Special Publication on Authenticated Encryption

Meltem Sönmez Turan

SHA-3 2014 Workshop

August 22, 2014

NIST

National Institute of Standards and Technology

Technology Administration, U.S. Department of Commerce

Outline

- Authenticated Encryption (AE)
- NIST-approved AE primitives
- Permutation-based AE modes
- NIST's plan and timeline
- Call for feedback

Authenticated Encryption

An Authenticated Encryption (AE) algorithm provides *message integrity* **AND** *confidentiality*.

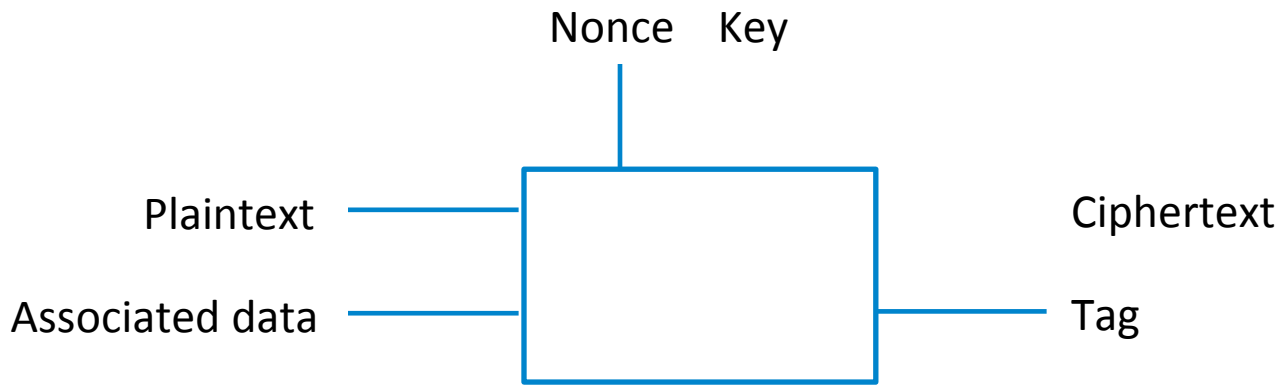
Approach I:

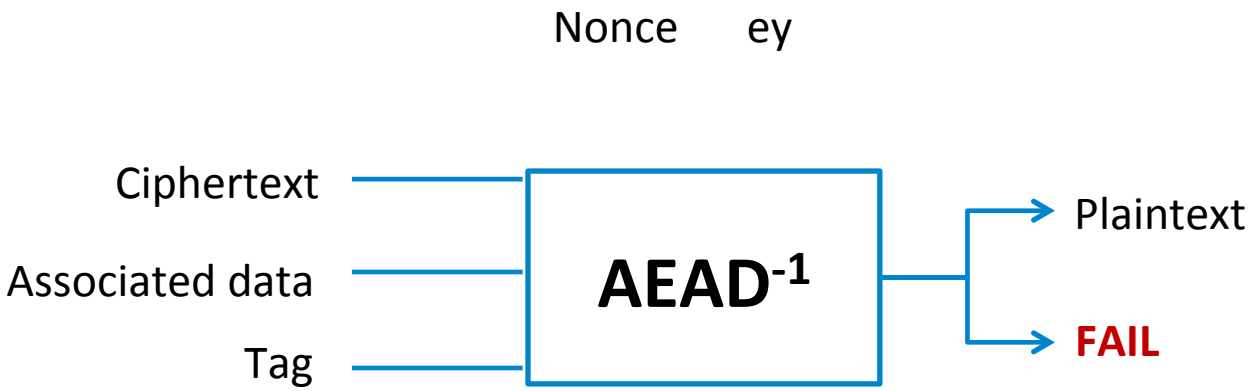
Authenticate using a MAC (e.g., HMAC) and encrypt using a block cipher (e.g., AES-CBC).

Approach II:

Use a dedicated AE algorithm.

Generic Structure





NIST Approved AE Algorithms

Based on block ciphers

- **SP 800-38C** specifies **CCM** mode of AES:
  - Combination of counter mode for privacy and cipher block chaining technique for authentication
- **SP 800-38D** specifies **GCM** (Galois/Counter Mode) of AES:
  - Combination of counter mode for privacy and universal hashing over binary Galois Field for authentication.
- **SP 800-38F** specifies Key Wrapping modes:
  - **KW**/**KWP** using AES
  - **TKW** using Triple DES

NIST's Plan

- In 2012, Keccak is selected as SHA-3, due to security/performance advantages and extra features, such as its built-in AE mode.

> *" … NIST may consider standardizing additional constructions based on the KECCAK permutation, such as an authenticated-encryption mode, in the future. "*
>
> *- from* "NISTIR 7896 - *Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition*" (Nov, 2012):

NIST's Plan (cont.)

Underlying Permutation:

- Draft *FIPS 202 SHA-3 Standard* specifies the family of the KECCAK-*f* [*b*] permutations with width *b*= {25, 50, 100, 200, 400, 800, 1600}.
- KECCAK-*f* [1600] (with 24 rounds) is well-analyzed and is believed to have a high security margin.
- Single primitive for hashing and AE

NIST's Plan (cont.)

Underlying Permutation:

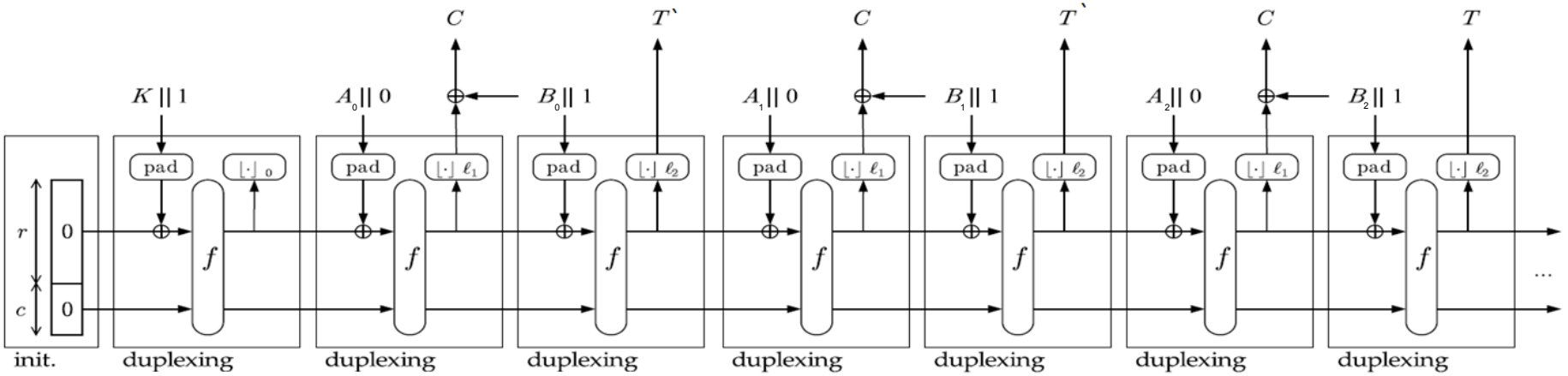
- Draft *FIPS 202 SHA-3 Standard* specifies the family of the KECCAK-*f* [*b*] permutations with width *b*= {25, 50, 100, 200, 400, 800, 1600}.
- KECCAK-*f* [1600] (with 24 rounds) is well-analyzed and is believed to have a high security margin.
- Single primitive for hashing and AE

AE Mode:

- Various permutation-based AE modes, including some of the CAESAR submissions (e.g., DUPLEXWRAP, MONKEYWRAP, PPAE, APE). However, we do not to want to influence the CAESAR competition.
- Initial plan is to approve the AE mode SPONGEWRAP.

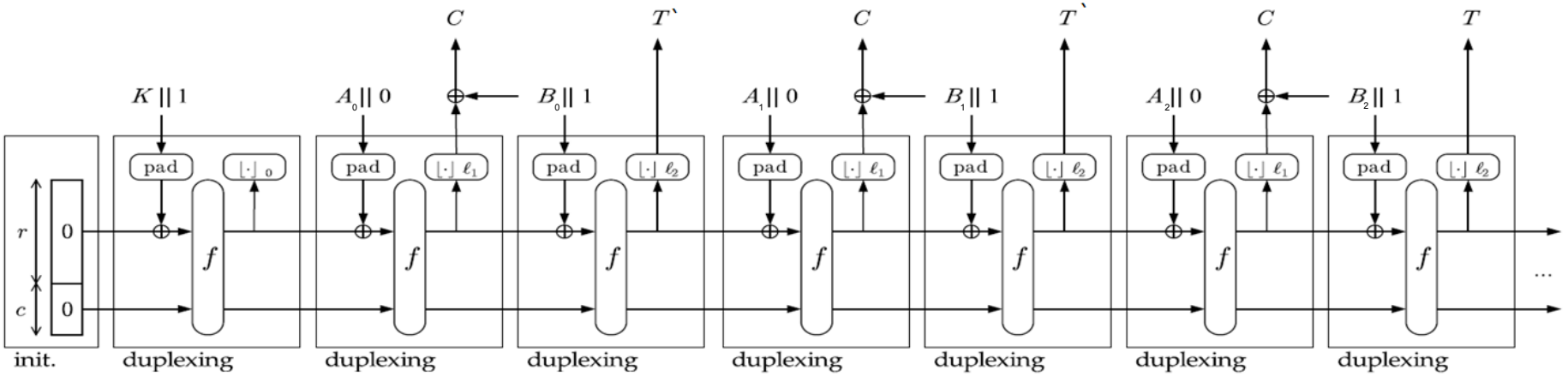
SPONGEWRAP

Proposed by the KECCAK team at SAC'11



SPONGEWRAP

Proposed by the KECCAK team at SAC'11



NIST plans to

- support 128- and 256- bit security levels, by using
  Capacity c = 2 x {security level} ,
- use multi-rate padding,
- support intermediate tags.

TIMELINE: Draft *Special Publication* for Authenticated Encryption – Q4 2014 for Public Comments

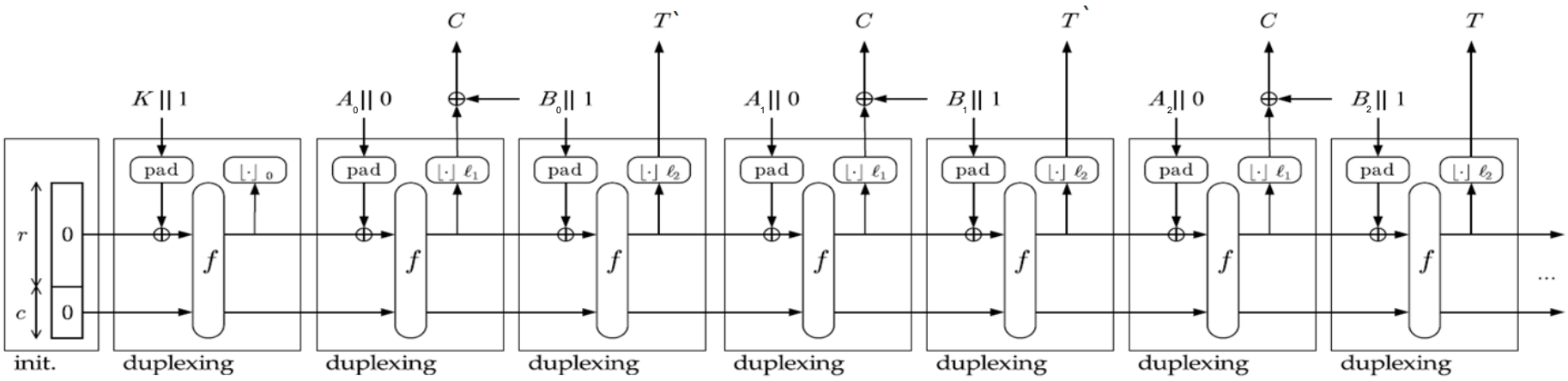
Call for Feedback

Q1) Based on the security proof of SPONGEWRAP, should we consider using lower capacities, i.e. $c = |K| +$ {max. online data complexity}? Can we assume maximum online data complexity is $\leq 2^{96}$?

Call for Feedback

Q1) Based on the security proof of SPONGEWRAP, should we consider using lower capacities, i.e. c = |K|+ {max. online data complexity}? Can we assume maximum online data complexity is $\leq 2^{96}$?

Q2) What should be the intermediate and final tag sizes? How frequent should the intermediate tags be given as output?



Call for Feedback

Q1) Based on the security proof of SPONGEWRAP, should we consider using lower capacities, i.e. $c = |K| + \{\text{max. online data complexity}\}$? Can we assume maximum online data complexity is $\leq 2^{96}$?

Q2) What should be the intermediate and final tag sizes? How frequent should the intermediate tags be given as output?

Q3) DUPLEXWRAP is an improved version of SPONGEWRAP. Should we consider DUPLEXWRAP?

Call for Feedback

Q1) Based on the security proof of SPONGEWRAP, should we consider using lower capacities, i.e. $c = |K| + \{\text{max. online data complexity}\}$? Can we assume maximum online data complexity is $\leq 2^{96}$?

Q2) What should be the intermediate and final tag sizes? How frequent should the intermediate tags be given as output?

Q3) DUPLEXWRAP is an improved version of SPONGEWRAP. Should we consider DUPLEXWRAP?

Q4) Are there any other issues we need to consider?

References

- Draft FIPS PUB 202:
  SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, 2014.
- NISTIR 7896:
  Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition, 2012.
- G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche,
  Duplexing the sponge: single-pass authenticated encryption and other applications,
  Selected Areas in Cryptography (SAC), 2011 (also in
  Second SHA-3 Candidate Conference, 2010)
- CAESAR Competition: http://competitions.cr.yp.to/caesar.html
- G. Bertoni, J. Daemen, M. Peeters, G. Van Assche:
  Duplexing the Sponge: Single-Pass Authenticated Encryption and Other
  Applications. Selected Areas in Cryptography 2011: 320-337

Special Publication on Authenticated Encryption

QUESTIONS?

meltem.turan@nist.gov

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce