CS 346 Class Notes

Mark Lindberg

Feb 22, 2016

Last Time:
Π' is an authentication scheme if it is

1. Unforgeable.
2. CCA-secure.

We built one last time from a CPA-secure encryption scheme Π_E, and a strongly secure MAC Π_M, using the "Encrypt, then authenticate" mentality.
The key claim was that Pr[valid query] is negligible.
Then $\mathcal{A}$ passes some (c, t) to Dec'_k oracle such that

1. $\mathsf{Dec}'_k((c, t)) \neq \perp$
2. (c, t) is not the output of a prior Enc'_k query.

This Time:
It remains to show that Π' is a CCA-secure.
Fix an adversary $\mathcal{A}$ in the experiment. Let $\mathsf{PrivK}^{\mathsf{CCA}}_{\mathcal{A},\Pi'}(n) = 1$ be the event "$\mathcal{A}$ succeeds".
We need $\Pr[\mathcal{A} \text{ succeeds}] \leq \frac{1}{2} + \mathtt{negl}(n)$.
Proof idea: Create an adversary $\mathcal{A}_E$ for the experiment $\mathsf{PrivK}^{\mathsf{CPA}}_{\mathcal{A}_E,\Pi_E}(n)$ that simulates $\mathcal{A}$.
$\mathcal{A}_E$ need to simulate oracle queries of $\mathcal{A}$. A key k_M is chosen at uniform.
Case 1: $\mathcal{A}_E$ calls Enc_{k_E} oracle on m, gets c. $\mathcal{A}_E$ computes $t = \mathsf{Mac}_{k_M}(c)$. $\mathcal{A}_E$ gives (c, t) to $\mathcal{A}$.
Case 2: $\mathcal{A}$ calls Dec'_k oracle on (c, t). If (c, t) output of a previous Enc'_k call, output corresponding m. Otherwise, return $\perp$.

$$\begin{aligned}\Pr[\mathcal{A} \text{ succeeds}] &= \Pr[\mathcal{A} \text{ succeeds} \wedge \text{valid query}] + \Pr[\mathcal{A} \text{ succeeds} \wedge \overline{\text{valid query}}] \\ &\leq \Pr[\text{valid query}] + \Pr[\mathcal{A} \text{ succeeds} \wedge \overline{\text{valid query}}]\end{aligned}$$

$\mathring{A}$ decides on m_1, m_2. $\mathcal{A}_E$ picks the same m_1, m_2. Gets back the ciphertext $\mathsf{Enc}_{k_E}(m_b)$. $\mathcal{A}_E$ computes $t = \mathsf{Mac}_{k_M}(c)$. It return (c, t) to $\mathcal{A}$.

The simulation of $\mathcal{A}$ by $\mathcal{A}_E$ is faithful as long as "valid query" does not occur.

$$\begin{aligned}\Pr[\mathcal{A} \text{ succeeds} \wedge \overline{\text{valid query}}] &= \Pr[\mathcal{A}_E \text{ succeeds} \wedge \overline{\text{valid query}}] \\ &\leq \Pr[\mathcal{A}_E \text{ succeeds}] \\ &\leq \frac{1}{2} + \mathtt{negl}(n)\end{aligned}$$

There's a nice example showing that it is crucial that k_E, k_M are chosen independently. Suppose both were set to the same k, F is a strong PRP. This implies that F^{-1} is also a strong PRP. (Pseudo-random permutation)

The CCA-scheme for $\frac{n}{2}$ bit messages is $c = F_k(r||m)$, where both are $\frac{n}{2}$-bit blocks.

For the strongly secure MAC, it is possible to use $t = F_k^{-1}(m)$. Yeah, uh...

If we compose them, the tag is the unencrypted message.

Section 4.7: Information-theoretic MACs.

Experiment: $\mathsf{Mac\text{-}forge}_{\mathcal{A},\Pi}^{1-\text{time}}$. $\mathcal{M}$ is the message space. $\mathcal{T}$ is the tag space. $\mathcal{K}$ is the key space. $\mathcal{A}$ picks a message $m' \in \mathcal{M}$, calls Mac_k oracle to get t'. $\mathcal{A}$ outputs a pair (m, t). $\mathcal{A}$ succeeds if $\mathsf{Vrfy}_k(m, t) = 1$ AND $m \neq m'$.

Is there a MAC Π such that $\Pr[\mathsf{Mac\text{-}forge}_{\mathcal{A},\Pi}^{\text{1-time}} = 1] \leq \frac{1}{|\mathcal{T}|}$ for ALL $\mathcal{A}$? (Not restricted to PPT.)

Yes. If we use a "strong universal function," also called a pairwise-independent family of functions or strongly uniform family of hash functions.

f is strongly universal if $\forall m, m'$ such that $m \neq m'$ and $t, t' \in \mathcal{T}$, $\Pr[f_k(m) = t \wedge f_k(m') = t'] = \frac{1}{|\mathcal{T}|^2}$.

Theorem: A strongly universal f gives a MAC Π which satisfies spiderweb.

Define $\mathsf{Mac}_k(m)$ is $f_k(m)$, with canonical verification.

Claim 1: $\forall m \in \mathcal{M}, t\mathcal{T} = \mathsf{Mac}_k(m)$, $\Pr[f_k(m) = t] = \frac{1}{|\mathcal{T}|}$.

Let $m' \in \mathcal{M}$, $m' \neq m$ (assuming $|\mathcal{M}| \geq 2$). Then

$$\begin{aligned}\Pr[f_k(m) = t] &= \sum_{t \in \mathcal{T}} \Pr[f_k(m) = t \wedge f_k(m') = t'] \\ &= \sum_{t \in \mathcal{T}} \frac{1}{|T|^2} \\ &= \frac{|\mathcal{T}|}{|\mathcal{T}|^2} \\ &= \frac{1}{|\mathcal{T}|}\end{aligned}$$

Then by conditional probability,

$$
\begin{aligned}
&\Pr[f_k(m) = t \mid f_k(m') = t'] \\
&\qquad = \frac{\Pr[f_k(m) = t \wedge f_k(m') = t']}{\Pr[f_k(m') = t']} \\
&\qquad = \frac{\frac{1}{|\mathcal{T}|^2}}{\frac{1}{|\mathcal{T}|}} \\
&\qquad = \frac{1}{|\mathcal{T}|}
\end{aligned}
$$

The classic strong universal function. Pick a prime p. Let $\mathcal{K} = \mathbb{Z}_p \times \mathbb{Z}_p$, $\mathcal{M} = \mathbb{Z}_p$, and $\mathcal{T} = \mathbb{Z}_p$.

$f_{a,b}(m) = (a \times m + b) \mod p$.

EXAM:

Study problem sets 1 and 2 solutions! Remember and learn the basic definitions and concepts.

PRG, PRF, PRP, weak PRF.

Notesheet, writing on both sides. Can be printed. YESSSSSS.