Properties of AEAD algorithms

draft-irtf-cfrg-aead-properties-01

Andrey Bozhko

IETF 116, March 2023

November 2022 – March 2023

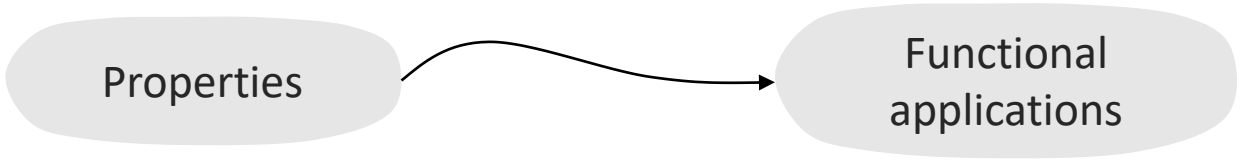
- Draft adopted by CFRG
- Community comments were addressed. Thanks everyone!
- Some new properties were added, some updated (22 in total, more to come)
- New section with basic AEAD definitions for consistency
- Classification of properties was improved and explained

How to make the document be useful for implementers?

Property

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

Step 1. Functional application – how the property can contribute to a higher level application; why do I need it for my AEAD choice?

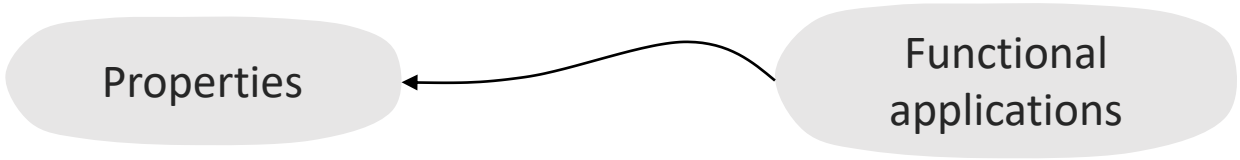


How to make the document be useful for implementers?

Functional application/requirement

- Description
- Properties needed
- Further reading
- Notes

Step 2. Compile a Functional applications vocabulary.
So that if an implementer has some functional requirement for AEAD, they could easily map it into properties.



How to make the document be useful for implementers?

Step 0. How to describe functional applications? How deep to go in details? Actually, what a functional application/requirement is?

How to make the document be useful for implementers?

Step 0. How to describe functional applications? How deep to go in details? Actually, what a functional application/requirement is?

Example.
– I can’t store the whole plaintext in a secure memory when I decrypt. Is it possible to do something with that?

How to make the document be useful for implementers?

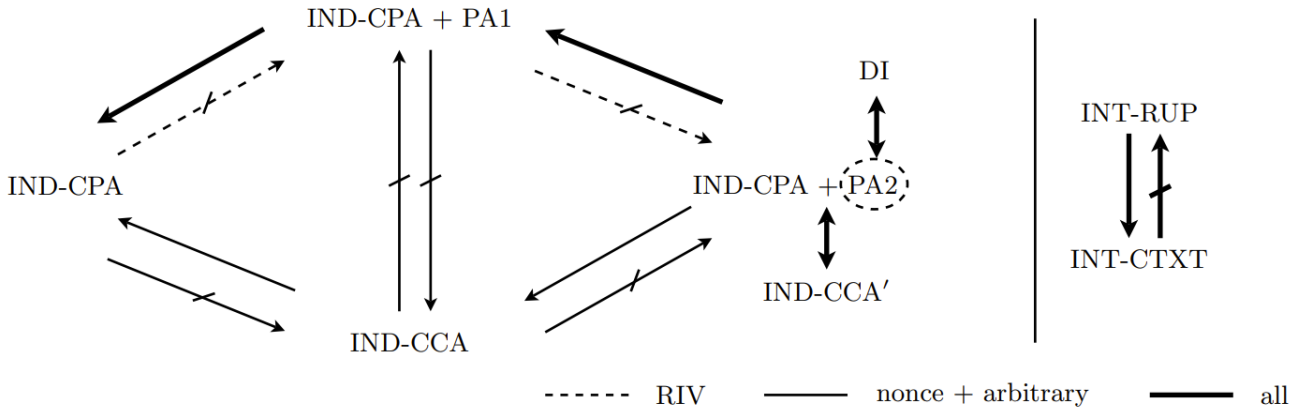
Step 0. How to describe functional applications? How deep to go in details? Actually, what a functional application/requirement is?

Example.
– I can’t store the whole plaintext in a secure memory when I decrypt. Is it possible to do something with that?
– Yeah, you should use RUP secure AEAD. But…

How to make the document be useful for implementers?

Step 0. How to describe functional applications? How deep to go in details? Actually, what a functional application/requirement is?

Example.
– I can't store the whole plaintext in a secure memory when I decrypt. Is it possible to do something with that?
– Yeah, you should use RUP secure AEAD. But… We have RUP integrity and we also have two flavors of RUP confidentiality. Let me draw a picture* for you…



*Andreeva, E. et al. (2014). How to Securely Release Unverified Plaintext in Authenticated Encryption. ASIACRYPT 2014.

In the next episode

- Step 0 and Step 1 of the plan
  If you have an opinion on the questions above, or know some good examples of functional applications, I would be happy to hear from you!

- Add new properties
  Let me know if you want any property to be covered in the document!

- Expand sections about current properties, make definitions more precise
  There's always room for improvement!

Questions?

Contacts:
andbogc@gmail.com