On properties of AEAD algorithms

`draft-irtf-cfrg-aead-properties`

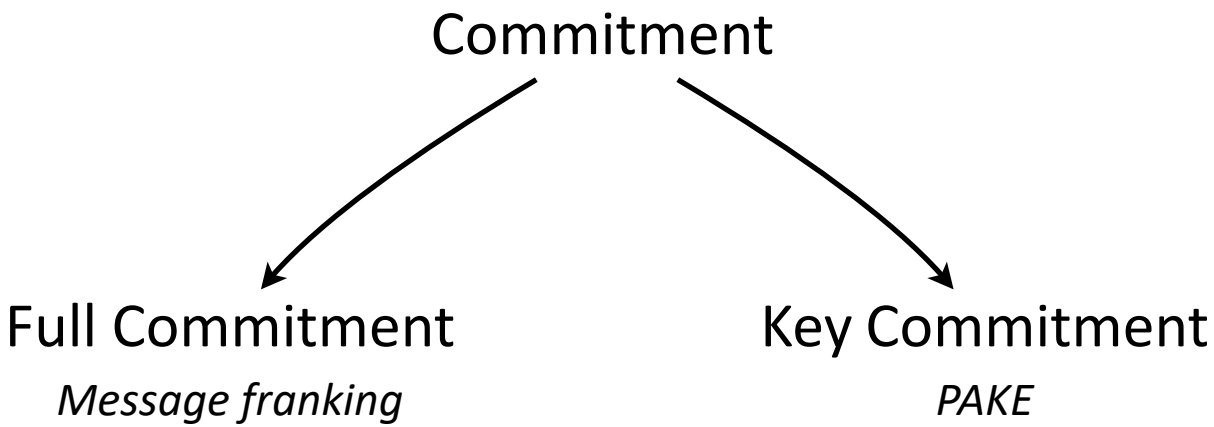
Andrey Bozhko

IETF 118, November 2023

Latest news

- After some problems with datatracker, the draft was updated to version 02.
- Some new properties and examples of functional applications were added.

  In particular (thanks to Samuel Lucas for noticing!):



Most requested property — Indifferentiability

Indifferentiability for AE in the sense of [1] has been asked to be added starting form version 0. I remember about it!

The problem

Indifferentiability is not an additional property, but an entirely different definition of AEAD security.

Will try to find an approach to that problem in the next version.

[1] M. Barbosa, P. Farshim (2018) “Indifferentiable Authenticated Encryption”

NIST Workshop on Block Cipher Modes of Operation

Topics for discussion include:

- The security and efficiency of current NIST modes
- Additional security features (e.g., misuse-resistance, key commitment, etc.) that would be desirable in a new encryption technique
- Case studies of encryption techniques for specific uses, such as storage and key wrapping
- The security and efficiency of tweakable wide encryption techniques

NIST Workshop on Block Cipher Modes of Operation

Topics for discussion include:

- The security and efficiency of current NIST modes
- Additional security features (e.g., misuse-resistance, key commitment, etc.) that would be desirable in a new encryption technique
- Case studies of encryption techniques for specific uses, such as storage and key wrapping
- The security and efficiency of tweakable wide encryption techniques

- At least 7 out of 14 accepted papers discuss additional properties (or redefine the standard ones)!

NIST Workshop on Block Cipher Modes of Operation

Topics for discussion include:

- The security and efficiency of current NIST modes
- Additional security features (e.g., misuse-resistance, key commitment, etc.) that would be desirable in a new encryption technique
- Case studies of encryption techniques for specific uses, such as storage and key wrapping
- The security and efficiency of tweakable wide encryption techniques

- At least 7 out of 14 accepted papers discuss additional properties (or redefine the standard ones)!

- At least 3 out of 7 are related to commitment

NIST Workshop on Block Cipher Modes of Operation

Topics for discussion include:

- The security and efficiency of current NIST modes
- Additional security features (e.g., misuse-resistance, key commitment, etc.) that would be desirable in a new encryption technique
- Case studies of encryption techniques for specific uses, such as storage and key wrapping
- The security and efficiency of tweakable wide encryption techniques

- At least 7 out of 14 accepted papers discuss additional properties (or redefine the standard ones)!
- At least 3 out of 7 are related to commitment
- At least 1 paper cites the draft 😀

Advertisement

Please contact me if:

- There is some property you want to see in the draft,
- There is some application/protocol you know which requires AEAD with additional properties,
- Your research is connected with the draft's problematic.

And on any other draft/AEAD related occasion!

Contacts:
andbogc@gmail.com