CSCI 1510

- Block Cipher Modes of Operation (continued)
- Practical Constructions of Hash Function
- Midterm Review
Block Cipher Modes of Operation

$F : \mathbb{F}_2^n \times \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$

Goal: Construct a CPA-secure encryption scheme for arbitrary-length messages.
Electronic Code Book (ECB) Mode

$$m = \begin{array}{c} m_1 \\ m_2 \\ m_3 \end{array}$$

**Enc:**

$$\begin{array}{c} F_k \\ F_k \\ F_k \end{array}$$

$$\begin{array}{c} c_1 \\ c_2 \\ c_3 \end{array}$$

**Dec:**

$$\begin{array}{c} F_k^{-1} \\ F_k^{-1} \\ F_k^{-1} \end{array}$$

$$\begin{array}{c} m_1 \\ m_2 \\ m_3 \end{array}$$

CPA secure? No!
Cipher Block Chaining (CBC) Mode

\[ M = \begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix} \]

\[ H_0: \text{Enc}(m_0) \]
\[ H_1: F_k \rightarrow f \]
\[ H_2: m_0 \rightarrow m_2 \]
\[ H_3: f \rightarrow F_k \]

Initialization Vector
\[ IV \leftarrow \{0,1\}^n \]

\[ C = \begin{bmatrix} IV \\ C_1 \\ C_2 \\ C_3 \end{bmatrix} \]

How to decrypt?
\[ F_k^{-1}(C_i) \oplus C_{i-1} \rightarrow m_i \]

CPA Secure? Yes!

Can we parallelize the computation? No for Enc, Yes for Dec.
Chained Cipher Block Chaining (CBC) Mode

\[ m = m_1 | m_2 | m_3 \]

\[ m' = m_4 | m_5 \]

\[ C = IV \oplus m_1 \oplus F_k (IV \oplus m_2) \oplus F_k (IV \oplus m_3) \]

\[ C' = C_4 \oplus C_5 \]

 CPA Secure?

\[ C = \text{IV} \parallel C_2 \parallel C_1 \parallel C_3 \]

\[ m^*_1 = C_3 \oplus \text{IV} \oplus m_2 \]

\[ m^*_2 = \text{arbitrary} \]

\[ C^* \]

\[ C^* \equiv C_1 \]
Counter (CTR) Mode

\[ \{0, 1\}^n \xrightarrow{\text{CTR}} \{0, 1\}^{n/2} \]

IV -> IV+1 -> IV+2 -> IV+3

\( H_0: \text{Enc}(m_0) \)

\( H_1: F_k \Rightarrow f \)

\( H_2: m_0 \Rightarrow m_1 \)

\( H_3: f \Rightarrow F_k \)

\[ C = \text{IV} \oplus \text{C}_1 \oplus \text{C}_2 \oplus \text{C}_3 \]

How to decrypt? \( F_k(\text{IV}+i) \oplus \text{C}_i \Rightarrow m_i \)

CPA secure? Yes!

Can we parallelize the computation? Yes!

PRG from PRF \( G_1: \{0, 1\}^{2n} \rightarrow \{0, 1\}^{3n} \)
Output Feedback (OFB) Mode

\( \{0,1\}^n \xrightarrow{\$} IV \)

\( F_k \)

\( m_1 \oplus m_2 \oplus m_3 \)

\( C = IV \oplus C_1 \oplus C_2 \oplus C_3 \)

How to decrypt?

CPA Secure?

Can we parallelize the computation?

PRG from PRF
Compression Function from Block Cipher

Block Cipher $\xrightarrow{\text{Davies-Meyer}}$ Compression Function $\xrightarrow{\text{Merkle-Damgård}}$ Arbitrary-length hash function (fixed-length hash function)

Input: $k \ x$

Output: $F(x)$

If $F$ is modeled as an "ideal cipher", then Davies-Meyer Construction is collision-resistant.
Practical Constructions of Hash Function

MD5: output length 128-bit
best know attack $2^{16}$
Collision found in 2004

Secure Hash Functions (SHA): Standardized by NIST.

- SHA-0: Standardized in 1993
  output length 160-bit
  best know attack $2^{39}$

- SHA-1: Standardized in 1995
  output length 160-bit
  best know attack $2^{63}$
  Collision found in 2017
Practical Constructions of Hash Function

Secure Hash Functions (SHA): Standardized by NIST.

- SHA-2: Standardized in 2001
  - Output length 224, 256, 384, 512-bit

- SHA-3: Competition 2007-2012
  - Released in 2015
  - Output length 224, 256, 384, 512-bit
Midterm Review

- Symmetric-Key Encryption
  - Syntax
  - Kerckhoff's Principle

- Perfect Security
  - Definition
  - Construction: One-Time Pad
  - Limitations: $|K| \geq |M|$

- Computational Security
  - Negligible function & Asymptotic approach
Midterm Review

* Computational Security for Message Secrecy
  * Semantic Security
    - Definition
    - Construction: Pseudo-OTP from PRG
    - Proof by reduction
    - Limitations: Cannot reuse key
  * CPA Security
    - Definition
    - Construction from PRF
    - Proof by hybrid argument + reduction
    - Limitations: Cannot query for decryption
  * CCA Security
    - Definition
Midterm Review

- Message Integrity
  * Message Authentication Code (MAC)
    - Syntax
    - Definitions: Secure / Strongly secure
    - Constructions
      Fixed-length MAC of length \( n \) from PRF
      Fixed-length MAC of length \( 2(n) \cdot n \) from PRF: CBC-MAC
      Arbitrary-length MAC: extension of CBC-MAC

- Unforgeability of Encryption Scheme
  - Definition

- Authenticated Encryption: Secrecy & Integrity
  - Definition: CCA Secure & Unforgeable
  - Constructions: CPA-Secure encryption + MAC
Midterm Review

- Practical Constructions
  - Block Cipher: PRP / PRF
  - Constructions: SPN / Feistel Network / DES / AES
  - Attacks on reduced rounds
  - Modes of Operation: pros & cons
Midterm Review

- Hash Function
  - Definition: Collision-Resistant
  - Birthday Attack & Implications
  - Merkle-Damgård Transform
  - Applications
  - Practical Constructions: Davies-Meyer / SHA