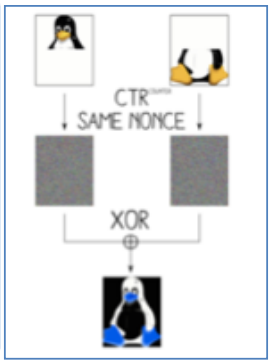
IoT環境のための認証付き暗号
Authenticated Encryption for IoT Environment

LAI YEE CHING・システム分科会・情報セキュリティ大学院大学

Authenticated Encryption (AE) is important as it make sure the authenticity and confidentiality of the data. In IoT environment, which is lack of entropy and many of device resets, Nonce-Misuse problem needs to be seriously considered during the implementation of AE.

Nonce-Misuse Problem

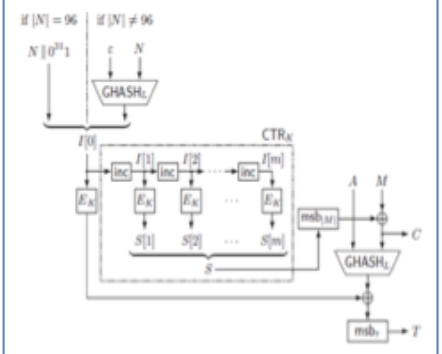
- Nonce is a value that can only be used once.
- One of the condition of securely using the nonce is to make sure there is no repetition occurs when generating nonce.
- If length of nonce is 32 bits, 2^{16} random nonce ⟹ 50% same nonce repeated.
- Causes of vulnerability to AE ciphers, especially in IoT environment that are lack of entropy resources.



Example of AE Implementation with Nonce-Misuse Problem and solution

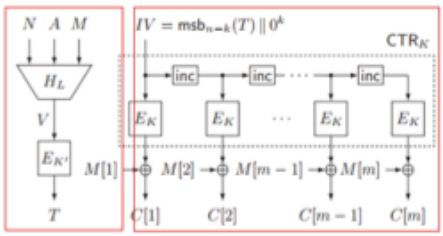
AES-GCM →

- Is an AEAD mode of operation of the AES algorithm that is recommended by NIST for its efficiency and performance.



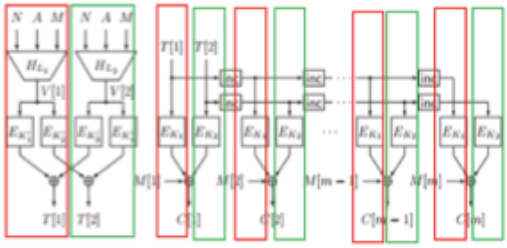
GCM-SIV →

- Variant of AES-GCM
- Resolve problem of Nonce-Misuse of AES-GCM.
- Vulnerable to Birthday Attack.



GCM-SIV2

- Variant of GCM-SIV.
- Resolve Birthday Attack problem for GCM-SIV.



Future work:
Designing and proving generic solution for SIV2