

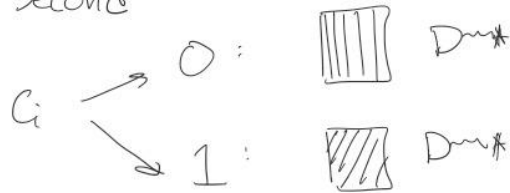
Bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
a	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0
b	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	1	1
c	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	1	0	1
e	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	2	2	2	2
f	0	0/1		0/1		0/1	1	0/1	0/1	0		0		1	0/1		2	2		
d	0	0/1		0/1		0/1	0/1	0/1	0/1	0/1		0		0/1	0/1		0	0/1		

Idea : BB84

a	b	Polarization
0	0	$\updownarrow$
0	1	$\longleftrightarrow$
1	0	$\nearrow$
1	1	$\nwarrow$

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



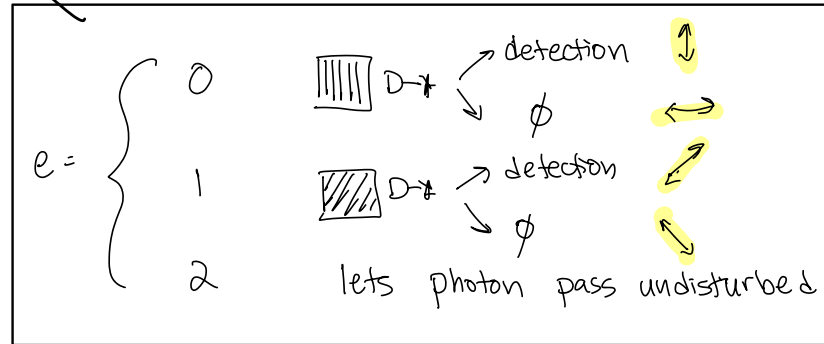
3. Bob records outcome in string d

Detection * : $d_i = 0$

No detection : $d_i = 1$

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

Eve



$f_i = \begin{cases} 0 & \text{detection} \\ 1 & \text{no detection} \\ 2 & \text{no meas} \end{cases}$