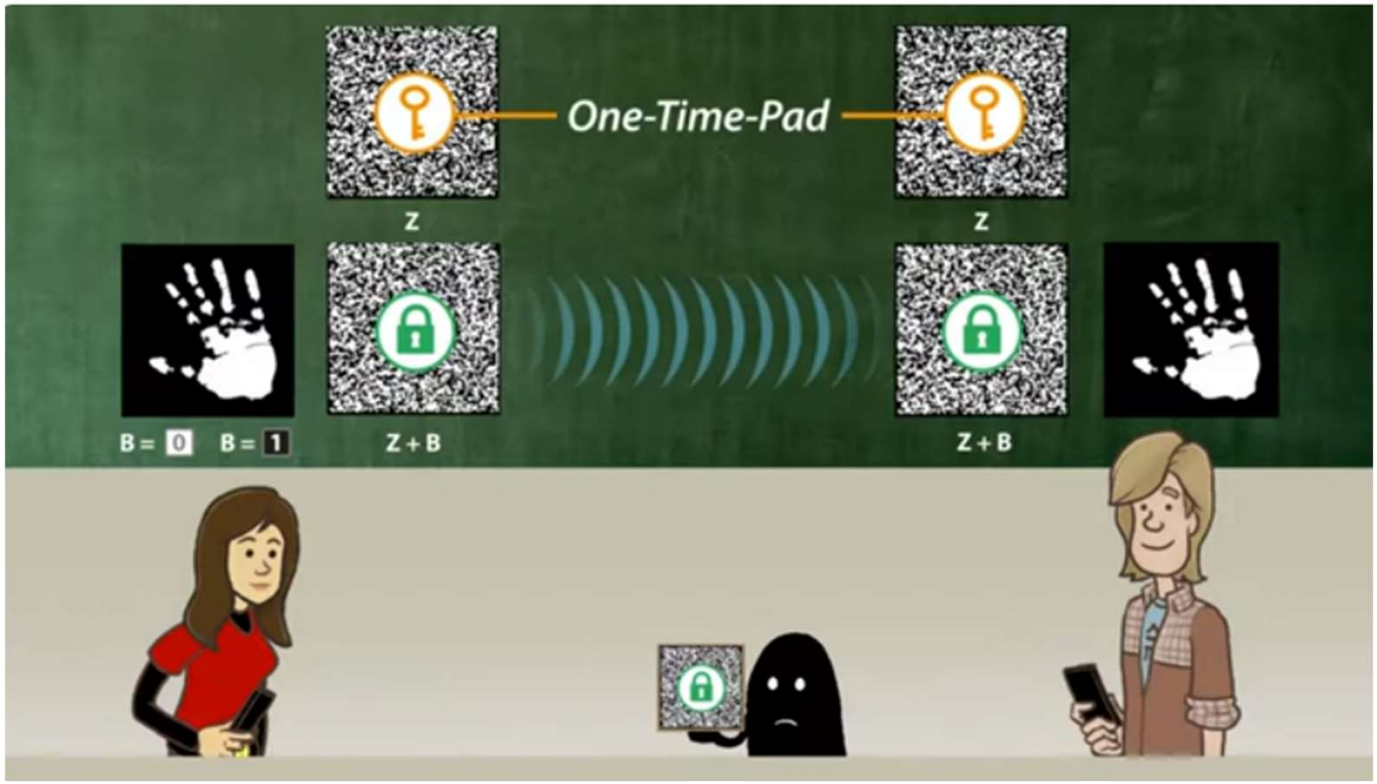
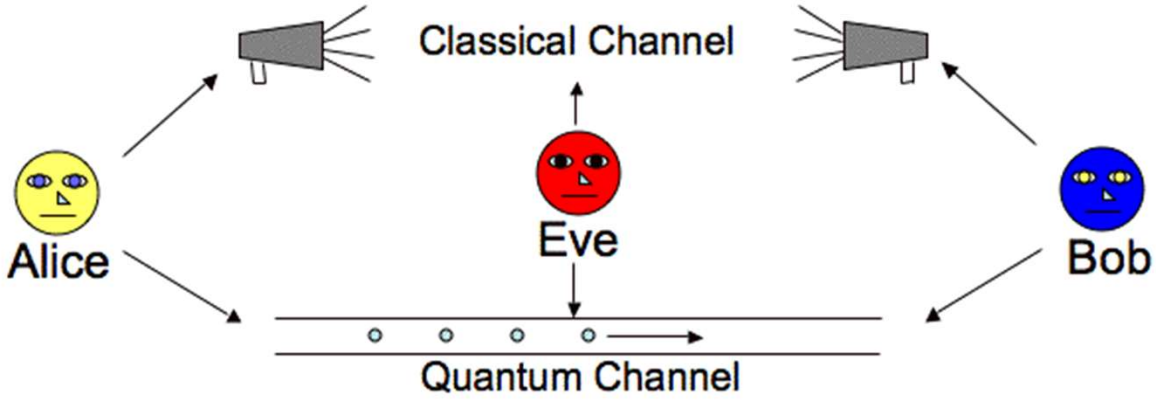
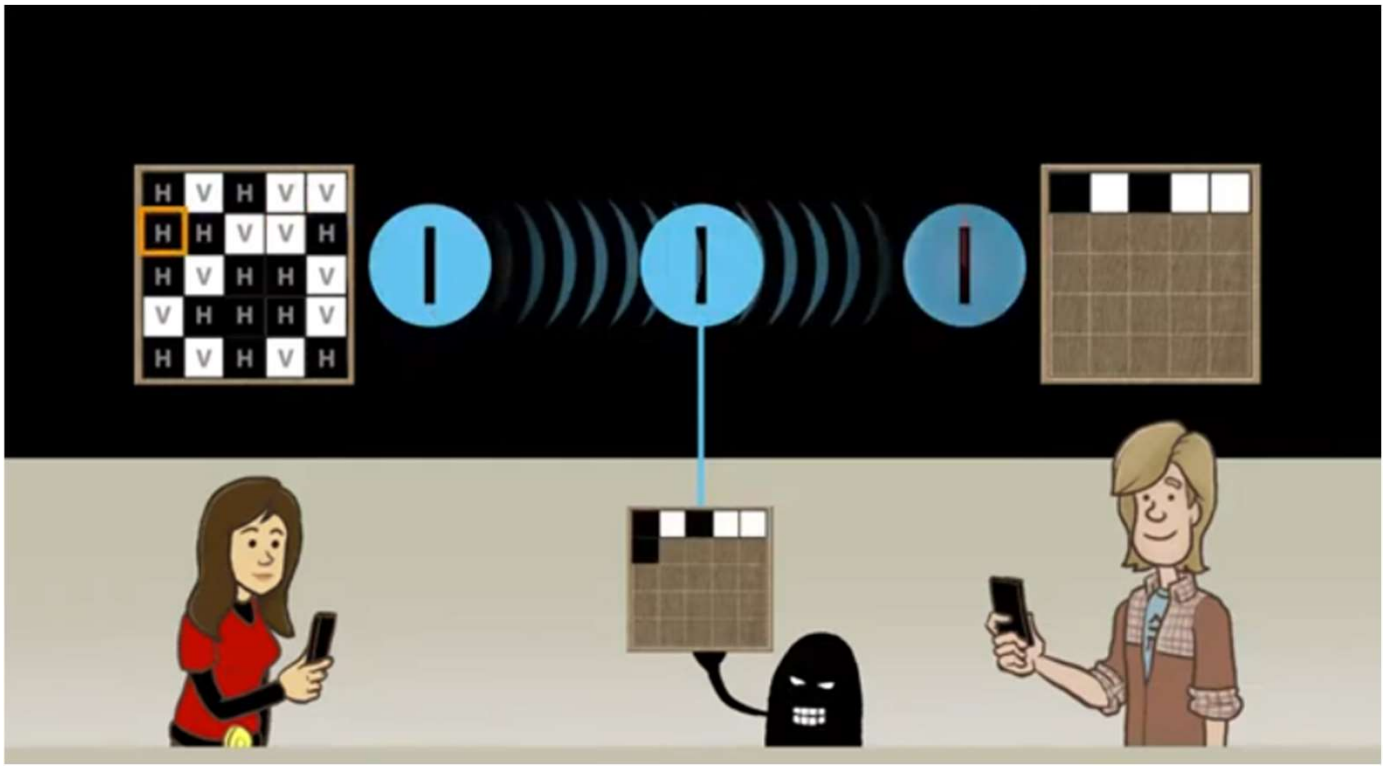
Quantum Key Distribution and BB84 Protocol


One-Time-Pad
Z
Z
B = 0
B = 1
Z + B
Z + B

Quantum Cryptography

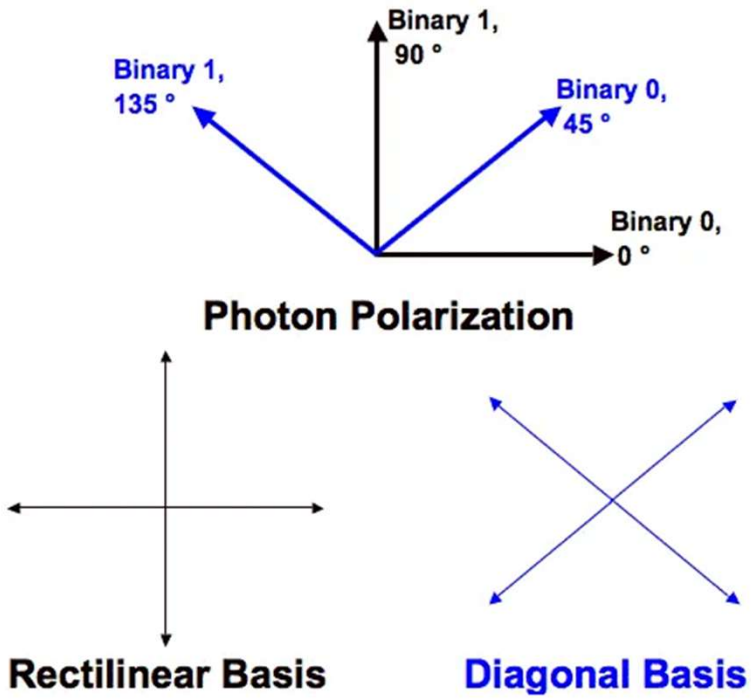
In contrast to classical cryptography, quantum key distribution and other protocols use quantum mechanics principles to provide an unconditionally secured public-key cryptosystem. These protocols can even detect the presence of an eavesdropper in the system who is attempting to learn the key.



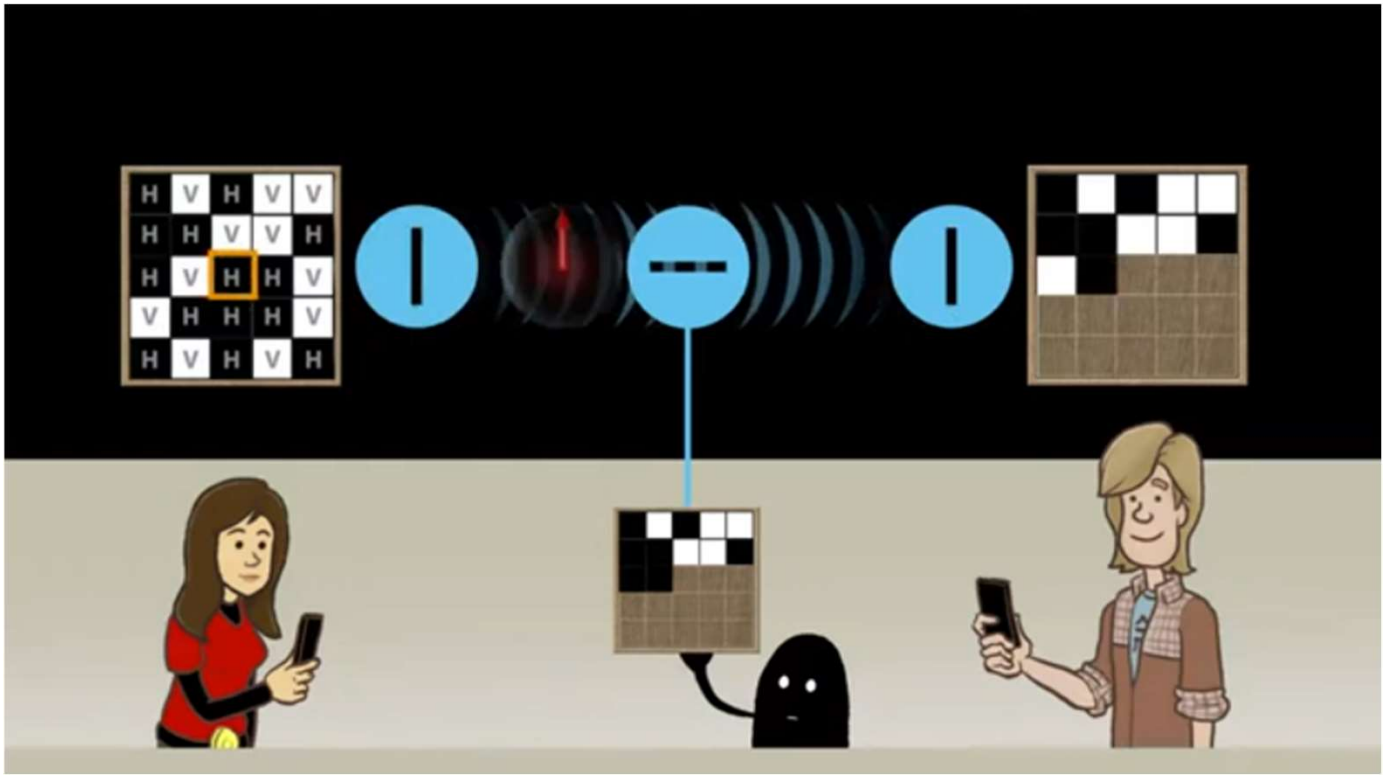

H V H V V
H H V V H
H V H H V
V H H H V
H V H V H

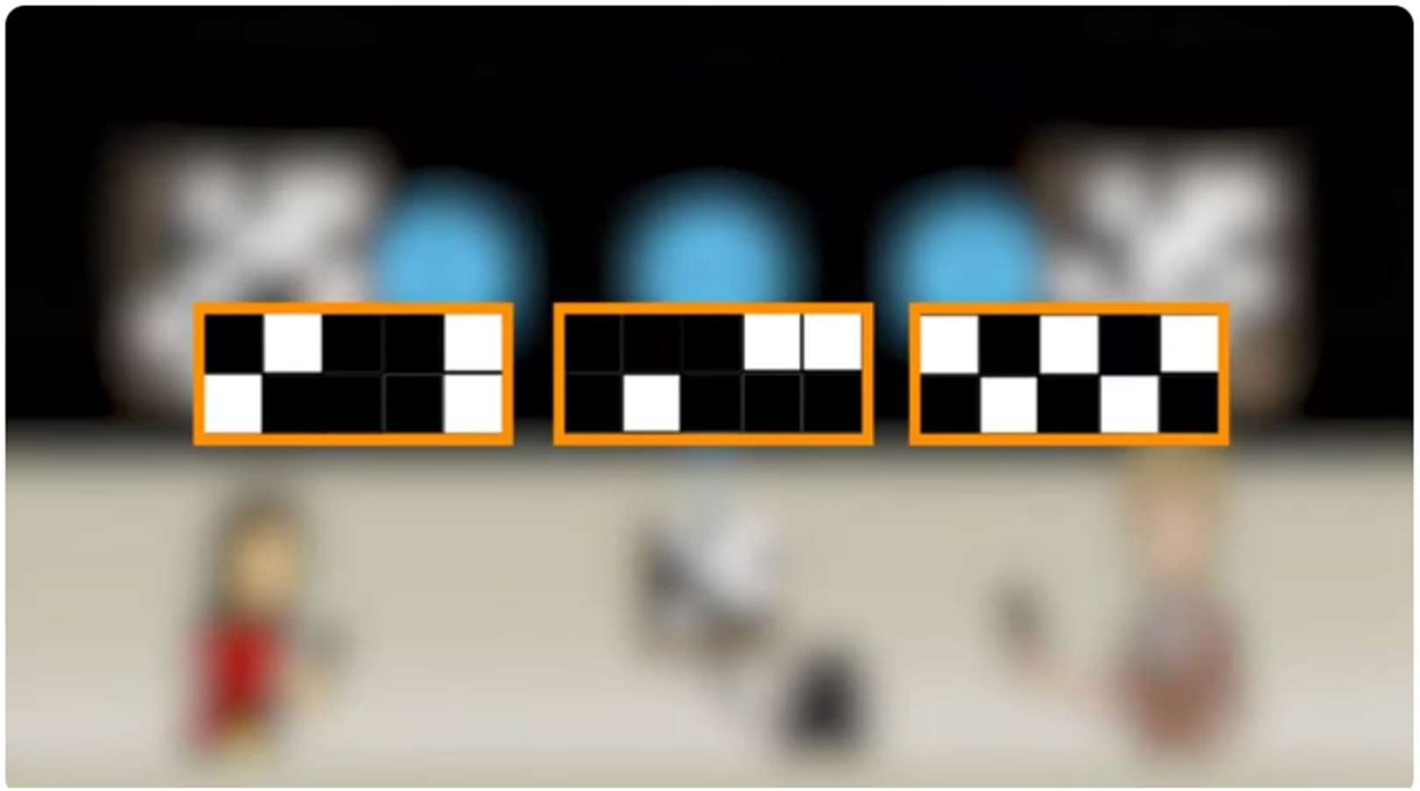
The BB84 Protocol

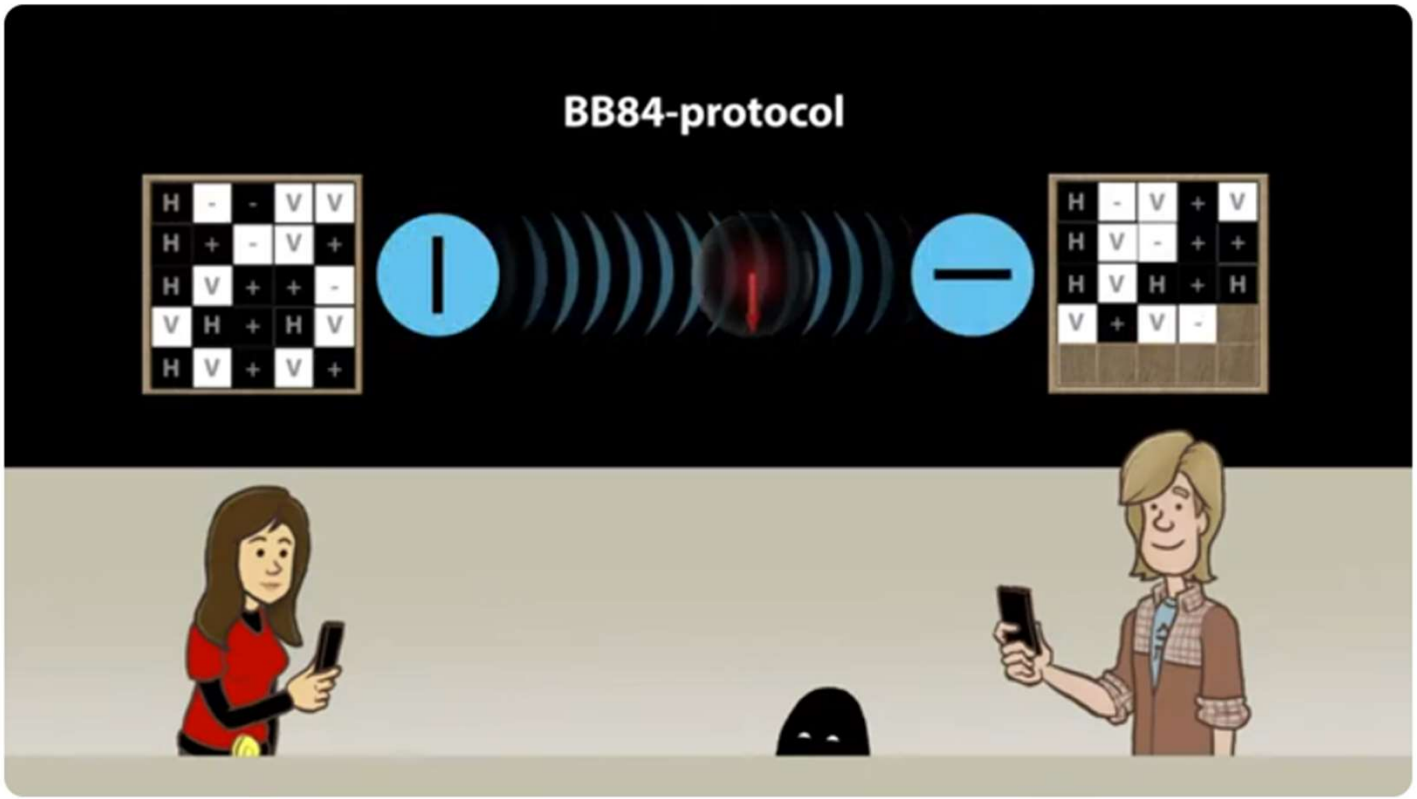
In 1984, Charles Bennett and Gilles Brassard published a protocol based on Heisenberg's uncertainty principle. The protocol is named BB84 after the authors' names and the year it was published. It is one of the most prominent quantum protocols. All the other protocols based on HUP are considered variants of BB84.



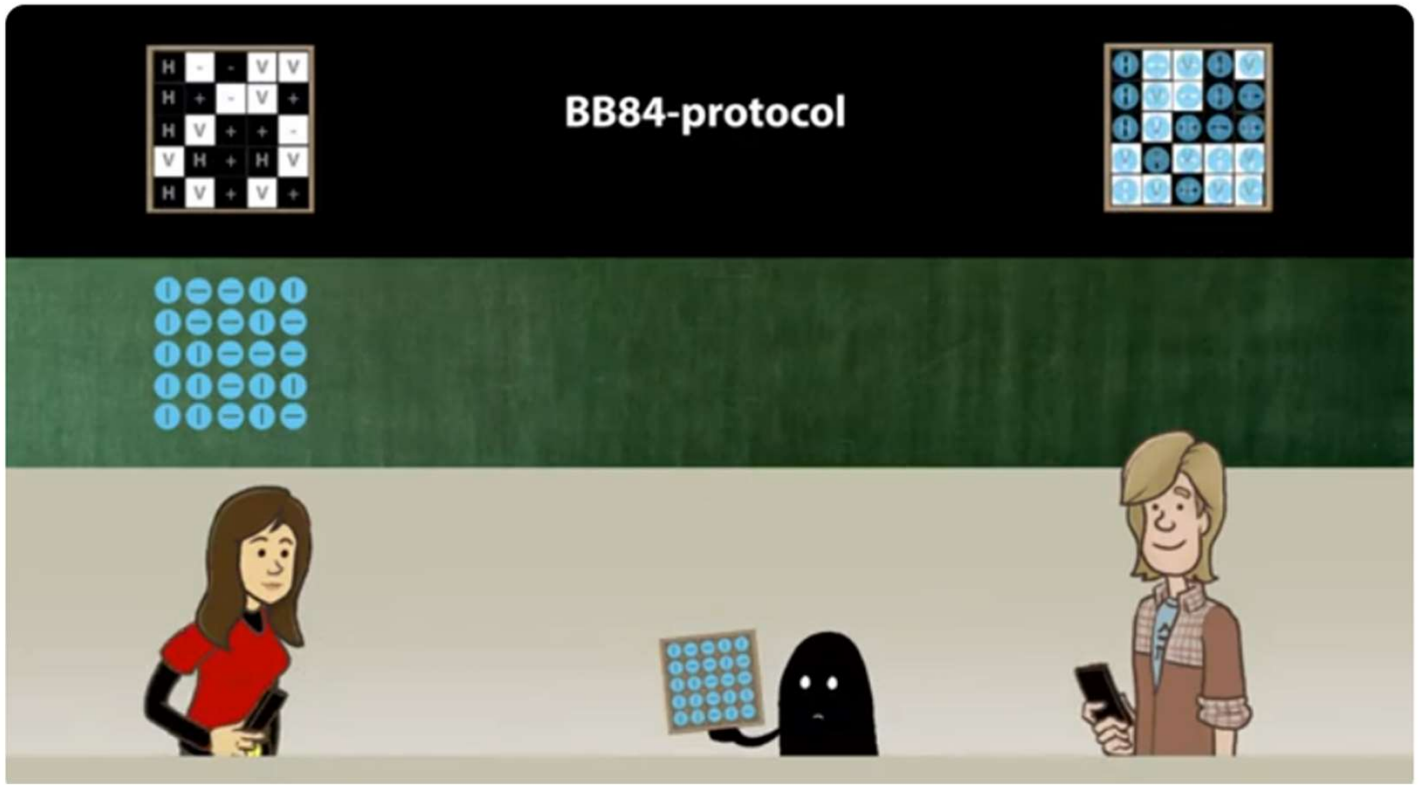
Bits are encoded in the polarization state of a photon. Image by Mart Haitjema.


H V H V V
H H V V H
H V H H V
V H H H V
H V H V H




BB84-protocol
H - - V V
H + - V +
H V + + -
V H + H V
H V + V +
H - V + V
H V - + +
H V H + H
V + V -

Alice's bit-string	1	0	0	1	1	0	1	0	0	1
Alice's encoding basis	+	×	×	+	×	+	+	+	+	+
Alice's polarization	V	D	D	V	A	H	H	H	H	H
Bob's measurement basis	+	+	×	+	+	×	+	+	+	×
Bob's polarization	V	V	D	V	H	A	H	H	H	D
Shifted Key	1	1	1	1	0	1	0	0	0	0


BB84-protocol