Introduction to Cryptology

6.2 - Authenticated Encryption

Federico Pintore
Mathematical Institute, University of Oxford (UK)

UNIVERSITY OF OXFORD

Michaelmas term 2020

Authenticated Encryption

Authenticated Encryption is a cryptographic primitive which achieves secrecy and integrity simultaneously.

Authenticated Encryption

Authenticated Encryption is a cryptographic primitive which achieves secrecy and integrity simultaneously.

- No standard terminology or definitions yet.
- CAESAR - Competition for Authenticated Encryption: Security, Applicability, and Robustness. http://competitions.cr.yp.to/caesar.html

Authenticated Encryption

Authenticated Encryption is a cryptographic primitive which achieves secrecy and integrity simultaneously.

- No standard terminology or definitions yet.
- CAESAR - Competition for Authenticated Encryption: Security, Applicability, and Robustness. http://competitions.cr.yp.to/caesar.html

Level of secrecy: CCA-security.

Level of integrity: a variant, for encryption schemes, of the message authentication experiment.

Unforgeable Encryption

Let $S = (\text{KeyGen}, \text{Enc}, \text{Dec})$ be an encryption scheme.

Unforgeable Encryption Experiment $\text{PrivK}^{\text{unforg}}_{\mathcal{A},S}(n)$

Unforgeable Encryption

Let $S = (\text{KeyGen}, \text{Enc}, \text{Dec})$ be an encryption scheme.

Unforgeable Encryption Experiment $\text{PrivK}^{\text{unforg}}_{\mathcal{A},S}(n)$

Challenger Ch	Adversary $\mathcal{A}$
$k \leftarrow \text{KeyGen(n)}$	
$Q = \{\text{queried}\, m\}$	Queries to $\text{Enc}(k, \cdot)$
	Outputs a *forgery* c

$\mathcal{A}$ wins the game, i.e. $\text{PrivK}^{\text{unforg}}_{\mathcal{A},S}(n) = 1$, if, for $m = \text{Dec}(k, c)$, it holds that $m \neq \perp$ and $m \notin Q$.

Unforgeable Encryption

Let $S = (\text{KeyGen}, \text{Enc}, \text{Dec})$ be an encryption scheme.

Unforgeable Encryption Experiment $\text{PrivK}^{\text{unforg}}_{\mathcal{A},S}(n)$

Challenger Ch	Adversary $\mathcal{A}$
$k \leftarrow \text{KeyGen(n)}$	
$Q = \{\text{queried } m\}$	Queries to $\text{Enc}(k, \cdot)$
	Outputs a *forgery* c

$\mathcal{A}$ wins the game, i.e. $\text{PrivK}^{\text{unforg}}_{\mathcal{A},S}(n) = 1$, if, for $m = \text{Dec}(k, c)$, it holds that $m \neq \perp$ and $m \notin Q$.

Definition

A symmetric-key encryption scheme S is unforgeable if, for every PPT adversary $\mathcal{A}$, $\Pr(\text{PrivK}^{\text{unforg}}_{\mathcal{A},S}(n) = 1) \leq \text{negl}(n)$.

Authenticated Encryption: A Definition

Definition

A symmetric-key encryption scheme is an authenticated encryption scheme is it is both CCA-secure and unforgeable.

Not any combination of a secure encryption scheme and a secure MAC would yield an authenticated encryption scheme.

Authenticated Encryption: A Definition

Definition

A symmetric-key encryption scheme is an authenticated encryption scheme is it is both CCA-secure and unforgeable.

Not any combination of a secure encryption scheme and a secure MAC would yield an authenticated encryption scheme.

More in general, combining two secure cryptographic schemes does not automatically provide a new secure scheme.

Authenticated Encryption from secure schemes

Any authenticated encryption scheme is also CCA-secure.

Authenticated Encryption from secure schemes

Any authenticated encryption scheme is also CCA-secure.

- Some CCA-secure encryption schemes are not unforgeable;
- so far, no encryption schemes only CCA-secure and more efficient than authenticated encryption schemes.

Authenticated Encryption from secure schemes

Any authenticated encryption scheme is also CCA-secure.

- Some CCA-secure encryption schemes are not unforgeable;
- so far, no encryption schemes only CCA-secure and more efficient than authenticated encryption schemes.

In the following, we try to combine:

- a CPA-secure encryption scheme $\Pi_E = (\mathrm{KeyGen}_E, \mathrm{Enc}, \mathrm{Dec})$, and
- a strongly secure MAC $\Pi_M = (\mathrm{KeyGen}_M, \mathrm{Mac}, \mathrm{Verify})$

to obtain authenticated encryption.

How to combine Π_E and Π_M

1. Mac and Enc: compute them independently and in parallel

$$c \leftarrow \text{Enc}(k_1, m) \text{ and } t \leftarrow \text{Mac}(k_2, m)$$

2. Mac then Enc: compute the tag and encrypt it with m

$$t \leftarrow \text{Mac}(k_2, m) \text{ then } c \leftarrow \text{Enc}(k_1, m||t)$$

3. Enc then Mac: compute them sequentially

$$c \leftarrow \text{Enc}(k_1, m) \text{ then } t \leftarrow \text{Mac}(k_2, c)$$

Mac and Enc

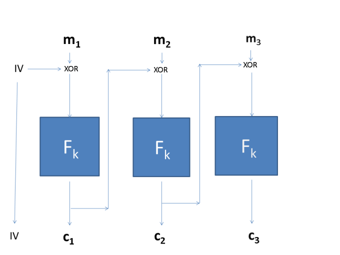
If Mac is deterministic (like for most MACs used in practice), the scheme is not even CPA-secure!

- CPA-security implies CPA-security for multiple encryptions;
- the attacker can submit (m, m) and (m, m') and deduce from the challenge ciphertexts which messages were encrypted.

Mac then Enc

It does not lead to an authenticated encryption in general.

- The CBC-mode encryption is CPA-secure but not CCA-secure, since the padding oracle attack applies.



- If $\mathcal{A}$ distinguishes between decryption and verification failure, they can still exploit the padding oracle attack.

Enc then Mac

The symmetric-key encryption scheme

$$S' = (\text{KeyGen}', \text{Enc}', \text{Dec}')$$

is defined from Π_E and Π_M as follows:

- $k \leftarrow \text{KeyGen}'(n)$: runs KeyGen_E and KeyGen_M on the security parameter n, obtaining k_1, k_2. Then $k = (k_1, k_2)$;
- $c_E \leftarrow \text{Enc}'(k, m)$: computes $c \leftarrow \text{Enc}(k_1, m)$ and then $t \leftarrow \text{Mac}(k_2, c)$. The ciphertext c_E is (c, t).
- $m \leftarrow \text{Dec}'(k, c_E)$:
  - if $\text{Verify}(k_2, c, t) = 1$, then it outputs $\text{Dec}(k_1, c)$;
  - otherwise, it outputs $\perp$.

Enc then Mac

If Π_E is CPA-secure and Π_M is strongly secure, then S' is an authenticated encryption scheme.

Enc then Mac

If Π_E is CPA-secure and Π_M is strongly secure, then S' is an authenticated encryption scheme.

Sketch of the proof:

- (c, t) is a valid ciphertext if $\text{Verify}(k_2, c, t) = 1$;
- $\mathcal{A}$ cannot generate a new ciphertext (i.e. not obtained from the encryption oracle) since Π_M is strongly secure;
- hence, S' is unforgeable and $\mathcal{A}$ cannot benefit from the decryption oracle of the CCA indistinguishable experiment;
- therefore, CPA-security of Π_E is enough.

Authenticated Encryption: Possible Attacks

An authenticated encryption is not enough, on its own, to provide full integrity over a communication channel.

Authenticated Encryption: Possible Attacks

An authenticated encryption is not enough, on its own, to provide full integrity over a communication channel.

- Replay attack: replay a previously-sent valid ciphertext.
- Reflection attack: change the direction of a message resending it to the sender instead of the receiver.

Authenticated Encryption: Possible Attacks

An authenticated encryption is not enough, on its own, to provide full integrity over a communication channel.

- Replay attack: replay a previously-sent valid ciphertext.
- Reflection attack: change the direction of a message resending it to the sender instead of the receiver.

Counters to prevent the first attack; different encryption keys for different directions, i.e. $K_{A \to B} \neq K_{B \to A}$, for the third.

Further Reading I

N.J. Al Fardan and K.G. Paterson.
Lucky thirteen: Breaking the TLS and DTLS record protocols.
In Security and Privacy (SP), 2013 IEEE Symposium on, pages 526–540, May 2013.

J Lawrence Carter and Mark N Wegman.
Universal classes of hash functions.
In Proceedings of the ninth annual ACM symposium on Theory of computing, pages 106–112. ACM, 1977.

Jean Paul Degabriele and Kenneth G Paterson.
On the (in) security of IPsec in MAC-then-Encrypt configurations.
In Proceedings of the 17th ACM conference on Computer and communications security, pages 493–504. ACM, 2010.

Further Reading II

Ted Krovetz and Phillip Rogaway.
The software performance of authenticated-encryption modes.
In Fast Software Encryption, pages 306–327. Springer, 2011.

Douglas R. Stinson.
Universal hashing and authentication codes.
Designs, Codes and Cryptography, 4(3):369–380, 1994.