

```

principal A
principal B

def cmp :  $\mathbb{Z}\{\text{isec}:A,B\} \rightarrow \mathbb{B}\{\text{yao}:A,B\}$ 
def cmp =  $\lambda$  xy  $\rightarrow$ 
  let x :  $\mathbb{Z}\{\text{yao}:A,B\}$ 
  let x = share{yao:A,B} xy.A
  let y :  $\mathbb{Z}\{\text{yao}:A,B\}$ 
  let y = share{yao:A,B} xy.B
  let r :  $\mathbb{B}\{\text{yao}:A,B\}$ 
  let r =  $x \leq y$ 
  in r

def cmp-rev :  $\mathbb{1} \rightarrow \{\text{inp}:A,B;\text{rev}:A,B\} \mathbb{B}\{\text{ssec}:A,B\}$ 
def cmp-rev =  $\lambda$  •  $\rightarrow$ 
  let r :  $\mathbb{B}\{\text{yao}:A,B\}$ 
  let r = cmp-mpc •
  let p :  $\mathbb{B}\{\text{ssec}:A,B\}$ 
  let p = reveal{A,B} r
  in p

def one-liner :  $\mathbb{1} \rightarrow \{\text{inp}:A,B;\text{rev}:A,B\} \mathbb{B}\{\text{ssec}:A,B\}$ 
def one-liner =  $\lambda$  •  $\rightarrow$ 
  let xy = {par:A,B} read  $\mathbb{Z}$  "el-input.txt"
  in reveal{A,B} (share{yao:A,B} xy.A)  $\leq$  (share{yao:A,B} xy.B)

def main :  $\mathbb{B}\{\text{ssec}:A,B\} \times \mathbb{B}\{\text{ssec}:A,B\}$ 
def main = cmp-mpc-rev • , one-liner •

```