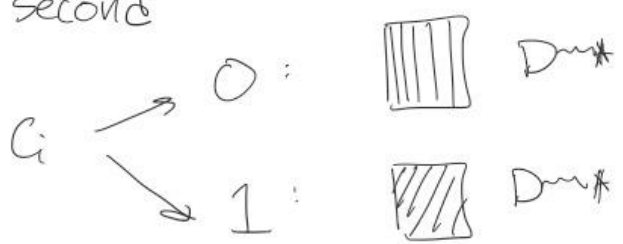
Idea : BB84

a	b	Polarization
0	0	↕
0	1	↔
1	0	↗↙
1	1	↖↘

1. Alice chooses $a, b \in \{0,1\}^n$ each random
   At i^{th} second, sends photon : $a_i \rightarrow$ basis
   $b_i \rightarrow$ bit

2. Bob chooses $c \in \{0,1\}^n$ randomly
   At i^{th} second



3. Bob records outcome in string d

   Detection $*$: $d_i = 0$

   No detection : $d_i = 1$

4. Alice + Bob publicly announce a, c
   (keep b, d private)

5. Alice and Bob throw out the bits of b, d where a $\neq c$