COS433/Math 473: Cryptography

Mark Zhandry
Princeton University
Spring 2017
Message Authentication Codes

Syntax:
• Key space $K_\lambda$
• Message space $M$
• Tag space $T_\lambda$
• $MAC(k,m) \rightarrow \sigma$
• $Ver(k,m,\sigma) \rightarrow 0/1$

Correctness:
• $\forall m,k, Ver(k,m, MAC(k,m)) = 1$
Message Authentication Codes

Goal: If Eve changed $m$, Bob should reject
Security For MACs

\[
m_i \in M \quad \Rightarrow \quad \sigma_i \quad \Rightarrow \quad (m^*, \sigma^*)
\]

\[
k \leftarrow K_\lambda
\]
\[
\sigma \leftarrow \text{MAC}(k, m_i)
\]

Output 1 iff:
- \( m^* \notin \{m_1, \ldots \} \)
- \( \text{Ver}(k, m^*, \sigma^*) = 1 \)

\[
\text{CMA-Adv}(\hat{\tau}, \lambda) = \Pr[\ \text{outputs 1}]
\]
Constructing MACs

Use a PRF

\[ F:K \times M \rightarrow T \]

\[ MAC(k,m) = F(k,m) \]
\[ Ver(k,m,\sigma) = (F(k,m) == \sigma) \]

Theorem: \((MAC, Ver)\) is CMA secure assuming \(1/|T|\) is negligible
Theorem: CBC-MAC is a secure PRF for fixed-length messages
Today

Improving Efficiency of MACs

Authenticated Encryption: combining secrecy and integrity
Improving efficiency
Limitations of CBC-MAC

Many block cipher evaluations

Sequential
Carter Wegman MAC

\[ k' = (k, h) \] where:

- \( k \) is a PRF key for \( F:K \times \mathbb{R} \rightarrow \mathbb{Y} \)
- \( h \) is sampled from a pairwise independent function family

\[ \text{MAC}(k', m) : \]

- Choose a random \( r \leftarrow \mathbb{R} \)
- Set \( \sigma = (r, F(k, r) \oplus h(m)) \)
**Theorem:** The Carter Wegman MAC is strongly CMA secure
Proof

Assume toward contradiction a PPT 🦾

Hybrids...
Proof

Hybrid 0

\[ k \leftarrow K \]
\[ h \]
\[ r_i \leftarrow R \]
\[ t_i \leftarrow F(k, r) \oplus h(m) \]

Output 1 iff:
1. \((m^*, r^*, t^*) \notin \{(m_i, r_i, t_i)\}\)
2. \(F(k, r^*) \oplus h(m^*) = t^*\)
Proof

Hybrid 1

Output 1 iff:
• \((m^*,r^*,t^*)\notin\{(m_i,r_i,t_i)\}\)
• \(F(k,r^*)\oplus h(m^*)=t^*\)
Proof

Hybrid 2

Proof:

\[ m_i \in M \]
\[ \sigma_i = (r_i, t_i) \]
\[ (m^*, r^*, t^*) \]

Output 1 iff:

- \( (m^*, r^*, t^*) \notin \{(m_i, r_i, t_i)\} \)
- \( H(r^*) \oplus h(m^*) = t^* \)

\( H \leftarrow \text{Funcs} \)
\[ h \]
\( (\text{Distinct } r_i) \)
\[ r_i \leftarrow R \]
\[ t_i \leftarrow H(r) \oplus h(m) \]
Proof

Claim: In Hybrid 2, negligible success probability

Possibilities:
- \( r^* \notin \{r_i\} \): then value of \( H(r^*) \) hidden from adversary, so \( \Pr[H(r^*) \oplus h(m^*) = t^*] \) is \( 1/|Y| \)
- \( r^* = r_i \) for some \( i \): then \( m^* \neq m_i \) (why?)
  \( h \) completely hidden from adversary
  \[ \Pr[H(r^*) \oplus h(m^*) = t^*] = \Pr[h(m^*) = t^* \oplus t_i \oplus h(m_i)] = 1/|Y| \]
Proof

Hybrid 1 and 2 are indistinguishable
• PRF security

Hybrid 0 and 1 are indistinguishable
• W.h.p. random $r_i$ will be distinct

Therefore, negligible success probability in Hybrid 0
Efficiency of CW MAC

\text{MAC}(k',m): 
\begin{itemize}
  \item Choose a random \( r \leftarrow R \)
  \item Set \( \sigma = (r, F(k,r) \oplus h(m)) \)
\end{itemize}

\( h \) much more efficient than PRFs

PRF applied only to small nonce \( r \)
\( h \) applied to large message \( m \)
PMAC: A Parallel MAC

\[ p \oplus k' \oplus F \oplus k' \oplus F \oplus k' \oplus F \oplus k' \oplus F \oplus k' \oplus F \oplus k' \oplus F \oplus k' \oplus F \oplus k' \oplus F \oplus k' \oplus k' \oplus p \oplus (p) \]

\[ \sigma \rightarrow F \rightarrow k \]
Authenticated Encryption
Authenticated Encryption

Goal: Eve cannot learn nor change plaintext
- Authenticated Encryption will satisfy two security properties
Syntax

Syntax:
• Enc: $K \times M \rightarrow C$
• Dec: $K \times C \rightarrow M \cup \{\perp\}$

Correctness:
• For all $k \in K$, $m \in M$, $\text{Dec}(k, \text{Enc}(k,m)) = m$
Unforgeability

\[ k \leftarrow K_{\lambda} \]
\[ c \leftarrow Enc(k,m_i) \]

Output 1 iff:
- \[ c^* \notin \{c_1, \ldots\} \]
- \[ \text{Dec}(k,c^*) \neq \perp \]
Definition: An encryption scheme \((\text{Enc}, \text{Dec})\) is an authenticated encryption scheme if it is unforgeable and CPA secure.
Constructing Authenticated Encryption

Three possible generic constructions:

1. MAC-then-Encrypt (SSL)

\[ k = (k_{\text{Enc}}, k_{\text{MAC}}) \]

\[ \text{MAC}(k_{\text{MAC}}, m) \]

\[ \text{Enc}(k_{\text{Enc}}, (m, \sigma)) \]

\[ \text{Dec}(k_{\text{Enc}}, c) \]

\[ \text{Ver}(k_{\text{MAC}}, m, \sigma) \]

\[ m \]

Accept

Reject
Constructing Authenticated Encryption

Three possible generic constructions:

2. Encrypt-then-MAC (IPsec)

\[ k = (k_{Enc}, k_{MAC}) \]

\[ Enc(k_{Enc}, m) \]

\[ MAC(k_{MAC}, c') \]
Constructing Authenticated Encryption

Three possible generic constructions:

3. Encrypt-and-MAC (SSH)

\[ k = (k_{Enc}, k_{MAC}) \]

\[ m \]

\[ \text{MAC}(k_{MAC}, m) \]

\[ \text{Enc}(k_{Enc}, m) \]

\[ c' \sigma \]

\[ c \]
Constructing Authenticated Encryption

1. MAC-then-Encrypt
2. Encrypt-then-MAC
3. Encrypt-and-MAC

Which one(s) **always** provides authenticated encryption (assuming strongly secure MAC)?
Constructing Authenticated Encryption

MAC-then-Encrypt?
Constructing Authenticated Encryption

Encrypt-then-MAC?
Constructing Authenticated Encryption

Encrypt-and-MAC?
Constructing Authenticated Encryption

Just because MAC-then-Encrypt and Encrypt-and-MAC are insecure for some MACs/encryption schemes, they may be secure in some settings.

Ex: MAC-then-Encrypt with CTR or CBC encryption
- For CTR, any one-time MAC is actually sufficient.
Theorem: MAC-then-Encrypt with any one-time MAC and CTR-mode encryption is an authenticated encryption scheme
Proof

CPA security: straightforward
• CPA security of encryption scheme guarantees message + mac is hidden
Proof

Integrity: assume towards contradiction a PPT ciphertext forger 🛡

Hybrids...
Proof

Hybrid 0:

\[ m_i \in M \quad (r_i, c_i) \quad (r^*, c^*) \]

\[ k_{\text{MAC}} \leftarrow K_{\text{MAC}} \]
\[ k_{\text{PRF}} \leftarrow K_{\text{PRF}} \]
\[ \sigma_i \leftarrow \text{MAC}(k_{\text{MAC}}, m_i) \]
\[ r_i \leftarrow R \]
\[ c_i \leftarrow F(k_{\text{PRF}}, r) \oplus (m_i, \sigma_i) \]

Output 1 iff:
- \((r^*, c^*) \notin \{(r_1, c_1), \ldots\}\)
- \(\text{Ver}(k_{\text{MAC}}, m^*, \sigma^*) = 1\) where
  \[(m^*, \sigma^*) \leftarrow F(k_{\text{PRF}}, r^*) \oplus c^*\]

Standard forgery experiment
Proof

Hybrid 1:

\[ m_i \in M \]
\[ (r_i, c_i) \]
\[ (r^*, c^*) \]

\[ k_{MAC} \leftarrow K_{MAC} \]
\[ H \leftarrow \text{Funcs} \]

\[ \sigma_i \leftarrow \text{MAC}(k_{MAC}, m_i) \]
\[ r_i \leftarrow R \]
\[ c_i \leftarrow H(r_i) \oplus (m_i, \sigma_i) \]

Output 1 iff:

- \((r^*, c^*) \notin \{(r_1, c_1), ...\}\)
- \(\text{Ver}(k_{MAC}, m^*, \sigma^*) = 1\) where \((m^*, \sigma^*) \leftarrow H(r^*) \oplus c^*\)
Proof

Hybrid 2:

\[ m_i \in M \]
\[ (r_i, c_i) \]
\[ (r^*, c^*) \]

\[ k_{MAC} \leftarrow K_{MAC} \]
\[ H \leftarrow Funcs \]
\[ \sigma_i \leftarrow MAC(k_{MAC}, m_i) \]
\[ r_i \leftarrow R \text{ (distinct)} \]
\[ c_i \leftarrow H(r_i) \oplus (m_i, \sigma_i) \]

Output 1 iff:

- \((r^*, c^*) \notin \{(r_1, c_1), \ldots\}\)
- \(\text{Ver}(k_{MAC}, m^*, \sigma^*) = 1\) where \((m^*, \sigma^*) \leftarrow H(r^*) \oplus c^*\)
Proof

Hybrid 3:

Setting:

\[ m_i \in M \]
\[ (r_i, c_i) \]
\[ (r^*, c^*) \]

\[ k_{MAC} \leftarrow K_{MAC} \]
\[ H \leftarrow Funcs \]

\[ \sigma_i \leftarrow MAC(k_{MAC}, m_i) \]
\[ r_i \leftarrow R \text{ (distinct)} \]
\[ c_i \leftarrow H(r) \oplus (m_i, \sigma_i) \]

Output 1 iff:

- \((r^*, c^*) \notin \{(r_1, c_1), \ldots\}\)
- \(r^* \in \{r_1, \ldots\}\)
- \(Ver(k_{MAC}, m^*, \sigma^*) = 1\)
- where \((m^*, \sigma^*) \leftarrow H(r^*) \oplus c^*\)
Proof

Hybrid 0 and Hybrid 1 are indistinguishable by PRF security

Hybrid 1 and Hybrid 2 are indistinguishable since the r’s are distinct with overwhelming probability

Hybrid 2 and Hybrid 3 are indistinguishable since if $r^* \notin \{r_1, \ldots\}$, then $H(r^*)$ hidden from adversary’s view

• For any $c^*$, $(m^*, \sigma^*) = H(r^*) \oplus c^*$ truly random
  → forgery with negligible probability
Proof

Suppose non-negligible prob of forgery in Hyb 3

Pick random $i^* \in \{1, \ldots, q\}$

If $i \neq i^*$, choose random $(r_i, c_i)$

If $i = i^*$,
  
  • Choose random $r_i^*, k^*$
  
  • $c_i^* \leftarrow k^* \oplus (m_i, \sigma)$

If $r^* \neq r_i^*$, abort

If $r^* = r_i^*$,
  
  • $(m^*, \sigma^*) \leftarrow k^* \oplus c^*$
Proof

Analysis

• Regardless of which $i^*$ picks, sees truly random ciphertexts (with distinct $r$)

• Therefore, $i^*$ independent of view of

• Forges exactly when $i^*$ forges AND guessed correct $i^*$

• $\Rightarrow$ Prob $forges$ is non-negligible
Chosen Ciphertext Attacks
Chosen Ciphertext Attacks

Often, adversary can fool server into decrypting certain ciphertexts

Even if adversary only learns partial information (e.g. whether ciphertext decrypted successfully), can use info to decrypt entire message

Therefore, want security even if adversary can mount decryption queries
Chosen Plaintext Security

\[ \text{Chosen Plaintext Security} \]

\[ \mathbf{b} \]

\[ \mathbf{k} \leftarrow \mathbf{K} \]

\[ \mathbf{c} \leftarrow \text{Enc}(\mathbf{k}, \mathbf{m}) \]

\[ \mathbf{c} \leftarrow \text{Enc}(\mathbf{k}, \mathbf{m}_b) \]

\[ \mathbf{c} \leftarrow \text{Enc}(\mathbf{k}, \mathbf{m}) \]

\[ \text{CPA-Exp}_{\mathbf{b}}(\text{\small \text{Charlie}}, \lambda) \]
Chosen Ciphertext Security?

\[ \begin{align*}
    k &\leftarrow K \\
    c &\leftarrow \text{Enc}(k,m) \\
    m &\leftarrow \text{Dec}(k,c) \\
    c^* &\leftarrow \text{Enc}(k,m_{b^*})
\end{align*} \]
Lunch-time CCA (CCA1)
Full CCA (CCA2)

\[ k \leftarrow K \]
\[ c \leftarrow \text{Enc}(k, m) \]
\[ m \leftarrow \text{Dec}(k, c) \]
\[ c^* \leftarrow \text{Enc}(k, m_{b^*}) \]
Theorem: If \((\text{Enc}, \text{Dec})\) is an authenticated encryption scheme, then it is also CCA secure
Proof Sketch

For any decryption query, two cases

1. Was the result of a CPA query
   • In this case, we know the answer already!

2. Was not the result of an encryption query
   • In this case, we have a ciphertext forgery
CCA vs Auth Enc

We know Auth Enc implies CCA security

What about the other direction?

For now, always strive for Authenticated Encryption
MAC-then-Encrypt with CBC

Even though MAC-then-Encrypt is secure for CBC encryption (which we did not prove), still hard to implement securely.

Recall: need padding for CBC

Therefore, two possible sources of error
  • Padding error
  • MAC error

If possible to tell which one, then can attack
Using Same Key for Encrypt and MAC

Suppose we’re combining CBC encryption and CBC-MAC

Can I use the same key for both?
Attack?
Using Same Key for Encrypt and MAC

In general, do not use same key for multiple purposes
• Schemes may interact poorly when using the same key

However, some modes of operation do allow same key to be used for both authentication and encryption
CCM Mode

CCM = Counter Mode with CBC-MAC in Authenticate-then-Encrypt combination

Possible to show that using same key for authentication and encryption still provides security
Efficiency

So far, all modes seen require two block cipher operations per block
• 1 for encryption
• 1 for authentication

Ideally, would have only 1 block cipher op per block
OCB Mode

\[ \Delta \leftarrow \text{Init}(N) \]
\[ \Delta \leftarrow \text{Inc}_1(\Delta) \]
\[ \Delta \leftarrow \text{Inc}_2(\Delta) \]
\[ \Delta \leftarrow \text{Inc}_3(\Delta) \]
\[ \Delta \leftarrow \text{Inc}_4(\Delta) \]

\[ M_1 \quad M_2 \quad M_3 \quad M_4 \]

\[ \oplus \quad \oplus \quad \oplus \quad \oplus \]
\[ \Delta \quad \Delta \quad \Delta \quad \Delta \]

\[ E_K \quad E_K \quad E_K \quad E_K \]

\[ \oplus \quad \oplus \quad \oplus \quad \oplus \]
\[ \Delta \quad \Delta \quad \Delta \quad \Delta \]

\[ C_1 \quad C_2 \quad C_3 \quad C_4 \]

\[ \Delta \leftarrow \text{Inc}_5(\Delta) \]

\[ \oplus \quad \oplus \quad \oplus \quad \oplus \]
\[ \Delta \]

\[ \text{Checksum} \]

\[ E_K \]

\[ \text{Final} \quad \text{Tag} \quad \text{Auth} \]

\[ T \]
OCB Mode

Twice as fast as other block cipher modes of operation

However, not used much in practice
• Patents!
Other Modes

GCM: Roughly CTR mode then Carter-Wegman MAC

EAX: CTR mode then CMAC (variant of CBC-MAC)
Deterministic Encryption
Deterministic Encryption

So far, we have insisted on CPA/CCA/Auth Enc security, which implies scheme must be randomized.

However, sometimes deterministic encryption is necessary.
• E.g. encrypting database records

How to resolve discrepancy?
Deterministic CPA Security

Where \( m_1^{(1)}, \ldots, m_1^{(q)} \) are distinct and \( m_1^{(1)}, \ldots, m_1^{(q)} \) are distinct
Achieving Det. CPA Security

Idea? used fixed det. IV
• CTR mode?
• CBC mode?

Better options:
• Derive IV as $\textbf{IV} = \text{PRF}(k',m)$
  • If using Auth Enc, get Det. Auth Enc
• Use “large” PRP: $c = \text{PRP}(k,m)$
  • Can get Det. Auth Enc by padding message
Next Time

Collision resistant hashing

Reminder: Starting at 3pm, midterm will be posted on Blackboard (though not on course webpage)
• Due 1pm on Wednesday