

```

-- input parties
principal A
principal B
-- compute parties
principal C
principal D
-- output parties
principal E
principal F

def cmp : Z{isec:A,B} → {inp:A,B} B{yao:C,D}
def cmp = λ xy →
  let x : Z{yao:C,D}
  let x = share{yao:C,D} xy.A
  let y : Z{yao:A,B}
  let y = share{yao:C,D} xy.B
  let r : B{yao:C,D}
  let r = x ≤ y
  in r

def cmp-mpc : 1 → {inp:A,B;rev:E,F} B{ssec:E,F}
def cmp-mpc = λ • →
  let xy : Z{isec:A,B}
  let xy = {par:A,B} read Z "el-input.txt"
  let r : B{yao:C,D}
  let r = cmp xy
  let o : B{ssec:E,F}
  let o = reveal{E,F} r
  in o

def one-liner : 1 → {inp:A,B;rev:E,F} B{ssec:E,F}
def one-liner = λ • →
  let xy = {par:A,B} read Z "el-input.txt"
  in reveal{E,F} (share{yao:C,D} xy.A) ≤ (share{yao:C,D} xy.B)

def main : B{ssec:A,B} × B{ssec:A,B}
def main = cmp-mpc • , one-liner •

```