Now, recall that \( F \) replace \( G \) middle games such that resulting in game \( G \) attacking \( F \). \( G \) have to start from some game \( A \) before we get into the proof, here are some remarks. In this kind of problems, we'll also a good PRF.

\[
\text{change from } f \text{ that } A \text{ as we shall see in our problem. In that case, we need to re-examine the adversary } A \text{ nothing. The change from past answers—if you repeat a prior query, you'll get the same prior answer—whereas the latter remembers nothing. The change from } f \text{ to $ may cost us a few games. Occasionally, the change might be problematic, as we shall see in our problem. In that case, we need to re-examine the adversary } A; \text{ often we can assume that } A \text{ belongs to a certain restricted class without loss of generality, but this restriction will smoothen the change from } f \text{ to $}. \text{ In our problem, we will assume that } A \text{ never repeats a prior query: the adversary can store the queries/answers it receives, and in both games } Real^A_F \text{ and } Rand^B_E, \text{ repeating a prior query will result in the same prior answer, which the adversary can retrieve from its storage without querying.}^1 \text{ Once we are in a game using $(), it'll be essentially the random game } Rand^B_E; \text{ one might need some equivalent transitions to make this explicit.}

In each game, we'll run \( A \) to produce a bit \( b' \)—we often write \( b' \leftrightarrow A^{Enc} \), meaning that the adversary \( A \) interacts with the oracle \( Enc \) and then outputs a bit \( b' \). The game then returns \( (b' = 1) \). Why returns \( (b' = 1) \)? For example, if \( G_0 \Rightarrow true \), it means that \( A \) outputs \( b' = 1 \) in the real game, in other words, \( Real^A_F \Rightarrow 1 \). Likewise, if \( G_t \Rightarrow true \), it means that \( A \) outputs \( b' = 1 \) in the random game, in other words, \( Rand^A_F \Rightarrow 1 \). Hence

\[
\Pr[G_0 \Rightarrow true] - \Pr[G_t \Rightarrow true] = \Pr[Real^A_F \Rightarrow 1] - \Pr[Rand^A_F \Rightarrow 1] = \text{Adv}^{prf}(A) .
\]

The proof. Let \( A \) be an efficient adversary attacking \( F \). Consider the following games \( G_0-G_4 \) in Figure 3.1. Game \( G_0 \) corresponds to the real game \( Real^A_F \), and game \( G_4 \) corresponds to the random game \( Rand^A_F \).

We now describe the game chain. Game \( G_1 \) is identical to game \( G_0 \), except that calls to \( E_K \) are replaced by

---

^1If we blindly impose this restriction, it may actually affect the complexity of \( A \), as it takes some additional cost (in both space and time) to store/retrieve the queries/answers. Thus the placement of the assumption needs to be handled with care.
Games $G_0, G_1$

$K \leftarrow \{0, 1\}^n$; $f \leftarrow \text{Func}(n)$; $b' \leftarrow A^{\text{Enc}}$

Return $(b' = 1)$

**procedure** $\text{ENC}(x)$

// For game $G_0$ only

Return $E_K(1||x)||E_K(0||x)$

// For game $G_1$ only

Return $f(1||x)||f(0||x)$

Game $G_2, G_3$

$b' \leftarrow A^{\text{Enc}}$

Return $(b' = 1)$

**procedure** $\text{ENC}(x)$

// For game $G_2$ only

$y_1 \leftarrow \{0, 1\}^n$; $y_2 \leftarrow \{0, 1\}^n$

Return $y_1||y_2$

// For game $G_3$ only

$y \leftarrow \{0, 1\}^{2n}$; Return $y$

Game $G_4$

$g \leftarrow \text{Func}(n - 1, 2n)$; $b' \leftarrow A^{\text{Enc}}$

Return $(b' = 1)$

**procedure** $\text{ENC}(x)$

Return $g(x)$

---

**Figure 3.1:** Games $G_0$–$G_4$. Here $	ext{Func}(n - 1, 2n)$ is the set of all functions $h : \{0, 1\}^{n-1} \rightarrow \{0, 1\}^{2n}$.

**Adversary $B^{\text{func}}$**

$b' \leftarrow A^{\text{Enc}}$

Return $b'$

**procedure** $\text{ENC}(x)$

$y_1 \leftarrow \text{FN}(1||x)$; $y_2 \leftarrow \text{FN}(0||x)$

Return $y_1||y_2$

**Figure 3.2:** Constructed adversary $B$ attacking $E$ from a given adversary $A$ attacking $F$.

the corresponding calls to a truly random function $f \leftarrow \text{Func}(n)$. To bound the gap between $G_0$ and $G_1$, we construct an adversary $B$ as in Figure 3.2. Specifically, adversary $B$ runs $A$. Each time the latter queries $x$, the former queries $1||x$ and $0||x$ to its own oracle $\text{FN}$ to get answers $y_1$ and $y_2$ respectively, and then gives $y_1||y_2$ back to $A$. Finally, when $A$ terminates and outputs a bit $b'$, adversary $B$ also outputs the same bit. Note that the adversary $B$ is about as efficient as $A$. Moreover, game $\text{Real}_E^B$ corresponds to game $G_0$, and game $\text{Rand}_E^B$ corresponds to game $G_1$, and thus

$$\Pr[\text{Real}_E^B \Rightarrow \text{true}] - \Pr[\text{Rand}_E^B \Rightarrow \text{true}] = \Pr[\text{Real}_E^B - \Pr[\text{Rand}_E^B] = \text{Adv}_E^{\text{prf}}(B).$$

We now bound the gap between $G_1$ and $G_4$. We claim that the gap between these two games is 0, for all (even computationally unbounded) adversaries $A$. We will now justify this claim. Since we consider computationally unbounded adversaries, without loss of generality, assume that the adversary $A$ does not repeat a prior query. Note that if $A$ makes $q$ distinct queries to $\text{ENC}$, in game $G_1$, it will result in $2q$ distinct queries to $f$. Since $f \leftarrow \text{Func}(n)$, the $2q$ answers will be independent and uniformly random. Thus we can rewrite game $G_1$ as in game $G_2$, in which for each query $\text{ENC}(x)$, instead of calling $y_1 \leftarrow f(1||x)$ and $y_2 \leftarrow f(0||x)$, we sample $y_1$ and $y_2$ at random. As game $G_2$ is equivalent to game $G_1$,

$$\Pr[\text{Real}_E^B \Rightarrow \text{true}] = \Pr[\text{Real}_E^B \Rightarrow \text{true}] .$$

Game $G_3$ is a further simplification of $G_2$. Instead of sampling $y_1, y_2 \leftarrow \{0, 1\}^n$ and returning $y \leftarrow y_1||y_2$, we’ll pick $y \leftarrow \{0, 1\}^{2n}$. Hence

$$\Pr[\text{Real}_E^B \Rightarrow \text{true}] = \Pr[\text{Real}_E^B \Rightarrow \text{true}] .$$

In game $G_4$, we explicitly sample a truly random function $g : \{0, 1\}^{n-1} \rightarrow \{0, 1\}^{2n}$, and for each query $\text{ENC}(x)$, we return $g(x)$. Since $A$ does not repeat prior queries, making $q$ distinct queries to $g(x)$ will result in $q$ independent, uniformly random answers. Hence games $G_3$ and $G_4$ are equivalent, and thus

$$\Pr[\text{Real}_E^B \Rightarrow \text{true}] = \Pr[\text{Real}_E^B \Rightarrow \text{true}] .$$

Hence $\Pr[\text{Real}_E^B \Rightarrow \text{true}] = \Pr[\text{Real}_E^B \Rightarrow \text{true}]$ as claimed. Summing up,

$$\text{Adv}_E^{\text{prf}}(A) = \Pr[\text{Real}_E^B \Rightarrow \text{true}] - \Pr[\text{Rand}_E^B \Rightarrow \text{true}]$$

$$= (\Pr[\text{Real}_E^B \Rightarrow \text{true}] - \Pr[\text{Real}_E^B \Rightarrow \text{true}] + (\Pr[\text{Real}_E^B \Rightarrow \text{true}] - \Pr[\text{Real}_E^B \Rightarrow \text{true}] = \text{Adv}_E^{\text{prf}}(B) .$$

Hence if $E$ is a secure PRF then $F$ is also a secure PRF.