

- Long nonce and nonce-resistance

Summary of desired properties

- Long nonce and nonce-resistance
- Beyond 2^{64} birthday bound

Summary of desired properties

- Long nonce and nonce-resistance
- Beyond 2^{64} birthday bound
- Committing security

Summary of desired properties

- Long nonce and nonce-resistance
- Beyond 2^{64} birthday bound
- Committing security
- Security against release of unverified plaintext

Summary of desired properties

- Long nonce and nonce-resistance
- Beyond 2^{64} birthday bound
- Committing security
- Security against release of unverified plaintext
- Support for sessions

Summary of desired properties

- Long nonce and nonce-resistance
- Beyond 2^{64} birthday bound
- Committing security
- Security against release of unverified plaintext
- Support for sessions
- Faster than SHAKE

How?

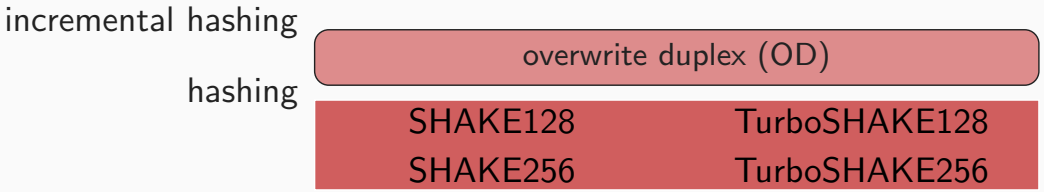
How we do it

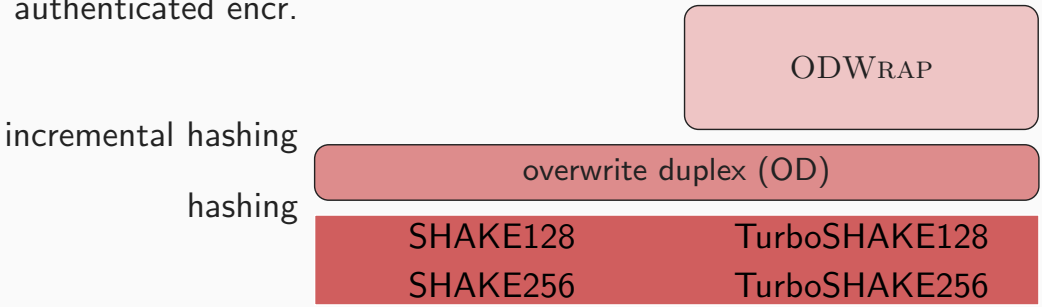
How we do it

hashing

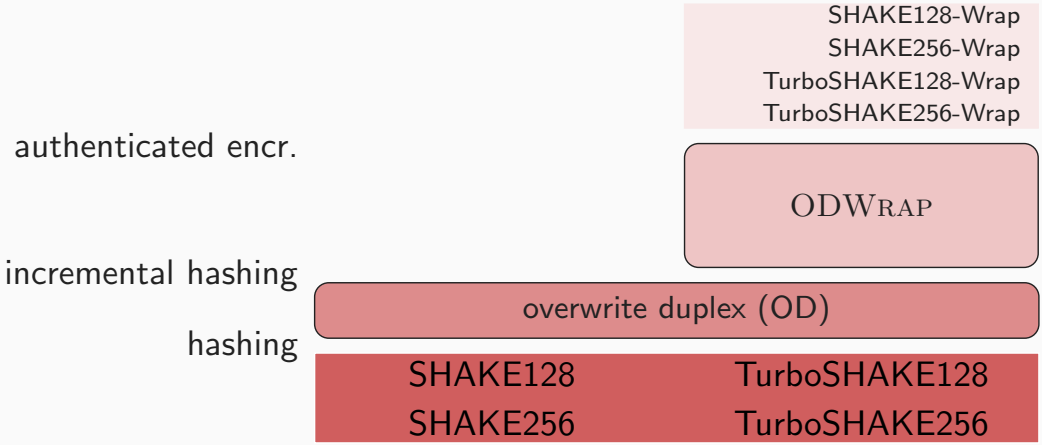
SHAKE128	TurboSHAKE128
SHAKE256	TurboSHAKE256

How we do it

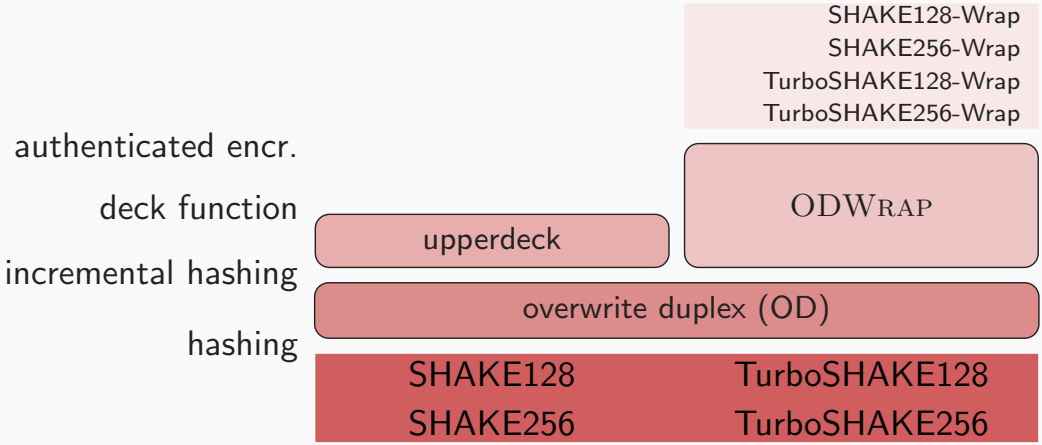

incremental hashing
overwrite duplex (OD)
hashing
SHAKE128
TurboSHAKE128
SHAKE256
TurboSHAKE256


authenticated encr.
ODWrap
incremental hashing
overwrite duplex (OD)
hashing
SHAKE128
SHAKE256
TurboSHAKE128
TurboSHAKE256

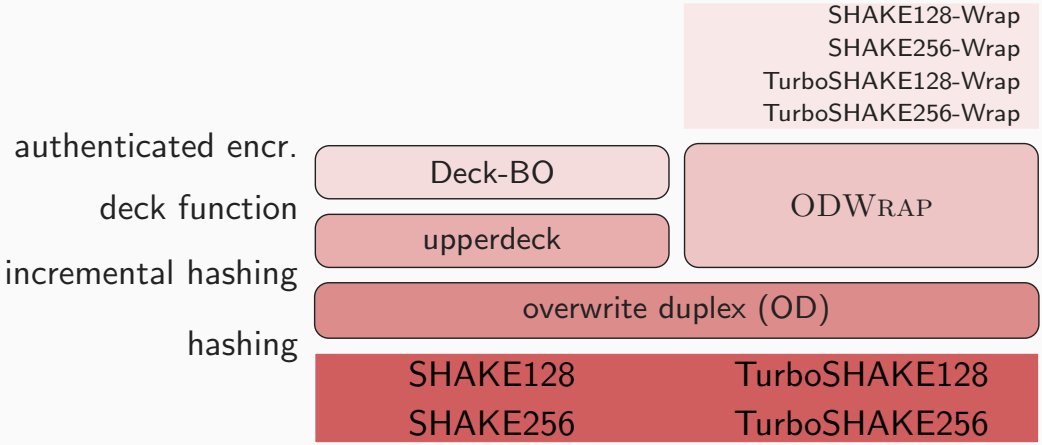
How we do it


SHAKE128-Wrap
SHAKE256-Wrap
TurboSHAKE128-Wrap
TurboSHAKE256-Wrap
authenticated encr.
ODWrap
incremental hashing
overwrite duplex (OD)
hashing
SHAKE128
TurboSHAKE128
SHAKE256
TurboSHAKE256

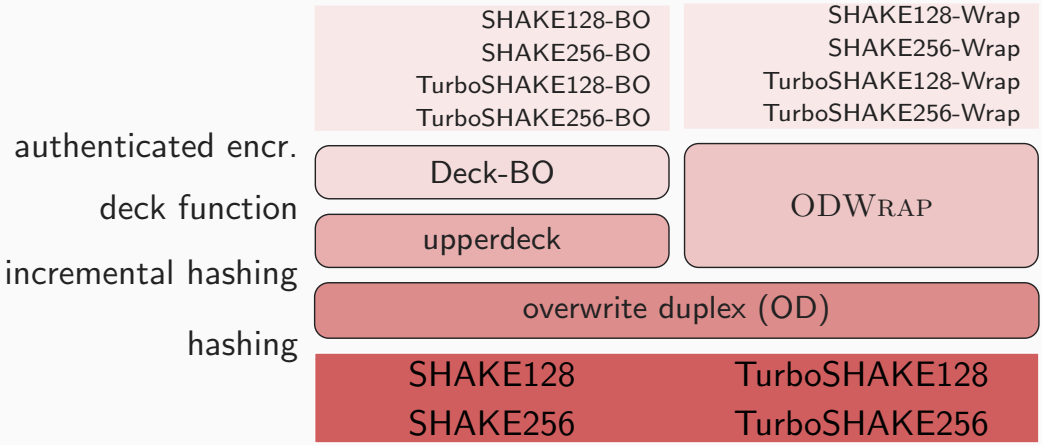
How we do it


SHAKE128-Wrap
SHAKE256-Wrap
TurboSHAKE128-Wrap
TurboSHAKE256-Wrap
authenticated encr.
deck function
incremental hashing
hashing
ODWrap
upperdeck
overwrite duplex (OD)
SHAKE128
SHAKE256
TurboSHAKE128
TurboSHAKE256

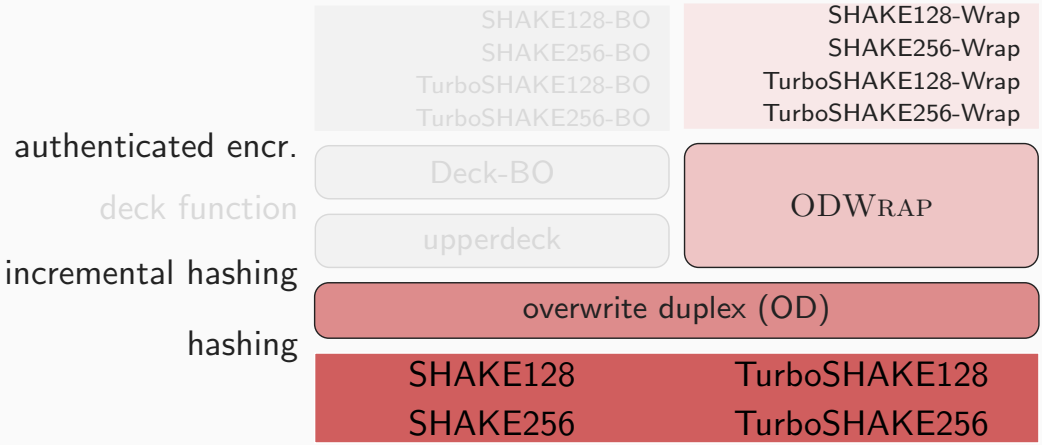
How we do it


SHAKE128-Wrap
SHAKE256-Wrap
TurboSHAKE128-Wrap
TurboSHAKE256-Wrap
authenticated encr.
deck function
incremental hashing
hashing
Deck-BO
upperdeck
ODWrap
overwrite duplex (OD)
SHAKE128
SHAKE256
TurboSHAKE128
TurboSHAKE256

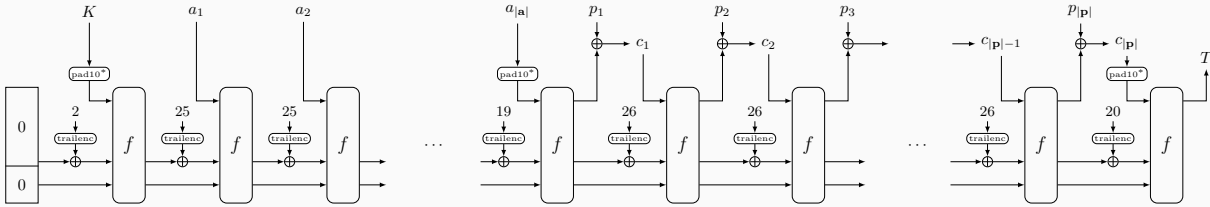
How we do it


SHAKE128-BO
SHAKE256-BO
TurboSHAKE128-BO
TurboSHAKE256-BO
SHAKE128-Wrap
SHAKE256-Wrap
TurboSHAKE128-Wrap
TurboSHAKE256-Wrap
authenticated encr.
deck function
incremental hashing
hashing
Deck-BO
ODWrap
upperdeck
overwrite duplex (OD)
SHAKE128
SHAKE256
TurboSHAKE128
TurboSHAKE256

Duplex-based authenticated encryption

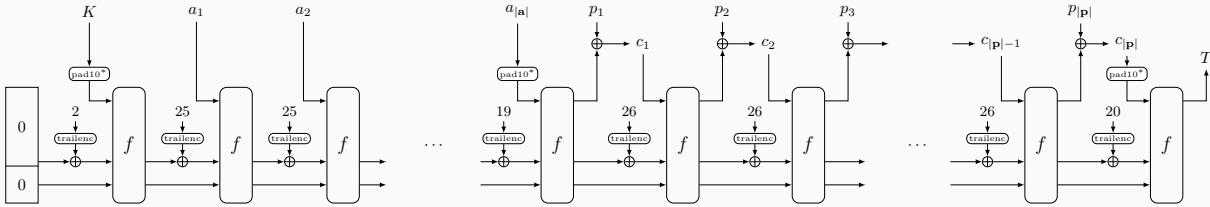


(Turbo)SHAKE-Wrap: nonce-based AE with sessions



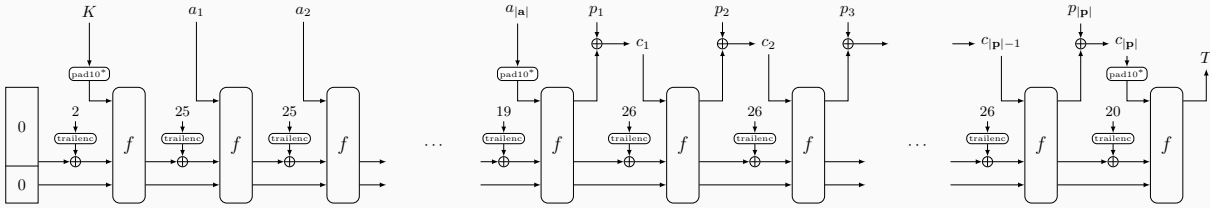
- Duplex-based mode similar to SpongeWrap [Bertoni et al., SAC 2011]
  - First AD of a session to be a nonce

(Turbo)SHAKE-Wrap: nonce-based AE with sessions



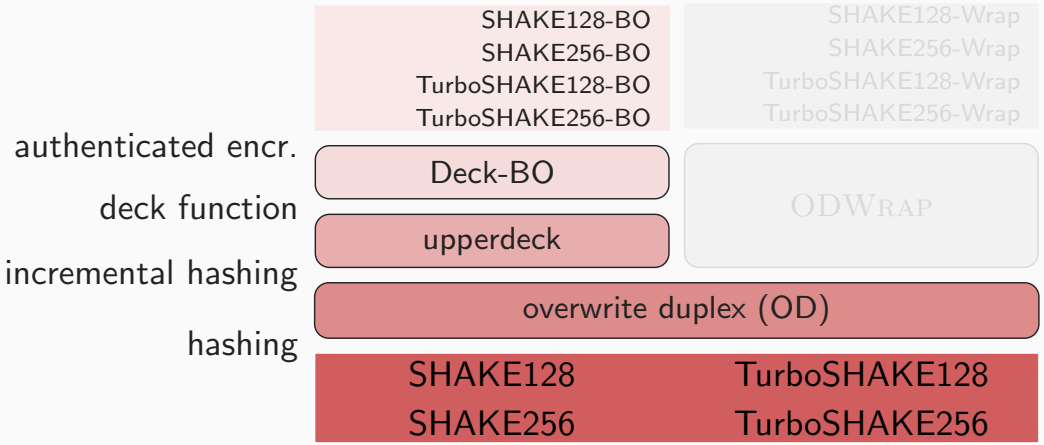
- Duplex-based mode similar to SpongeWrap [Bertoni et al., SAC 2011]
  - First AD of a session to be a nonce
- Confidentiality and integrity ⇐ PRF security of keyed (Turbo)SHAKE

(Turbo)SHAKE-Wrap: nonce-based AE with sessions

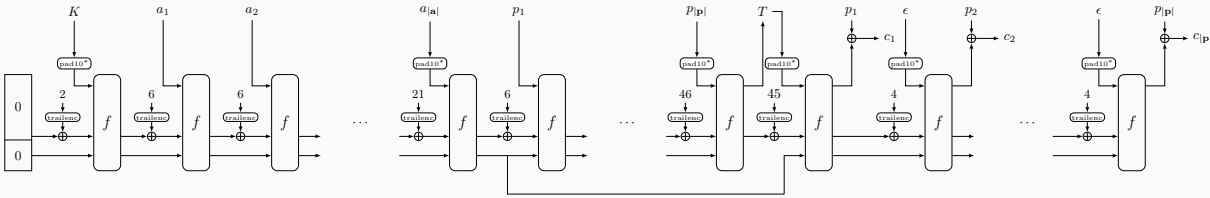


- Duplex-based mode similar to SpongeWrap [Bertoni et al., SAC 2011]
  - First AD of a session to be a nonce
- Confidentiality and integrity ⇐ PRF security of keyed (Turbo)SHAKE
- Committing security ⇐ collision resistance of (Turbo)SHAKE

Deck-based authenticated encryption



(Turbo)SHAKE-BO: SIV-type AE with sessions



- Based on Deck-BO [Băcuieti et al., ASIACRYPT 2022]
  - A session-supporting version of Synthetic Initialization Value (SIV) AE modes
  - Does not require a nonce
- Confidentiality and integrity ⇐ PRF security of keyed (Turbo)SHAKE
- Committing security ⇐ collision resistance of (Turbo)SHAKE

Features

Solution	Security strength	Nonce-misuse resistance	Session support	Committing security
(Turbo)SHAKE128-Wrap	128 bits	no	yes	128 bits
(Turbo)SHAKE256-Wrap	256 bits	no	yes	256 bits
(Turbo)SHAKE128-BO	128 bits	yes	yes	128 bits
(Turbo)SHAKE256-BO	256 bits	yes	yes	256 bits
Ascon-AEAD128	128 bits	no	no	64 bits
ChaCha20-Poly1305	106 bits	**no**	no	no
AES128-GCM	64 bits	**no**	no	no
AES128-GCM-SIV	64 bits	yes	no	no

Table: Comparison with standard AE

Performance (fully software)

	...-Wrap	...-BO	
		AD	P or C
TurboSHAKE128	3.33	3.04	6.23
TurboSHAKE256	4.06	3.84	7.82
SHAKE128	6.41	6.27	12.58
SHAKE256	8.07	7.80	15.72
ChaCha20-Poly1305	3.72		
AES128-GCM	32.32		
AES256-GCM	41.69		
Ascon-128a	4.60[1]		

Table: Performance (ns/byte) on Raspberry Pi 4 equipped with ARM Cortex-A72 running at 1.5 GHz.

[1] from https://ascon.iaik.tugraz.at/implementations.html

Where?

Pre-print

Available at `https://eprint.iacr.org/2024/1618`

Final version

Will appear at EuroS&P 2025

Conclusions

Two approaches for **committing** and **session-supporting** AE with (Turbo)SHAKE:

- performance of duplex-based mode
- robustness and flexibility of deck-based modes, see also
  - JAMBO, BOREE, and JAMBOREE modes [Băcuieti et al., ASIACRYPT 2022]
  - nonce-encrypting modes [Hoffert, ePrint 2022/1711]

And simplicity of the modes once the layers are merged

Conclusions

Two approaches for **committing** and **session-supporting** AE with (Turbo)SHAKE:

- performance of duplex-based mode
- robustness and flexibility of deck-based modes, see also
  - JAMBO, BOREE, and JAMBOREE modes [Băcuieti et al., ASIACRYPT 2022]
  - nonce-encrypting modes [Hoffert, ePrint 2022/1711]

And simplicity of the modes once the layers are merged

Thanks for your attention!