Exercise 6.2.2

If we have a resource inequality $[c \to c]_{\mathrm{priv}} \geq [cc]_{\mathrm{priv}}$, it means that

- The private noiseless classical bit channel can simulate the secret key distribution

Note that the resource inequality would not indicate that the secret key distribution cannot simulate the private noiseless channel. We could consider the following procedure and show that it satisfies two statements above. To check the first statement, suppose that we have a protocol that consists of following steps,

- Step 1: Alice prepares a random classical bit with probability of getting 0 and 1 are both $1/2$, and Eve prepare her own random classical bit with probability of getting 0 and 1 are p_E and $1 - p_E$, respectively. Make sure Eve has no idea about what Alice has prepared so Eve's preparation is independent with Alice's preparation.
- Step 2: Alice performs experiments and send her result to Bob through the private classical noiseless channel. Then Bob would also has a random classical bit with probability of getting 0 and 1 are both $1/2$. If we make sure Eve does not know what Bob has (private), Alice and Bob would get same result, and the probability of getting 00 and 11 are both $1/2$. In this case, the probability of getting (a, b, e) is given by

  $$\begin{cases} p(0,0,0) = 0.5p_E \\ p(0,0,1) = 0.5(1-p_E) \\ p(1,1,0) = 0.5p_E \\ p(1,1,1) = 0.5(1-p_E) \end{cases} \tag{1}$$

  which shows the distribution satisfies $p_{A,B,E}(a,b,e) = \delta_{b,a} p_E(e)/2$.

To check the second statements, we could consider a counter-example:

- Step 1: If Alice prepares a random classical bit with probability of getting 0 and 1 are $1/3$ and $2/3$, respectively, and Eve prepare her own random classical bit with probability of getting 0 and 1 are p_E and $1 - p_E$, respectively. Make sure Eve has no idea about what Alice has prepared so Eve's preparation is independent with Alice's preparation.
- Step 2: Alice performs experiments and send her result to Bob through the private classical noiseless channel. Then Bob also has a random classical bit with probability of getting 0 and 1 are are $1/3$ and $2/3$. If we make sure Eve does not know what Bob has (private), Alice and Bob would get same result, and the probability of getting 00 and 11 are $1/3$ and $2/3$, respectively. In this case, the probability of getting (a, b, e) is given by

  $$\begin{cases} p(0,0,0) = p_E/3 \\ p(0,0,1) = (1-p_E)/3 \\ p(1,1,0) = 2p_E/3 \\ p(1,1,1) = 2(1-p_E)/3 \end{cases} \tag{2}$$

  However, a secret key can only produce what we have in eq. (1), so the secret key cannot simulate the noiseless private bit channel.

Therefore, we can use the protocol shown above to implement a resource with inequality $[c \to c]_{\text{priv}} \geq [cc]_{\text{priv}}$.