On properties of AEAD algorithms

draft-bozhko-cfrg-aead-properties

Andrey Bozhko

IETF 117, July 2023
April – July 2023

• A short pause for a research stage – looking for and classifying functional applications

• The next version is scheduled by the next IETF meeting

• Some minor changes
April – July 2023

- A short pause for a research stage – looking for and classifying functional applications
- The next version is scheduled by the next IETF meeting
- Some minor changes

If your application/protocol has some specific requirements for AEAD, please let me now!
All properties are divided into four groups:

1. Basic (security) properties – confidentiality, integrity
2. Security properties
3. Implementation properties
4. Additional functionality properties

With these two everything is clear

Where is the verge between these two?
Security vs additional functionality

Basic security – nonce-respecting adversary wants to break confidentiality or integrity

ENC \[ (N, A, P) \]
\[ (C, T) \]

DEC \[ (N, A, C, T) \]
\[ P \text{ or } \perp \]

\( N \) must be unique
\( N \) may be repeated

Wants to break confidentiality or integrity
Security vs additional functionality

Additional security – we extend what an adversary can do or wants to achieve

ENC

$\left( N, A, P \right)$

$\left( C, T \right)$

\[ \text{N may be repeated} \]

\[ \text{Wants to break confidentiality or integrity} \]

DEC

$\left( N, A, C, T \right)$

$P$ \text{ or } \bot

\[ \text{N may be repeated} \]
Security vs additional functionality

Additional security – we extend what an adversary can do or wants to achieve

$\text{ENC}$

\[
(N, A, P) \quad \Rightarrow \quad (C, T)
\]

$N$ must be unique

$\text{DEC}$

\[
(N, A, C, T) \quad \Rightarrow \quad P \text{ or } \bot
\]

$N$ may be repeated

Wants to make not only one but many forgeries
Security vs additional functionality

Additional functionality – we extend what the authenticated encryption scheme can do (usually implies different interface)

\[ (N, A, A', M', C, T) \]
\[ (C', T') \]

**ENC**

\[ (N, A, P) \]
\[ (C, T) \]

\( N \) must be unique

**UPDATE**

\[ (N, A, A', M', C, T) \]
\[ (C', T') \]

Wants to break confidentiality or integrity (but in a new sense)

**DEC**

\[ (N, A, C, T) \]

\( P \) or \( \perp \)

\( N \) may be repeated
Security vs additional functionality

**Additional security properties**

Extended adversarial capabilities and threats for usual AEAD schemes

Every AEAD scheme can be analyzed for that property (but might not have it)

**Additional functionality properties**

Implies an extension of the usual AEAD interface – defines a new class of algorithms

Basic threats and adversarial capabilities have to be redefined for that new class

**Properties**

- Nonce misuse
- Key commitment
- KDM
- Multi-user security
- RUP
- Incremental
- Robust
- Remotely-keyed
Questions?

Contacts:
andbogc@gmail.com