Authenticated Encryption

We have now learned about message secrecy ($\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$, $\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}$, $\mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi}$), and message integrity ($\text{Mac-forge}_{\mathcal{A},\Pi}$).

Authenticated Encryption

We have now learned about message secrecy ($\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$, $\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}$, $\mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi}$), and message integrity ($\text{Mac-forge}_{\mathcal{A},\Pi}$).

What if we want both, simultaneously?

Authenticated Encryption

We have now learned about message secrecy ($\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}$, $\text{PrivK}^{\text{cpa}}_{\mathcal{A},\Pi}$, $\text{PrivK}^{\text{cca}}_{\mathcal{A},\Pi}$), and message integrity ($\text{Mac-forge}_{\mathcal{A},\Pi}$).

What if we want both, simultaneously?

Authenticated encryption :

- Secrecy: CCA security
- Integrity: Unforgeable ciphertexts
  - Adversary cannot create any valid ciphertext that decrypts to a message that was not previously queried (for encryption).

Authenticated Encryption

We have now learned about message secrecy ($\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}, \mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}, \mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi}$), and message integrity ($\mathsf{Mac\text{-}forge}_{\mathcal{A},\Pi}$).

What if we want both, simultaneously?

Authenticated encryption :

- Secrecy: CCA security
- Integrity: Unforgeable ciphertexts
  - Adversary cannot create any valid ciphertext that decrypts to a message that was not previously queried (for encryption).

Encrypt THEN Authenticate:
$c \leftarrow \mathsf{Enc}(k_1, m)$
$t = \mathsf{Mac}(k_2, c)$
Output (c, t)

Authenticated Encryption

We have now learned about message secrecy ($\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}, \mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}, \mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi}$), and message integrity ($\text{Mac-forge}_{\mathcal{A},\Pi}$).

What if we want both, simultaneously?

Authenticated encryption :

- Secrecy: CCA security
- Integrity: Unforgeable ciphertexts
  - Adversary cannot create any valid ciphertext that decrypts to a message that was not previously queried (for encryption).

Encrypt THEN Authenticate:
$c \leftarrow \mathsf{Enc}(k_1, m)$
$t = \mathsf{Mac}(k_2, c)$
Output (c, t)

If the encryption scheme is CPA secure, and the MAC is secure (with unique tags), then this gives a good authenticated encryption scheme.

Authenticated Encryption

We have now learned about message secrecy ($\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}$, $\text{PrivK}^{\text{cpa}}_{\mathcal{A},\Pi}$, $\text{PrivK}^{\text{cca}}_{\mathcal{A},\Pi}$), and message integrity ($\text{Mac-forge}_{\mathcal{A},\Pi}$).

What if we want both, simultaneously?

Authenticated encryption :

- Secrecy: CCA security
- Integrity: Unforgeable ciphertexts
  - Adversary cannot create any valid ciphertext that decrypts to a message that was not previously queried (for encryption).

Encrypt AND Authenticate? $\big(\text{Enc}(k_1, m), \text{Mac}(k_2, m)\big)$

Authenticated Encryption

We have now learned about message secrecy ($\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}$, $\text{PrivK}^{\text{cpa}}_{\mathcal{A},\Pi}$, $\text{PrivK}^{\text{cca}}_{\mathcal{A},\Pi}$), and message integrity ($\text{Mac-forge}_{\mathcal{A},\Pi}$).

What if we want both, simultaneously?

Authenticated encryption :

- Secrecy: CCA security
- Integrity: Unforgeable ciphertexts
  - Adversary cannot create any valid ciphertext that decrypts to a message that was not previously queried (for encryption).

Encrypt AND Authenticate? $\big(\text{Enc}(k_1, m), \text{Mac}(k_2, m)\big)$ Insecure!

Authenticated Encryption

We have now learned about message secrecy ($\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}$, $\text{PrivK}^{\text{cpa}}_{\mathcal{A},\Pi}$, $\text{PrivK}^{\text{cca}}_{\mathcal{A},\Pi}$), and message integrity ($\text{Mac-forge}_{\mathcal{A},\Pi}$).

What if we want both, simultaneously?

Authenticated encryption :

- Secrecy: CCA security
- Integrity: Unforgeable ciphertexts
  - Adversary cannot create any valid ciphertext that decrypts to a message that was not previously queried (for encryption).

Encrypt AND Authenticate? $\big(\text{Enc}(k_1, m), \text{Mac}(k_2, m)\big)$ Insecure!
If the tag is included "next to" the message, the tag itself is not CCA secure.
It might be deterministic.
It might even include the message itself as part of the tag!

Authenticated Encryption

We have now learned about message secrecy ($\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}$, $\text{PrivK}^{\text{cpa}}_{\mathcal{A},\Pi}$, $\text{PrivK}^{\text{cca}}_{\mathcal{A},\Pi}$), and message integrity ($\text{Mac-forge}_{\mathcal{A},\Pi}$).

What if we want both, simultaneously?

Authenticated encryption :

- Secrecy: CCA security
- Integrity: Unforgeable ciphertexts
  - Adversary cannot create any valid ciphertext that decrypts to a message that was not previously queried (for encryption).

Authenticate THEN Encrypt? $\text{Enc}\big(k_1, m||\text{Mac}(k_2, m)\big)$

Authenticated Encryption

We have now learned about message secrecy ($\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}$, $\text{PrivK}^{\text{cpa}}_{\mathcal{A},\Pi}$, $\text{PrivK}^{\text{cca}}_{\mathcal{A},\Pi}$), and message integrity ($\text{Mac-forge}_{\mathcal{A},\Pi}$).

What if we want both, simultaneously?

Authenticated encryption :

- Secrecy: CCA security
- Integrity: Unforgeable ciphertexts
  - Adversary cannot create any valid ciphertext that decrypts to a message that was not previously queried (for encryption).

Authenticate THEN Encrypt? $\text{Enc}\big(k_1, m||\text{Mac}(k_2, m)\big)$ Insecure!

Authenticated Encryption

We have now learned about message secrecy ($\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}$, $\text{PrivK}^{\text{cpa}}_{\mathcal{A},\Pi}$, $\text{PrivK}^{\text{cca}}_{\mathcal{A},\Pi}$), and message integrity ($\text{Mac-forge}_{\mathcal{A},\Pi}$).

What if we want both, simultaneously?

Authenticated encryption :

- Secrecy: CCA security
- Integrity: Unforgeable ciphertexts
  - Adversary cannot create any valid ciphertext that decrypts to a message that was not previously queried (for encryption).

Authenticate THEN Encrypt? $\text{Enc}\big(k_1, m||\text{Mac}(k_2, m)\big)$ Insecure!

The same padding oracle attack can be used, if Enc is only CPA secure.
(Assuming you can distinguish padding failures from MAC verification failures.)