Cryptography: Project

(Deadline: 10am, 2022/12/30)

- (50 points) Implement the garbled circuit based protocol for computing $\mathbf{GE}(a, b)$ (lecture 23), where $a = a_1a_0 \in \{0,1\}^2$ and $b = b_1b_0 \in \{0,1\}^2$. The implementation should contain
  - a procedure that takes $\mathbf{GE}(a, b)$ as input and outputs a garbled circuit of $\mathbf{GE}(a, b)$; and
  - a procedure that takes a garbled circuit of $\mathbf{GE}(a, b)$ and a set of input labels as input, evaluates the garbled circuit, and produces an output label.

  For simplicity, you do not need to implement the OT in the protocol. Instead, you may simply ask Alice to send the labels $k_1^{b_1}, k_2^{b_1}$ and $k_5^{b_0}$ to Bob.

  Hint: Given a length-preserving PRF $H : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, the function $G : \{0,1\}^n \to \{0,1\}^{2n}$ defined by $G(k) = H_k(1) \| H_k(2)$ is a length-doubling PRG. You may define a length-doubling PRF $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{2n}$ in the following way:

  $$F_k(x) = G(H_k(x)), \forall k, x \in \{0,1\}^n.$$

  You may choose DES or AES as the PRF H.