CS276 Cryptography **Spring 2006**

Lecture 7: 2.7.05

Lecturer: David Wagner *Scribe: Adrian Mettler*

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

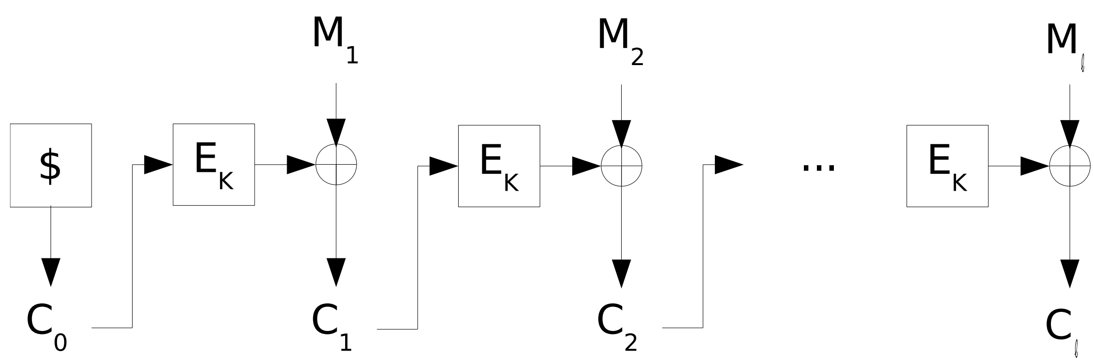

Figure 7.1: CFB\$ Mode of Operation

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 ℓ be the number of blocks in a message.

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

Proof:

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

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

3. $\Pr[Bad]$ 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.

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

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

5. $CFB\$[R](\cdot)$ is $(\infty, \frac{q^2}{2^{n+1}})$-indistinguishable from $CFB\$[E_K](\$(\cdot))$. This is an application of the conditioning rule from Homework 1: when Bad is false, $CFB\$[R](\cdot)$ and $CFB\$[E_K](\$(\cdot))$ are both uniform, so their distinguishability is information-theoretically limited by the probability that 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 yeilds that $CFB\$[E_K](\$(\cdot))$ is $(t - O(q), \epsilon+\frac{q^2}{2^n})$-indistinguishable from $CFB\$[E_K](\$(\cdot))$ assuming no more than q queries are made. Since $CFB\$$ makes ℓ 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 $(t, q, \epsilon) - PRF$:

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

7.4 CBC$: Cipher Block Chaining with random Initialization Vector

Lemma 7.2 *$CBC\$[R]$ is $(\infty, \frac{q^2}{2^{n+1}})$-indistinguishable from $\$ \circ CBC\$[R]$.*

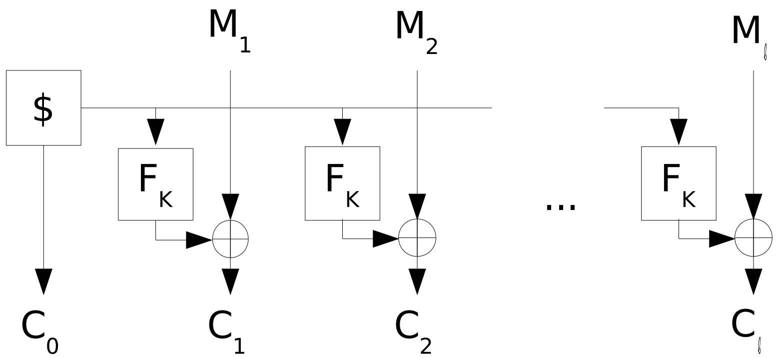

Figure 7.2: CTR$ Mode of Operation

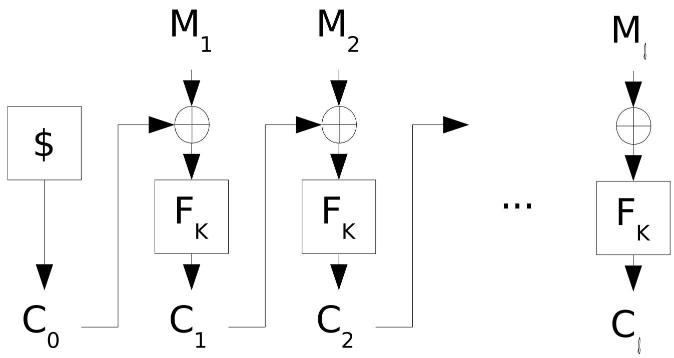

Figure 7.3: CBC$ Mode of Operation

Proof: Game-based proof with Games G0 and G1.

Common initialization steps

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

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

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

Game G0 returns a uniform random string. It implements $\$ \circ CBC\$[R]$.

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

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

Game G1 implements $CBC\$[R]$.

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*.

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

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

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

■

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

Proof:

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

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