Introduction to Cryptology

6.3 - Information Theoretic MACs

Federico Pintore

Mathematical Institute, University of Oxford (UK)

UNIVERSITY OF OXFORD

Michaelmas term 2020

Information Theoretic MACs

So far, we have considered computational security for MACs.

Does there exist a MAC that is secure even in the presence of unbounded adversaries?

Information Theoretic MACs

So far, we have considered computational security for MACs.

Does there exist a MAC that is secure even in the presence of unbounded adversaries?

- The probability of guessing a valid tag is at least $1/2^{|t|}$ (where $|t|$ is the tag length).
- Information theoretic MACs: success probability cannot be better than $1/2^{|t|}$.
- Achievable provided that the number of messages that can be authenticated is bounded.

Information Theoretic MACs

Basic case: only one message can be authenticated.

Information Theoretic MACs

Basic case: only one message can be authenticated.

One-time Message Authentication Experiment $\mathrm{Mac}^{1-\mathrm{unforg}}_{\mathcal{A},S}$

Challenger Ch	Adversary $\mathcal{A}$
$k \leftarrow \mathrm{KeyGen}$	
	One query m' to Mac_k
$t' = \mathrm{Mac}_k(m')$ is sent	
	Outputs a forgery (m, t)

Information Theoretic MACs

Basic case: only one message can be authenticated.

One-time Message Authentication Experiment $\text{Mac}_{\mathcal{A},S}^{1-\text{unforg}}$

Challenger Ch	Adversary $\mathcal{A}$
$k \leftarrow \text{KeyGen}$	
	One query m' to Mac_k
$t' = \text{Mac}_k(m')$ is sent	
	Outputs a forgery (m, t)

$\mathcal{A}$ wins the game, i.e. $\text{Mac}_{\mathcal{A},S}^{1-\text{unforg}} = 1$, if:

- $\text{Verify}_k(m, t) = 1$;
- $m \neq m'$.

Information Theoretic MACs

Definition

A message authentication code S is one-time ϵ-secure if, for every adversary $\mathcal{A}$ (including unbounded ones), it holds that

$$\Pr(\mathrm{Mac}^{1-time}_{\mathcal{A},S} = 1) \leq \epsilon.$$

Information Theoretic MACs

To construct information theoretic MACs, strongly universal functions[1] can be used.

[1] Also called pairwise-independent functions

Information Theoretic MACs

To construct information theoretic MACs, strongly universal functions[1] can be used.

Definition

A keyed function $h : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$*, where* $h(k, m) := h_k(m)$*, is strongly universal if, for all* $m \neq m'$ *and* $t, t' \in \mathcal{T}$*, it holds*

$$\Pr(h_k(m) = t \wedge h_k(m') = t') = 1/|\mathcal{T}|^2$$

where the probability is taken over uniform choice of $k \in K$*.*

[1] Also called pairwise-independent functions

An Information Theoretic MAC

Let $h : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$ be a strongly universal function. Define a MAC

$$S = (\text{KeyGen}, \text{Mac}, \text{Verify})$$

with message space $\mathcal{M}$ as follows:

- $k \leftarrow \text{KeyGen}$: outputs a uniform element k from $\mathcal{K}$.
- $t \leftarrow \text{Mac}(k, m)$: outputs the tag $h_k(m)$.
- $1/0 \leftarrow \text{Verify}(k, m, t)$: outputs 1 if $m \in \mathcal{M}$ and $t == h_k(m)$, 0 otherwise (canonical verification).

An Information Theoretic MAC

Let $h : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$ be a strongly universal function. Define a MAC

$$S = (\text{KeyGen}, \text{Mac}, \text{Verify})$$

with message space $\mathcal{M}$ as follows:

- $k \leftarrow \text{KeyGen}$: outputs a uniform element k from $\mathcal{K}$.
- $t \leftarrow \text{Mac}(k, m)$: outputs the tag $h_k(m)$.
- $1/0 \leftarrow \text{Verify}(k, m, t)$: outputs 1 if $m \in \mathcal{M}$ and $t == h_k(m)$, 0 otherwise (canonical verification).

Theorem

The message authentication code S is one-time $1/|\mathcal{T}|$-secure.

An Example of Strongly Universal Function

Example

Consider $\mathbb{Z}_p$ for a prime p. Let:

- $\mathcal{M} = \mathcal{T} = \mathbb{Z}_p$, and
- $\mathcal{K} = \mathbb{Z}_p \times \mathbb{Z}_p$.

Define the keyed function $h : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$ as

$$h_{a,b}(m) = a \cdot m + b \mod p.$$

An Example of Strongly Universal Function

Example

Consider $\mathbb{Z}_p$ for a prime p. Let:

- $\mathcal{M} = \mathcal{T} = \mathbb{Z}_p$, and
- $\mathcal{K} = \mathbb{Z}_p \times \mathbb{Z}_p$.

Define the keyed function $h : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$ as

$$h_{a,b}(m) = a \cdot m + b \mod p.$$

Theorem

For any prime p, the function h is strongly universal.

Limitations of Information Theoretic MACs

Theorem

If S is a one-time 2^{-n}-secure message authentication code with constant size keys, then

$$|k| \geq 2n.$$

Limitations of Information Theoretic MACs

Theorem

If S is a one-time 2^{-n}-secure message authentication code with constant size keys, then

$$|k| \geq 2n.$$

Theorem

If S is a ℓ-time 2^{-n}-secure message authentication code with constant size keys, then $|k| \geq (\ell + 1)n$.

Limitations of Information Theoretic MACs

Theorem

If S is a one-time 2^{-n}-secure message authentication code with constant size keys, then

$$|k| \geq 2n.$$

Theorem

If S is a ℓ-time 2^{-n}-secure message authentication code with constant size keys, then $|k| \geq (\ell + 1)n$.

Corollary

If the key-length of a given MAC is bounded, then it is not information-theoretic secure when authenticating an unbounded number of messages.

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.