IND-CPA security of CTR mode from a PRF (sketch of the proof)

Notations.

- $E : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ is a block cipher
- Func_n is the set of all functions $f : \{0,1\}^n \to \{0,1\}^n$
- $\mathrm{CTR}[E]$ is the encryption scheme obtained using the CTR mode with the block cipher E
- $\mathrm{CTR}[f]$ is the unrealistic encryption scheme obtained from $\mathrm{CTR}[E]$ by replacing E_k by f, where $f \in \mathrm{Func}_n$

PRF advantage.
The PRF advantage is defined with the same game as the PRP advantage, but the Challenger samples a random function rather than a random permutation. In particular, for a block cipher E, the *PRF advantage function* $\mathsf{Adv}_E^{\mathsf{PRF}}(q,t)$ satisfies that for any (oracle) algorithm $\mathcal{A}_{q,t}$ that makes q queries to its oracle and has running time t,

$$\left|\Pr\left[\mathcal{A}_{q,t}^{\mathcal{O}} \to 1 : \mathcal{O} \twoheadleftarrow \mathrm{Func}_n\right] - \Pr\left[\mathcal{A}_{q,t}^{\mathcal{O}} \to 1 : \mathcal{O} = E_k, k \twoheadleftarrow \mathcal{K}\right]\right| \leq \mathsf{Adv}_E^{\mathsf{PRF}}(q,t).$$

Theorem.
Let E be a block cipher and consider the encryption scheme $\mathrm{CTR}[E]$. Let $\mathcal{A}$ be an adversary for the IND-CPA game that runs in time t, makes q queries of total length Q. Then

$$\mathsf{Adv}_{\mathrm{CTR}[E]}^{\mathsf{IND\text{-}CPA}}(\mathcal{A}) \leq \frac{Q(Q-1)}{2^{n+1}} + 2\mathsf{Adv}_E^{\mathsf{PRF}}(Q,t).$$

Proof. Let $m_{i,0}$, $m_{i,1}$ and $c_i \leftarrow \mathrm{CTR}[E_k](m_{i,b})$, $0 \leq i < q$, be the q queries of the adversary and their answers. For $0 \leq i < q$, let $m_{i,j} = m_{i,j}^1 \| \cdots \| m_{i,j}^{\ell_i}$ and $c_i = IV_i \| c_i^1 \| \cdots \| c_i^{\ell_i}$ for some uniform IV_i and where $c_i^s = m_{i,j}^s \oplus E_k(IV_i + s)$. The total length is $Q = \sum_{i=0}^{q-1} \ell_i$.
To bound the advantage of an adversary $\mathcal{A}$ in the IND-CPA game for $\mathrm{CTR}[E]$, we proceed in two steps. First we show that this advantage is very close to the situation where E is replaced by a random function $f \twoheadleftarrow \mathrm{Func}_n$,

that is where $\mathcal{A}$ plays the game with the (unrealistic) encryption scheme $\text{CTR}[f]$. Then we bound the advantage in this situation.

We want to compare the advantages of an adversary $\mathcal{A}$ in the IND-CPA game for the two encryption schemes $\text{CTR}[E]$ and $\text{CTR}[f]$. There are therefore four situations: either $b = 0$ and $b = 1$ in the IND-CPA game, and the encryption scheme is either $\text{CTR}[E]$ or $\text{CTR}[f]$. If we fix b to either of both values, $\mathcal{A}$ is playing a game with either $\text{CTR}[E]$ or $\text{CTR}[f]$. Then $\left|\Pr\left[\mathcal{A}^{\text{CTR}[E]} \to 1\right] - \Pr\left[\mathcal{A}^{\text{CTR}[f]} \to 1\right]\right| \leq \mathsf{Adv}_E^{\mathsf{PRF}}(Q,t)$. Indeed, an adversary in the PRF game can simulate the IND-CPA game, simply using the oracle (of the PRF game) when it has to apply the block cipher. The difference in behavior for this PRF adversary is bounded, by definition, by the PRF advantage. We now want to bound

$$\left|\left|\Pr\left[\mathcal{A}^{\text{CTR}[E]} \to 1 : b = 1\right] - \Pr\left[\mathcal{A}^{\text{CTR}[E]} \to 1 : b = 0\right]\right| - \left|\Pr\left[\mathcal{A}^{\text{CTR}[f]} \to 1 : b = 1\right] - \Pr\left[\mathcal{A}^{\text{CTR}[f]} \to 1 : b = 1\right]\right|\right|.$$

By reordering the terms, this is at most $2\mathsf{Adv}_E^{\mathsf{PRF}}(Q,t)$.

We now consider the CTR mode replacing E_k by a truly random function f. Assume first that there is no collision of the form $IV_i + s = IV_{i'} + s'$ for any i, i', s, s'. This means that the values $f(IV_i + s)$ are uniformly sampled (since f is a random function). As a result, $\text{CTR}[f]$ is exactly a one-time pad. It means that under that assumption, any adversary has advantage exactly 0 in the IND-CPA game.

We now bound $\Pr\left[\exists i, i', s, s', IV_i + s = IV_{i'} + s'\right]$. The number of values of the form $IV_i + s$ is Q by definition, and we look for a *collision* between two of them. We can apply the birthday bound. Actually, there cannot be any collision $IV_i + s$ with $IV_i + s'$ (with the same i), but this only reduces the probability of collisions. Therefore, $\Pr\left[\exists i, i', s, s', IV_i + s = IV_{i'} + s'\right] \leq Q(Q-1)/2^{n+1}$.

Writing COLL for the event "$\exists i, i', s, s'$ such that $IV_i + s = IV_{i'} + s'$", the law of total probabilities implies

$$\Pr\left[\mathcal{A}^{\text{CTR}[f]} \to 1 \middle| b = 1\right] = \Pr\left[\mathcal{A}^{\text{CTR}[f]} \middle| b = 1 \wedge C\right]\Pr[C] + \Pr\left[\mathcal{A}^{\text{CTR}[f]} \middle| b = 1 \wedge \neg C\right]\Pr[\neg C].$$

Therefore

$$\begin{aligned}
&\left|\Pr\left[\mathcal{A}^{\mathrm{CTR}[f]} \to 1 \middle| b = 1\right] - \Pr\left[\mathcal{A}^{\mathrm{CTR}[f]} \to 1 \middle| b = 0\right]\right| \\
&\quad = \Big|\Pr[C]\left(\Pr\left[\mathcal{A}^{\mathrm{CTR}[f]} \to 1 \middle| b = 1 \wedge C\right] - \Pr\left[\mathcal{A}^{\mathrm{CTR}[f]} \to 1 \middle| b = 0 \wedge C\right]\right) \\
&\qquad - \Pr[\neg C]\left(\Pr\left[\mathcal{A}^{\mathrm{CTR}[f]} \to 1 \middle| b = 1 \wedge \neg C\right] - \Pr\left[\mathcal{A}^{\mathrm{CTR}[f]} \to 1 \middle| b = 0 \wedge \neg C\right]\right)\Big|.
\end{aligned}$$

Now we bound $\Pr[C] \leq Q(Q-1)/2^{n+1}$ and the first parenthesis by 1 in absolute value, and the second parenthesis is 0 as argued before. Altogether

$$\left|\Pr\left[\mathcal{A}^{\mathrm{CTR}[f]} \to 1 \middle| b = 1\right] - \Pr\left[\mathcal{A}^{\mathrm{CTR}[f]} \to 1 \middle| b = 0\right]\right| \leq Q(Q-1)/2^{n+1}.$$

Finally, the advantage of the adversary $\mathcal{A}$ is at most $2\mathsf{Adv}_E^{\mathsf{PRF}}(Q,t) + Q(Q-1)/2^{n+1}$.