7.1 Stream Cipher Modes of Operation

The original DES Modes of Operation Specification (FIPS 81) specified four operating modes:

- Electronic Codebook (ECB) Mode
- Cipher Block Chaining (CBC) Mode
- Cipher Feedback (CFB) Mode
- Output Feedback (OFB) Mode

ECB mode was shown to be insecure last lecture. We will look at CFB and later CBC mode in this lecture.

7.2 CFB$: CFB Mode with a random Initialization Vector

![Figure 7.1: CFB$ Mode of Operation](image)

A few pragmatic characteristics: Encryption is not parallelizable, but decryption is. Any errors made during encryption are propagated through the remaining ciphertext.

We wish to show that if $E_K$ is a PRP, then $CFB[E_K]$ is real-or-random secure. Let $\ell$ be the number of blocks in a message.

**Theorem 7.1** If $E_K$ is a $(t, q, \epsilon)$ PRP, then $CFB[E_K]$ is $(t - O(q), q/\ell, \epsilon + \frac{q^2}{2^n})$ rr-secure.
Lecture 7: 2.7.05

Proof:

1. $\text{CFBS}[E_K] \sim \text{CFBS}[R]$; specifically, applying CFB mode to $E_K$ is $(t - O(q), \epsilon + \frac{q^2}{2^{n+1}})$-indistinguishable from applying CFB mode to a true random function.

   Since $E_K$ is a $(t,q,\epsilon)$-PRP, and CFB$ is a (randomized) algorithm computable in $O(q)$ time that queries its cipher $q$ times, $\text{CFB}[E_K]$ must be $(t - O(q), \epsilon)$-indistinguishable from $\text{CFBS}[RP]$, where $\text{RP}$ is a true random permutation or else CFB$ breaks $E_K$. Since a true random permutation is an $(\infty, q, q^2 2^{n+1})$-PRF, by similar reasoning $\text{CFB}[RP]$ is $(\infty, q^2 2^{n+1})$-indistinguishable from $\text{CFBS}[R]$. By the triangle inequality of indistinguishability, we get $\text{CFBS}[E_K]$ is $(t - O(q), \epsilon + \frac{q^2}{2^{n+1}})$-indistinguishable from $\text{CFBS}[R]$.

2. Define $\text{Bad} \equiv \exists (i, i') \neq (j, j') \cdot C_i[i'] = C_j[j']$, i.e. there exist messages $i, j$ such that distinct blocks of the messages $i', j'$ have the same ciphertext. If $\text{Bad}$ is false, then given a random oracle as the cipher, every ciphertext is a sequence of uniformly random blocks: $\text{CFBS}[R](m) | \text{Bad}$ is uniform.

3. $\Pr[\text{Bad}]$ is upper-bounded by a union bound: the sum of the chance that a bad event happens for the first time at all possible positions.

   $\Pr[\text{Bad}] \leq 0 + \frac{1}{2^n} + \frac{2}{2^n} + \ldots + \frac{q-1}{2^n} = \frac{q}{2^n} \leq \frac{q^2}{2^{n+1}}$

4. $\text{CFBS}[E_K](\$(M))$ is uniform. The xor of a uniform random value with anything is another uniform random value.

5. $\text{CFBS}[R](\cdot)$ is $(\infty, \frac{q^2}{2^{n+1}})$-indistinguishable from $\text{CFBS}[E_K](\$(\cdot))$. This is an application of the conditioning rule from Homework 1: when $\text{Bad}$ is false, $\text{CFBS}[R](\cdot)$ and $\text{CFBS}[E_K](\$(\cdot))$ are both uniform, so their distinguishability is information-theoretically limited by the probability that $\text{Bad}$ is true, which is no more than $\frac{q^2}{2^{n+1}}$.

Applying the triangle inequality to the indistinguishabilities in 1 and 5 yields that $\text{CFBS}[E_K](\$(\cdot))$ is $(t - O(q), \epsilon + \frac{q^2}{2^{n+1}})$-indistinguishable from $\text{CFBS}[E_K](\$(\cdot))$ assuming no more than $q$ queries are made. Since CFB$ makes $\ell$ queries, this makes it $(t - O(q), q/\ell, \epsilon + \frac{q^2}{2^n})$ real-or-random secure.

7.3 CTR$\$ and CTRC

Encryption and decryption can both be parallelized with either of these modes.

If $F_K$ is a $(t,q,\epsilon) - \text{PRF}$:

- $\text{CTR}[F_K]$ is $t - O(q), q/\ell, \epsilon + \frac{q^2}{2^{n+1}}$ real-or-random secure.
- $\text{CTRC}[F_K]$ is $t - O(q), q/\ell, \epsilon$ real-or-random secure.

7.4 CBC$\$: Cipher Block Chaining with random Initialization Vector

Lemma 7.2 $\text{CBC}[R]$ is $(\infty, \frac{q^2}{2^{n+1}})$-indistinguishable from $\$ \circ \text{CBC}[R]$.
Proof: Game-based proof with Games G0 and G1.

Common initialization steps

1. for $x \in \{0, 1\}^n$, $f(x) \leftarrow$ undefined
2. bad $\leftarrow$ false

Game G0. In response to oracle query, $M = (M_1, M_2, \ldots, M_\ell)$

1. $C_0 \leftarrow \{0, 1\}^n$
2. for $i \leftarrow 1, 2, \ldots, \ell$ do
3. \hspace{1em} $X_i \leftarrow M_i \oplus C_{i-1}$
4. \hspace{1em} $C_i \leftarrow \{0, 1\}^n$
5. \hspace{1em} if $X_i \in \text{Domain}(f)$, bad $\leftarrow$ true
6. \hspace{1em} \hspace{1em} $f(X_i) \leftarrow C_i$
7. Return $C = (C_0, C_1, \ldots, C_\ell)$
Game G0 returns a uniform random string. It implements $\circledast_{\mathrm{CBC}}[R]$

Game G1. In response to oracle query, $M = (M_1, M_2, \ldots, M_\ell)$

1. $C_0 \overset{\$}{\leftarrow}\{0,1\}^n$
2. for $i \leftarrow 1, 2, \ldots, \ell$ do
3. $X_i \leftarrow M_i \oplus C_{i-1}$
4. $C_i \overset{\$}{\leftarrow}\{0,1\}^n$
5. $X_i \in \text{Domain}(f)$, bad $\leftarrow$ true and $C_i = f(X_i)$
6. $f(X_i) \leftarrow C_i$
7. Return $C = (C_0, C_1, \ldots, C_\ell)$

Game G1 implements $\circledast_{\mathrm{CBC}}[R]$.

G0 and G1 are indistinguishable in the case where bad is false at their completion, so the distinguishability between them is bounded by the probability that bad is true.

$$\text{AdvA} \leq \Pr[A^{G0}; \text{bad} = \text{true}]$$

This is bounded by a union bound over the chance that bad is first set to true on a given $X_i$; for algorithm G0, $C_i$ is uniformly random, so $X_i$ is uniformly random and therefore has no correlation with any values already in the domain of $f$, so the chance of collision is bounded by

$$0 + \frac{1}{2^n} + \frac{2}{2^n} + \ldots + \frac{q-1}{2^n} = \frac{(q)}{2^n} \leq \frac{q^2}{2^{n+1}}$$

**Theorem 7.3** If $F_K$ is a $(t, q, \epsilon)$-PRF, $\circledast_{\mathrm{CBC}}[F_K]$ is $(t - O(q), q/\ell, 2\epsilon + \frac{q^2}{2^n})$ real-or-random secure.

**Proof:**

1. $\circledast_{\mathrm{CBC}}[F_K](\cdot)$ is $(t - O(q), \epsilon)$-indistinguishable from $\circledast_{\mathrm{CBC}}[R](\cdot)$ by data processing.
2. $\circledast_{\mathrm{CBC}}[R](\cdot)$ is $(\infty, \frac{q^2}{2^n})$-indistinguishable from $\$\circledast_{\mathrm{CBC}}[R](\cdot)$ by Lemma 7.2.
3. $\$(\circledast_{\mathrm{CBC}}[R](\cdot)) = \$(\circledast_{\mathrm{CBC}}[R](\$(\cdot)))$. They are uniform random strings of equal length.
4. $\$(\circledast_{\mathrm{CBC}}[R](\$(\cdot)))$ is $(\infty, \frac{q^2}{2^n})$-indistinguishable from (\circledast_{\mathrm{CBC}}[R](\$(\cdot)))$ by Lemma 7.2.
5. $\circledast_{\mathrm{CBC}}[F_K](\$(\cdot))$ is $(t - O(q), \epsilon)$-indistinguishable from $\circledast_{\mathrm{CBC}}[R](\$(\cdot))$ by data processing.

Repeated application of the triangle inequality for indistinguishability yeilds $\circledast_{\mathrm{CBC}}[F_K](\cdot)$ is $(t - O(q), 2\epsilon + \frac{q^2}{2^n})$-indistinguishable from $\circledast_{\mathrm{CBC}}[R](\$(\cdot))$ provided no more than $q$ queries are made to $E_K$. Since $\circledast_{\mathrm{CBC}}$ invokes $E_K$ $\ell$ times, this makes it $(t - O(q), q/\ell, 2\epsilon + \frac{q^2}{2^n})$ real-or-random secure. 

$\blacksquare$