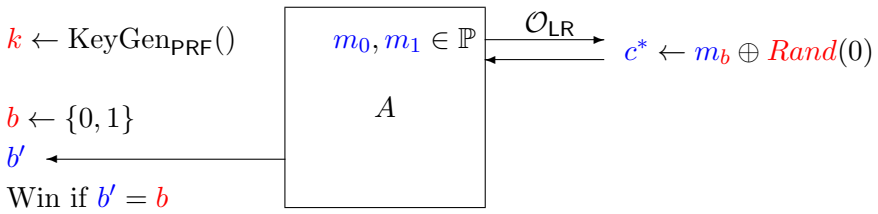

FIGURE 12.2. "Hopped" security game G_1 for the scheme $c \leftarrow m \oplus Rand(0)$

G_0 and G_1 respectively. We have the following relationships between the various probabilities:

$$\left|\Pr[b'_0 = 1 | b_0 = 1] - \Pr[b'_1 = 1 | b_1 = 1]\right| = \text{Adv}^{\mathsf{PRF}}_{\{F_k\}_K}(A), \tag{14}$$

and

$$\left|\Pr[b'_0 = 1 | b_0 = 0] - \Pr[b'_1 = 1 | b_1 = 0]\right| = \text{Adv}^{\mathsf{PRF}}_{\{F_k\}_K}(A), \tag{15}$$

i.e. for fixed b in both games the difference in the winning probabilities between the two games is the same as the advantage in distinguishing a member of a PRF family from a random function. Also note that

$$\Pr[b'_1 = 1 | b_1 = 1] - \Pr[b'_1 = 1 | b_1 = 0] = 0 \tag{16}$$

since if we have a random function then an "encryption" of m_0 is a random string, as is an "encryption" of m_1; this is essentially the security of the one-time pad. Thus the probability of the adversary winning in game G_1 is equal to $1/2$. Putting this together we have

$$\begin{aligned}
\text{Adv}^{\mathsf{IND\text{-}PASS}}_{\Pi}(A) &= \left|\Pr[b'_0 = 1 | b_0 = 1] - \Pr[b'_0 = 1 | b_0 = 0]\right| && \text{by definition} \\
&= \Big|\Pr[b'_0 = 1 | b_0 = 1] \\
&\qquad - \big(\Pr[b'_1 = 1 | b_1 = 1] - \Pr[b'_1 = 1 | b_1 = 1]\big) \\
&\qquad - \Pr[b'_0 = 1 | b_0 = 0]\Big| && \text{adding zero} \\
&\leq \left|\Pr[b'_0 = 1 | b_0 = 1] - \Pr[b'_1 = 1 | b_1 = 1]\right| \\
&\qquad + \left|\Pr[b'_1 = 1 | b_1 = 1] - \Pr[b'_0 = 1 | b_0 = 0]\right| && \text{triangle inequality} \\
&\leq \text{Adv}^{\mathsf{PRF}}_{\{F_k\}_K}(A) + \left|\Pr[b'_1 = 1 | b_1 = 1] - \Pr[b'_0 = 1 | b_0 = 0]\right| && \text{by equation (14)} \\
&= \text{Adv}^{\mathsf{PRF}}_{\{F_k\}_K}(A) + \Big|\Pr[b'_1 = 1 | b_1 = 1] - \Pr[b'_0 = 1 | b_0 = 0] \\
&\qquad - \big(\Pr[b'_1 = 1 | b_1 = 0] - \Pr[b'_1 = 1 | b_1 = 0]\big)\Big| && \text{adding zero again} \\
&\leq \text{Adv}^{\mathsf{PRF}}_{\{F_k\}_K}(A) + \left|\Pr[b'_1 = 1 | b_1 = 1] - \Pr[b'_1 = 1 | b_1 = 0]\right| \\
&\qquad + \left|\Pr[b'_1 = 1 | b_1 = 0] - \Pr[b'_0 = 1 | b_0 = 0]\right| && \text{triangle inequality} \\
&= \text{Adv}^{\mathsf{PRF}}_{\{F_k\}_K}(A) + \left|\Pr[b'_1 = 1 | b_1 = 0] - \Pr[b'_0 = 1 | b_0 = 0]\right| && \text{by equation (16)} \\
&\leq 2 \cdot \text{Adv}^{\mathsf{PRF}}_{\{F_k\}_K}(A) && \text{by equation (15).}
\end{aligned}$$

□