認証付き暗号の最新動向

Recent Progress of Authenticated Encryption

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 one of the cipher which can protect the confidentiality, integrity and authenticity of the data in all communication throughout the Internet. Here we explain on the basic of AE and the recent developments of AE which includes on the recent AE competition called CAESAR and focus on the use case 3 – defense in depth. This poster includes the view point on what makes defense in depth so important for AE. The viewpoints are: Nonce-Misuse Problem, Beyond Birthday Bound (BBB), and Quantum Computation.

Authenticated Encryption

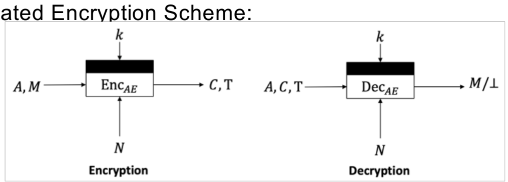
Encryption: Outsider **cannot** learn anything about data.

Authentication: Outsider **cannot** manipulate data.

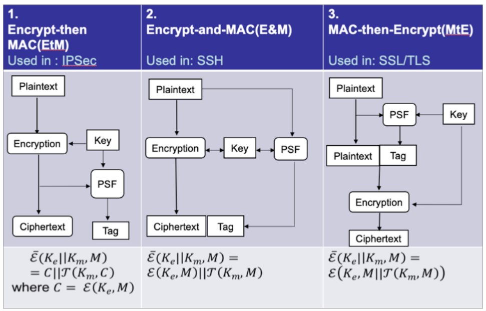
With AE, the data are safe from data tampering and eavesdropping.

There are 6 standardized methods for AE (ISO/IEC 19772:2009):
OCB 2.0, Key Wrap, CCM, EAX, Encrypt-then-MAC(EtM), GCM

Authenticated Encryption Scheme:



Three Approaches for Authenticated Encryption:



1. Encrypt-then MAC(EtM) Used in : IPSec	2. Encrypt-and-MAC(E&M) Used in: SSH	3. MAC-then-Encrypt(MtE) Used in: SSL/TLS
$\bar{\mathcal{E}}(K_e \Vert K_m, M) = C \Vert \mathcal{T}(K_m, C)$ where $C = \mathcal{E}(K_e, M)$	$\bar{\mathcal{E}}(K_e \Vert K_m, M) = \mathcal{E}(K_e, M) \Vert \mathcal{T}(K_m, M)$	$\bar{\mathcal{E}}(K_e \Vert K_m, M) = \mathcal{E}(K_e, M \Vert \mathcal{T}(K_m, M))$

CAESAR Competition

CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness)

Aim: To find a portfolio which is able to offer the advantages over AES-GCM and suitable for widespread adoption.

Competition	Cipher	No. of Candidates	Remarks
First Round (Submission: 15/3/2014)	ACORN, AEGIS, ASCON, COLM, Deoxys, MORUS, OCB, AES-JAMBU, AES-OTR, AEZ, CLOC, Ketje, Keyak, NORX, SILC, Tiaoxin, HS1-SIV, ICEPOLE, Joltik, Minalpher, OMD, PAEQ, π-Cipher, POET, PRIMATEs, SCREAM, SHELL, STRIBOB, TriviA-ck, ++AE, AES-CMCC, AES-COBRA, AES-CPFB, Artemia, AVALANCHE, Calico, CBA, CBEAM, Enchilada, FASER, HKC, iFeed, Julius, KIASU, LAC, Marble, McMambo, PAES, PANDA, POLAWIS, Prøst, Raviyoyla, Sablier, Silver, Wheesht, YAES	56	9 Candidates Withdrawn (mark in purple)
Second Round (Announcement: 7/7/2015)	ACORN, AEGIS, ASCON, COLM, Deoxys, MORUS, OCB, AES-JAMBU, AES-OTR, AEZ, CLOC, Ketje, Keyak, NORX, SILC, Tiaoxin, HS1-SIV, ICEPOLE, Joltik, Minalpher, OMD, PAEQ, π-Cipher, POET, PRIMATEs, SCREAM, SHELL, STRIBOB, TriviA-ck	29	
Third Round (Announcement: 15/8/2016)	ACORN, AEGIS, ASCON, COLM, Deoxys, MORUS, OCB, AES-JAMBU, AES-OTR, AEZ, CLOC, Ketje, Keyak, NORX, SILC, Tiaoxin.	15	**COLM is merged with COPA and ELmD **CLOC and SILC is combined.
Final Round (Announcement: 5/3/2018)	ACORN, AEGIS, ASCON, COLM, Deoxys, MORUS, OCB	7	

CAESAR Candidates Hardware Performance:

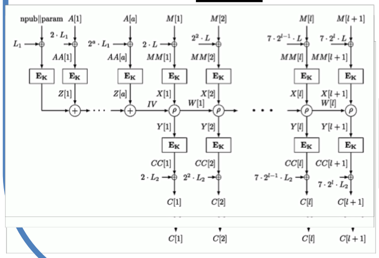
Algorithm	Throughput (Mbps)	Area (LUTs)	Throughput/ Area (Mbps/LUT)
MORUS	49,556	3,397	14.5
AEGIS	70,934	3,460	9.3
ACORN	11,304	508	9.1
ASCON	5,085	1,270	3.2
Deoxys	2,882	3,175	0.91
OCB	3,109	4,254	0.73
COLM	3,109	7,143	0.39

CAESAR Use Case

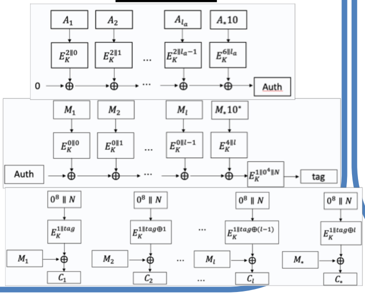
CAESAR Finalists are categorized in three use case:

Use Case	Use Case Criteria	Finalists
Use Case 1: Lightweight Applications	• Fits into small hardware are and/or small code for 8-bit CPUs.	ACORN ASCON
Use Case 2: High-Performance Applications	• Efficiency on 64-bit CPUs (servers) and/or dedicated hardware.	AEGIS MORUS OCB
Use Case 3: Defense in Depth	• Critical: Authenticity despite nonce misuse. • Desirable: Limited privacy damage from nonce misuse. • Desirable: Authenticity despite release of unverified plaintexts. • Desirable: Limited privacy damage from release of unverified plaintexts. • Desirable: Robustness in more scenarios; e.g., huge amounts of data.	COLM Deoxys-II

COLM

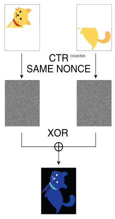


Deoxys-II



Nonce-Misuse, BBB, Quantum Computation

Nonce-Misuse: Nonce is a value that can only be used once. If a nonce is repeated, it will cause disastrous result.



The causes of Nonce-Misuse problem:

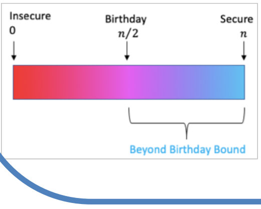
- Birthday Paradox
  Lengths of nonce is 32 bits. 2^{16}random nonce is equivalent to 50% same nonce repeated.
- Bad User Management
- Bad Implementations

Beyond Birthday Bound

Security Proofs of AE

- Birthday Bound
- σ : amount of data adversary obtains
- Success probability $O\ (\sigma^2/2^n)$

→ $\frac{n}{2}$-bit security



Quantum Computation

Example of attack against CBC-MAC

$$f: \{0,1\} \times \{0,1\}^n \rightarrow \{0,1\}^n$$

$$b, x \mapsto \text{CBC-MAC}(\alpha_b \parallel x) = E_{k'}\left(E_k(x \oplus E_k(\alpha_b))\right)$$

$$f(b', x') = f(b, x) \Leftrightarrow x \oplus E_k(\alpha_b) = x' \oplus E_k(\alpha_{b'})$$

$$\Leftrightarrow \begin{cases} x' \oplus x = 0 & \text{if } b' = b \\ x' \oplus x = E_k(\alpha_0) \oplus E_k(\alpha_1) & \text{if } b' \neq b \end{cases}$$

Simon's Algorithm → $E_k(\alpha_0) \oplus E_k(\alpha_1)$

At least 256 bits size of secret key in AE scheme should be used for any long-term security against quantum adversary.

Cipher	Post-Quantum Security Level	Remarks
COLM	64-bit	Not suited for long-term security
Deoxys-II	128-bit	Suitable for long-term security