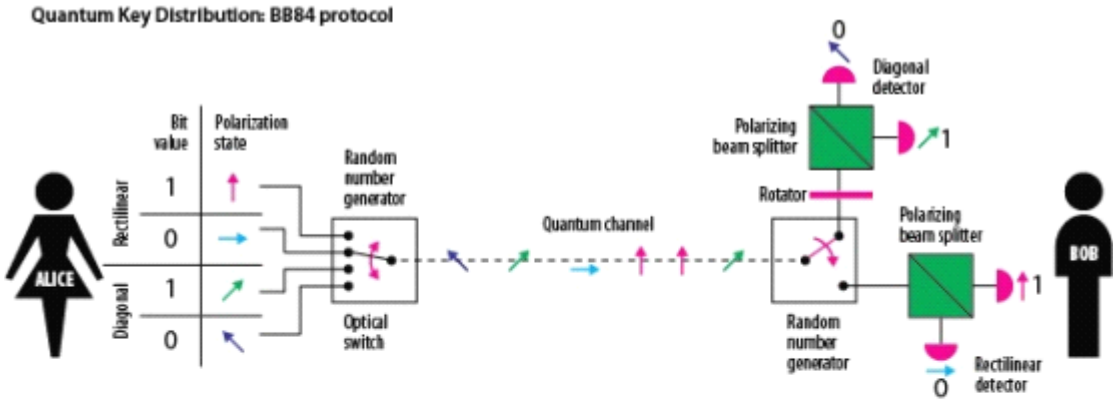
A crack method, on the BB84 protocol

LIWeiGang

(Binjiang school,Ankang725011,China)

On the BB84 protocol, the diagram accurately reflects the essence of the BB84 protocol



Quantum transmission & detection	ALICE sends photons	↖	↗	→	↑	↑	↗	↖	↑
	ALICE's random bits	0	1	0	1	1	1	0	1
	BOB's detection events	↑	↗	↖	↑	↗	↗	↖	↖
	BOB's detected bit values	1	1	0	1	1	1	0	0
Public discussion (i.e., sifting)	BOB tells ALICE the basis choices he made	Rect	Diag	Diag	Rect	Diag	Diag	Diag	Diag
	ALICE tells BOB which bits to keep		✔		✔		✔	✔	
	ALICE and BOB's shared sifted key	–	1	–	1	–	1	0	–

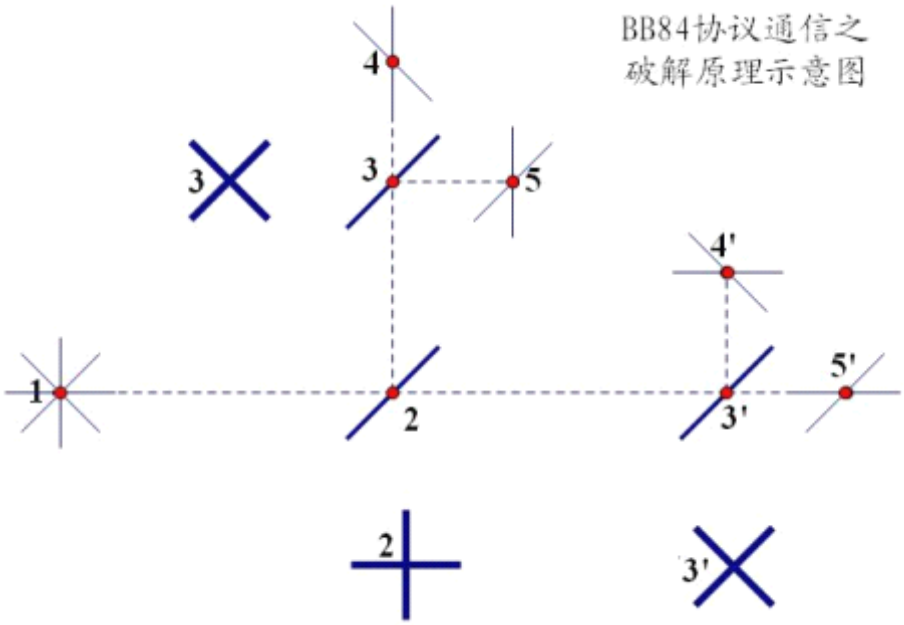
In the figure, the green square of Bob represents the PBS, which is the "polarizing beam splitter" mentioned above. Its basic function is to divide two linearly polarized photons whose polarization states are orthogonal to each other - to two different (Dd) as represented by the purple semilunar icon in the picture; if Bob uses the wrong analyzer (the light path switch identified as RNG in the figure to toggle in the wrong state), as shown in the figure, the photodetector (Dd) In the

fourth row of the Schedule, the detector responds with a probability of 50% to 0; with a 50% chance to respond to 1; the root cause is the 45 ° oblique polarization of the detector with two orthogonal optical axes Photons, the probability of being distributed to the two optical paths 50% each.

The simplest "polarizing beam splitter" (PBS) is a glass plate that is parallel to both sides. When the incident photon is projected to the glass at the "Brewster angle", the polarization direction and the incident plane of the photon When the incident photon is projected onto the glass at the "Brewster angle", and the polarization direction and the incident plane of the photon line are in the direction of the plane of the incident light, (In the plane defined by the incident ray and the normal of the slide), the photon enters the reflected light path at a high probability and enters the fluoroscopic path at a very low probability (in order that the two polarizations which are polarized perpendicularly to each other Polarized photons are distributed to different optical paths, using the "slide stack" that allows the photon to pass through multiple slides several times in succession);When the direction of the polarization of the incident photon is oblique to the incident surface, the incident photon will only enter

the transmitted light path, or only enter the reflected light path, which will make the BB84 protocol easier to crack (in this case, no special discussion) ; The relative trouble is that when the polarization direction of the incident photon and the incident surface is oblique state, the incident photon random access to the middle of the two optical path of a (the following description of the program to crack the relatively troublesome situation as the main premise Expand)!

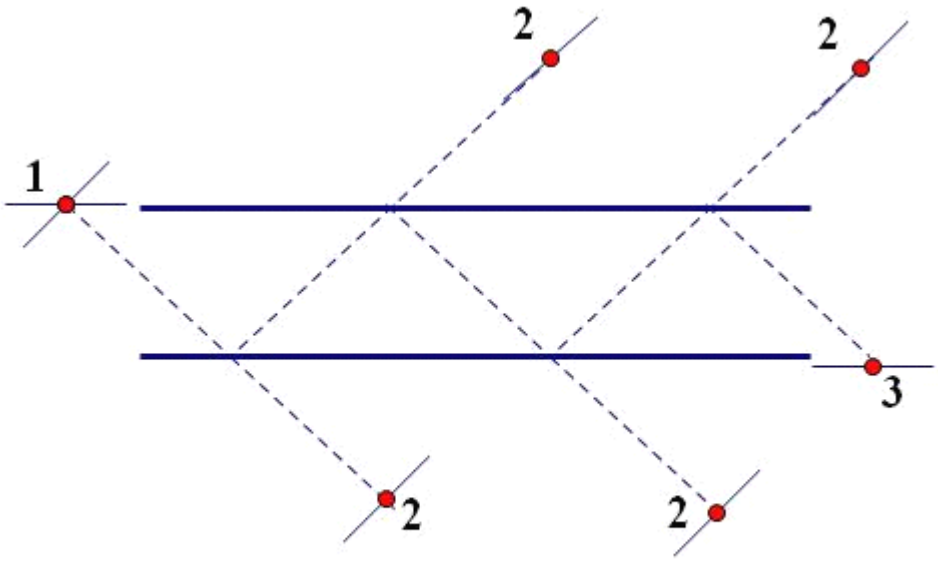
The following is a combination of the following BB84 protocol communication schematic diagram of the crack, brief description of the protocol for the crack method:



As shown in the figure, 1 is a single-photon with polarization state encoded by the listener and has 4 possible states of polarization. After passing through the first-order

cross-polarized beam splitter placed in 2 places, 3 ’position of the X-polarized beam splitter, corresponding to four possible optical path, may reach 4,5,4’, 5 ’of a total of four locations; as shown, arrived at the above four positions of the photon, There are only two possible polarization states, and the angle between the two linear polarization directions is 45 degrees.

For each of the four optical paths described above, a ″45 degree linearly polarized beam splitter″ is further connected (as shown in the figure below)



分离偏振态相差45度光子光路示意图

As shown, thick lines indicate two slides placed parallel to one another, one representing a single photon with only two possible linear polarization states, and two oblique intersections between the two possible linear polarization

states of 45 degrees; dashed lines represent Although the oblique polarized photons have a certain probability of being reflected at a certain time, they are emitted as a reflected light after reaching a plurality of reflections, and arrive at In the figure, the single photon at the 3 position has a great chance of being a linearly polarized photon which is parallel to the plane of the slide.Regardless of where the photons are transmitted in the illustrated path, they must be linearly polarized photons at 45 degrees. Thus, we can identify the linear polarization state of the intercepted photon with a very high correct rate, which of the four possible states of polarization; furthermore, according to the detection results, we can send Bob a single photon of the same polarization state ; To achieve based on the BB84 protocol "quantum secret communication" is not aware of the monitor, decipher.

Note:

1. In this paper, based on the above, and further improve the accuracy of recognition from 85% to a hope to achieve any correct rate; This is in the discussion with friends davidli91 formed friends davidli91 contributed a very important judgments.

2. On the BB84 protocol various popular science introduction article, will be encoded photon polarization state is simplified as four different linear polarization state ; Precisely, the four polarization states, two are orthogonal to each other linear polarization state; the other two polarization states, one is the left-handed state, one is the right-handed state. A person familiar with this technical detail may therefore be skeptical of this scheme, which is not necessary. Because, at the beginning, a very thin λ / 4 plate (whose optical axis is aligned with the polarization direction of the two linearly polarized photons) can be inserted and the left-handed and right-handed single photons are transformed into 45 °, 135 ° linear polarization Photons without affecting the original linear polarization state of the linearly polarized photon; hence, the scheme of the present invention is illustrated in the context of one of the four possible linearly polarized states of the captured photon.