On properties of AEAD algorithms

draft-bozhko-cfrg-aead-properties

Andrey Bozhko

IETF 115, November 2022

[Cfrg] Do we need a selection contest for AEAD? Fri, 19 June 2020

Paul Grubbs, **Wed, 24 June 2020:**

Recently I've been studying the AEAD landscape, and there seem to be a lot of gaps between the needs of applications/protocols and the properties widely-used schemes provide.

Yevgeniy Dodis, **Wed, 24 June 2020:**

I feel AEAD landscape is getting a bit out of hand, even despite the CEASAR competition. Would be good to bring back more structure and understanding, so when people in the industry need an AEAD scheme, they have a clear guide what to choose from.

Mridul Nandi, **Wed, 24 June 2020:**

I think we are lacking formal added security requirements of AEAD. Beyond the classical definition of AEAD, it would be really interesting if we can list the additional features in a more formal way.

Jim Schaad, **Wed, 01 July 2020:**

Having a document that I can point to that gives what the properties are and do I care about them when deciding on an algorithm would be very useful.

AEAD properties zoo

Nonce-hiding

Nonce misuse resistance

ZK-friendly

Online

KDM security
(key dependent messages)

Key commitment

RUP security
(release unverified plaintext)

Multi-user security

Remotely-keyed

Incremental

Leakage resistance

Properties vocabulary

Property1

- Definition
- Synonyms
- Functional applications
- Algorithms examples
- Further reading
- Notes

Property2

- Definition
- Synonyms
- Functional applications
- Algorithms examples
- Further reading
- Notes

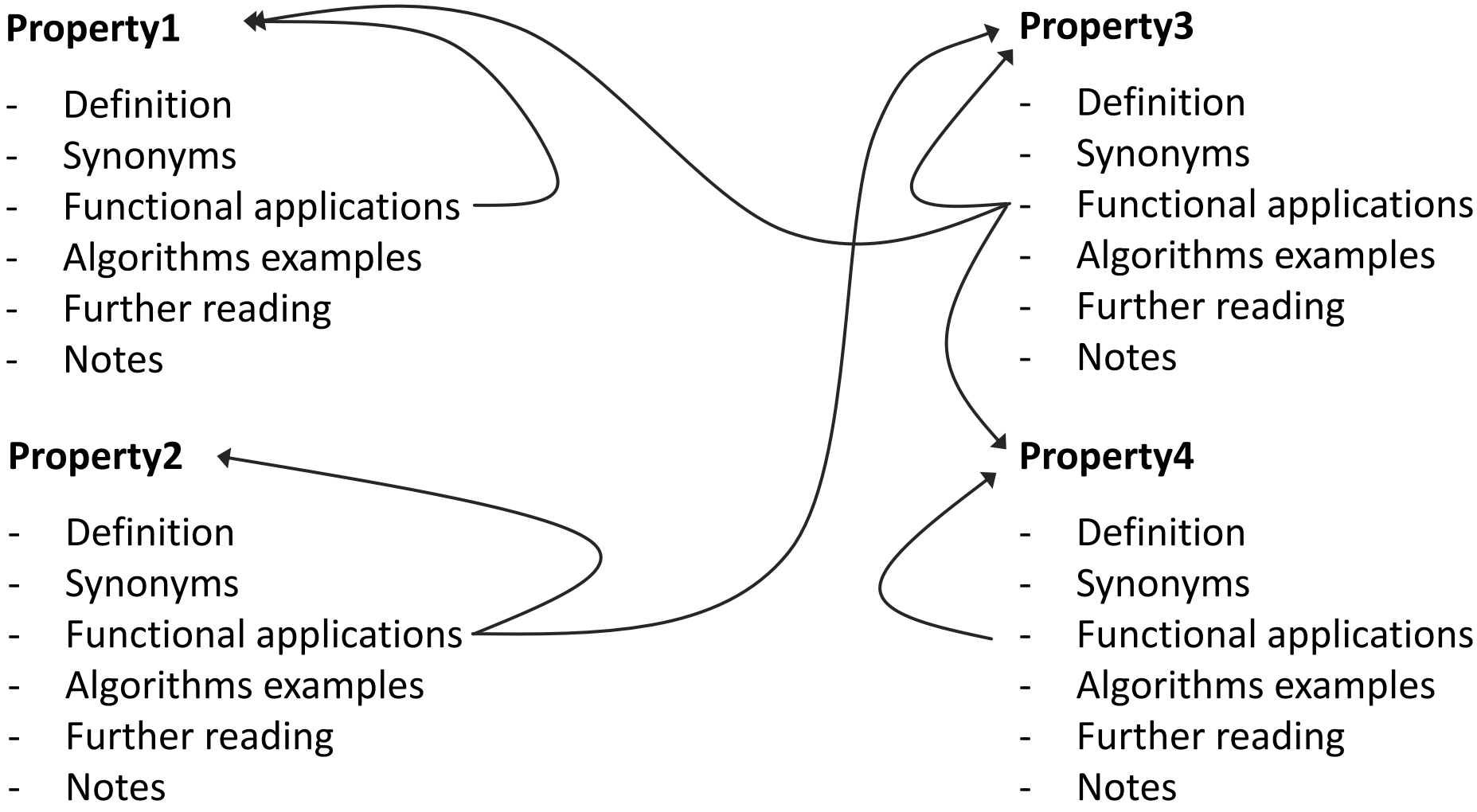
Property3

- Definition
- Synonyms
- Functional applications
- Algorithms examples
- Further reading
- Notes

Property4

- Definition
- Synonyms
- Functional applications
- Algorithms examples
- Further reading
- Notes

How make the document be helpful for protocol designers?



Property1

- Definition
- Synonyms
- Functional applications
- Algorithms examples
- Further reading
- Notes

Property2

- Definition
- Synonyms
- Functional applications
- Algorithms examples
- Further reading
- Notes

Property3

- Definition
- Synonyms
- Functional applications
- Algorithms examples
- Further reading
- Notes

Property4

- Definition
- Synonyms
- Functional applications
- Algorithms examples
- Further reading
- Notes

Draft, version 02

- Address new ideas that emerged after significant help from Chris Wood (thanks a lot, Chris!)
- Solve the issue with the interfaces of AEAD – some properties imply non-standard (non-RFC5116) interfaces
- Improve classification of properties
- Add first functional applications examples
- Add new properties

Questions for the CFRG

Do we need such document? Will it be helpful from your point of view?

What properties do you find necessary to be covered?

What applications do you find necessary to be covered?

Questions?

☺

Contacts:
andbogc@gmail.com