How they interact:

Bob learns if he can receive blood from Alice

Alice	Bob

$(F, \underset{=}{e}^{(e_x \| e_y)}, d) \leftarrow Gb(1^k, f, T)$

$\xleftarrow{\quad F \quad}$

$Y \leftarrow En(e_y, y)$

$\xleftarrow{\quad Y \quad}$

$\xrightarrow{x_i}$ $\boxed{OT}$ $\xleftarrow{K_0^i, K_1^i}$ Run 3 times

$\xleftarrow{K^i_{x_i}}$

Note this gives A $X \leftarrow En(e_x, x)$

$X = [K^1_{x_1}, K^2_{x_2}, K^3_{x_3}]$

$Z \leftarrow Ev(F, (X \| Y))$

$\xrightarrow{\quad Z \quad}$

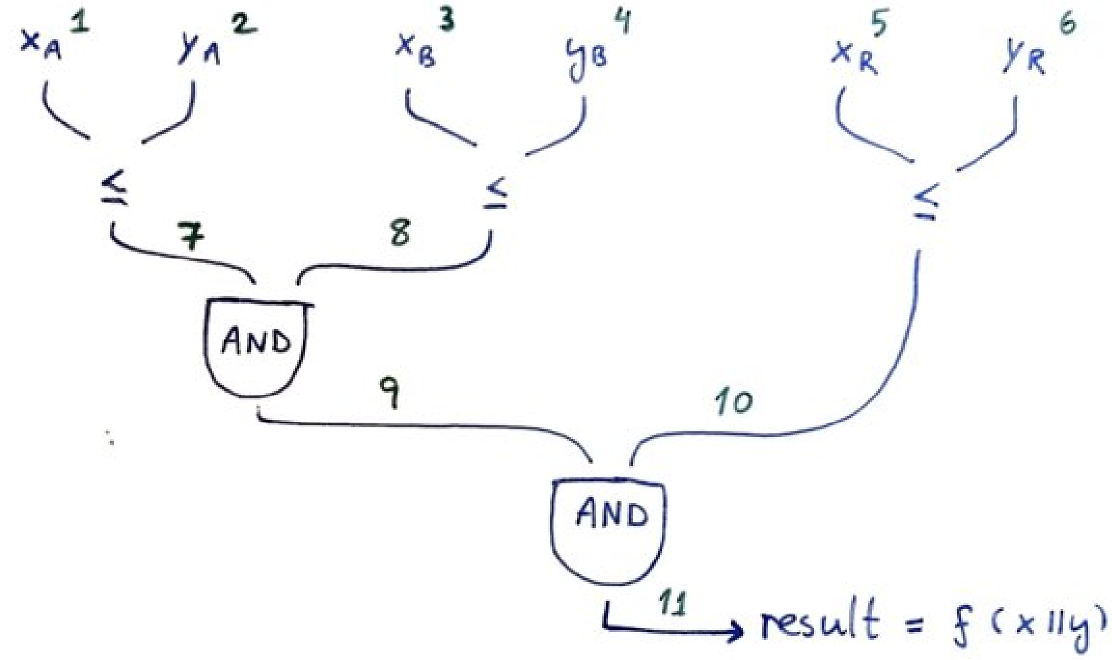
output $z \leftarrow De(d, Z)$

Circuit $f: \{0,1\}^6 \to \{0,1\}$, $T = 11$ wires

input on form $f(x \| y)$, see if y can receive blood from x.

$$f((x_A, x_B, x_R), (y_A, y_B, y_R)) = (((x_A \le y_A) \cdot (x_B \le y_B)) \cdot (x_R \le y_R))$$

Visualized as follows:



Numbering of wires:

w_i for $i \in [1, \_, 6]$ input wires

w_i for $i \in [7, 8, 9, 10]$ internal wires

w_T for $T = 11$ output wire.

Notation: $w_i = \text{Eval}(w_{L(i)}, w_{R(i)})$, where $L, R : [7, 11] \to [1, \_, 11]$:

$w_7 = w_1 \le w_2$, $w_8 = w_3 \le w_4$, $w_{10} = w_5 \le w_6$, Should make dictionary for L and R, need to look up later.

$w_9 = w_7 \wedge w_8$, $w_{11} = w_9 \wedge w_{10}$

Eval is either "$\le$" or "$\wedge$". Note $L(i) \le R(i) < i$.

$$L: \begin{array}{l} 7 \to 1 \\ 8 \to 3 \\ 9 \to 7 \\ 10 \to 5 \\ 11 \to 9 \end{array} \qquad R: \begin{array}{l} 7 \to 2 \\ 8 \to 4 \\ 9 \to 8 \\ 10 \to 6 \\ 11 \to 10 \end{array}$$

We need to have a PRF

$$G : \{0,1\}^k \times \{0,1\}^k \times [1, \dots, 11] \to \{0,1\}^{2\cdot 128},$$

use SHA-256.

"set length of wire labels to 128 bits $\to k = 128$?"

Circuit generation : Want output (F, e, d)

Gb$(f, 11)$:

```
For i in range(1, 12):                 // i = 1, ..., 11
                 (11+1)
    choose (K_0^i, K_1^i) <-$ {0,1}^k x {0,1}^k
    All_key_values.append(K_0^i, K_1^i)   // store all keys somewhere
    if i < 7:                  // if i ∈ {1,2,3,4,5,6}
        e.append((K_0^i, K_1^i))   // store keys for input wires in some way
                                   ok to access
    if i = 11:
        d := (Z_0, Z_1) = (K_0^11, K_1^11)
```

Note $e = (e_x \| e_y)$, where $e_x = \{K_0^i, K_1^i\}_{i \in \{1,2,3\}}$ is controlled by Alice, and $e_y = \{K_0^i, K_1^i\}_{i \in \{4,5,6\}}$ is controlled by Bob.

→

For i in range$(7, \overset{=11+1}{12})$: // define $C_0^i, \dots, C_3^i$ for F

$$C_{00}^{i} = G(K_0^{L(i)}, K_0^{R(i)}, i) \oplus (K^i_{Eval(0,0)}, 0^k)$$
$$C_{01}' = G(K_0^{L(i)}, K_1^{R(i)}, i) \oplus (K^i_{Eval(0,1)}, 0^k)$$
$$C_{10}' = G(K_1^{L(i)}, K_0^{R(i)}, i) \oplus (K^i_{Eval(1,0)}, 0^k)$$
$$C_{11}' = G(K_1^{L(i)}, K_1^{R(i)}, i) \oplus (K^i_{Eval(1,1)}, 0^k)$$

when naming C's, give some kind of double index.

choose random permutation $\pi: \{0,1,2,3\} \to \{0,1\} \times \{0,1\}$

$$(C_0^i, C_1^i, C_2^i, C_3^i) = (C'_{\pi(0)}, C'_{\pi(1)}, C'_{\pi(2)}, C'_{\pi(3)})$$

F. append$((C_0^i, C_1^i, C_2^i, C_3^i))$

Encoding:

$En(e, \overset{\in\{0,1\}^3}{x})$:

Parse $e = [[K_0^1, K_1^1], \dots, [K_0^6, K_1^6]]$

For Alice:

Return $X = [K^1_{x_1}, K^2_{x_2}, K^3_{x_3}]$

For Bob:

Return $Y = [K^4_{x_1}, K^5_{x_2}, K^6_{x_3}]$

Evaluate:

$Ev(F, X)$:

Parse $X = [K^1, K^2, K^3]$

For i in range$(7, \overset{11+1}{12})$:

Access $(C_0^i, C_1^i, C_2^i, C_3^i)$

For j in range(4):

$$(K'_j, \tau_j) = G(K^{L(i)}, K^{R(i)}, i) \oplus C_j^i$$

Must save all values, check for correct result outside of loop since uniqueness of result

If unique j st $\tau_j = 0^k$:

$K^i = K'_j$

Else: Abort, return $\perp$

Output $Z' = K^{11}$

Decoding:

De(d, Z):

Parse $d = (Z_0, Z_1)$

If $Z = Z_0$:

Return 0

If $Z = Z_1$:

Return 1

else:

Return $\perp$