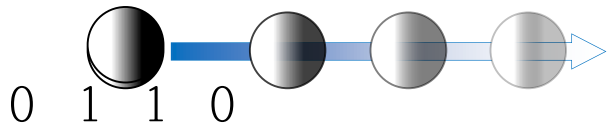
Summary of previous lecture

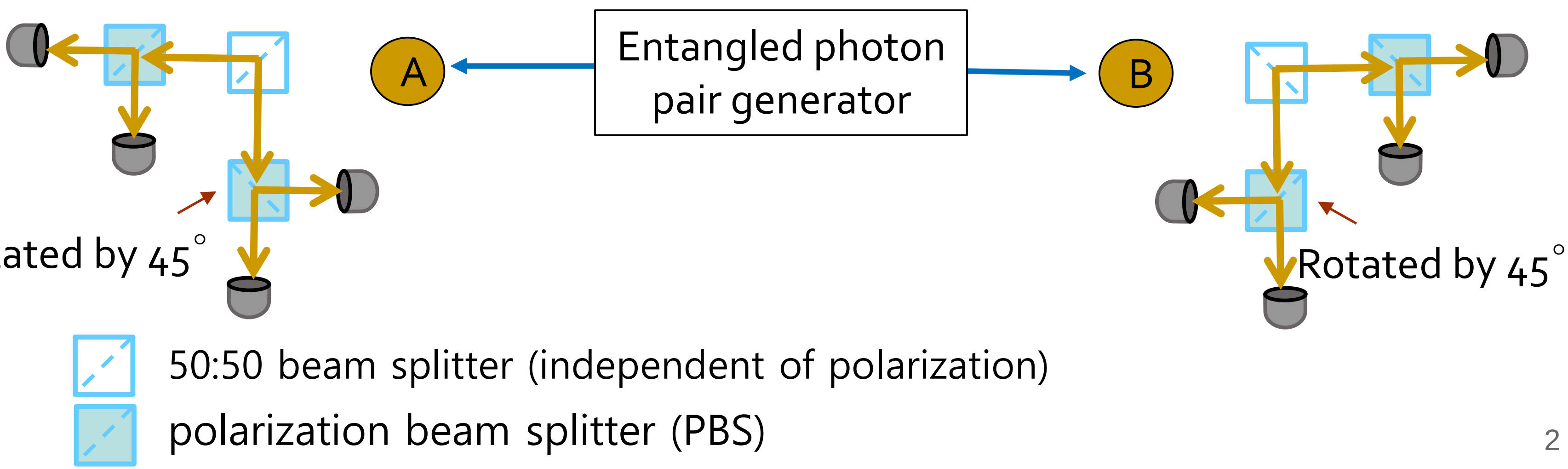
- Quantum cryptography
  - Called Quantum Key Distribution or simply QKD
  - Symmetric key system (compared with public key system)
  - BB84 (symmetric cryptography) ➔ depends on the no-cloning property and ambiguity coming from non-commuting measurement operators
  - One of the candidates for the post-quantum cryptography

QKD based on entanglement I

- Why are we interested in QKD based on entanglement?
  - Attenuation of a single photon in an optical fiber



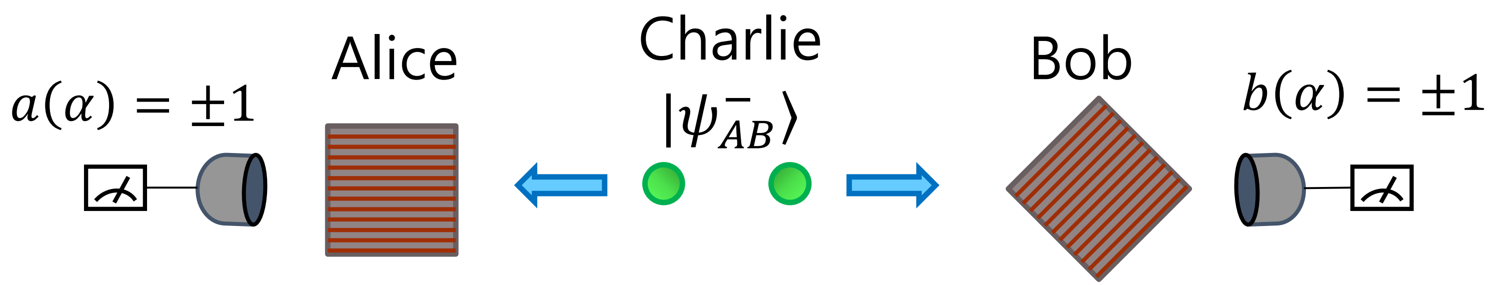
  - Entangled state can be extended to a long distance using entanglement swapping
- One way to implement BB84
  - $|\psi^{-}\rangle = [|H\rangle_A |V\rangle_B - |V\rangle_A |H\rangle_B]/\sqrt{2}$
  - Measure one of the photon A, then Alice can know exactly the state of photon B ➔ equivalent to BB84



EPR and the Bell Inequality

- Section 2.6
- Test of local hidden variable theory
  - Assume that local hidden variable theory is correct, and design an experiment that will produce a result which cannot be explained by such a theory
- Consider polarization-entangled photon pair:

$$|\psi^-\rangle = (|H_A\rangle|V_B\rangle - |V_A\rangle|H_B\rangle)/\sqrt{2}$$

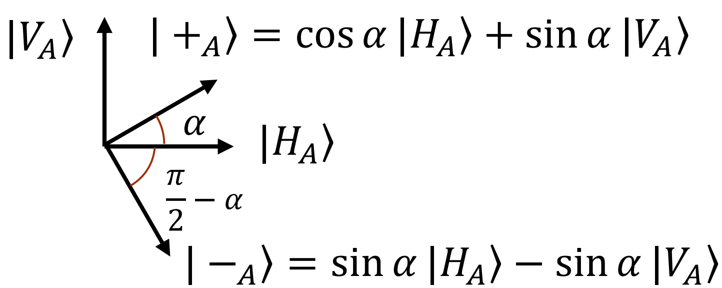


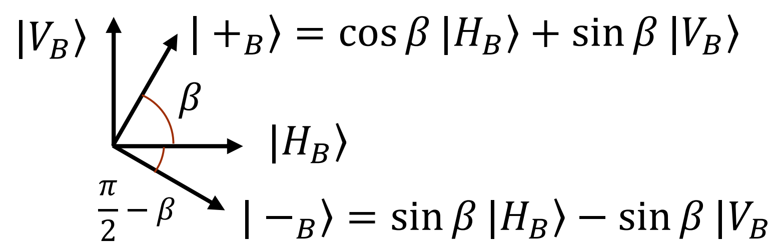
Detect at angle α Detect at angle β

- +1 if photon is detected. -1 if no photon is detected.

CHSH measurement

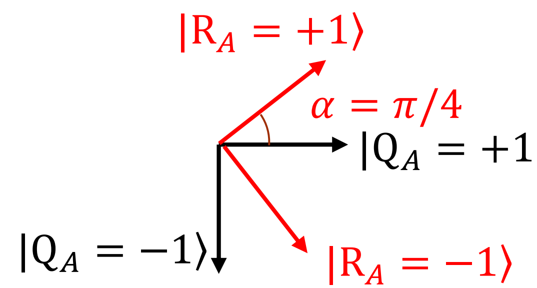
- Clauser-Horne-Shimony-Holt inequality
  - One type of Bell's inequality ➔ starts with an assumption that quantum mechanics is wrong
  - Test of local hidden variable theory
- Define 4 types of measurements
  - Q represents Alice's measurement result when $\alpha = 0$ and R for $\alpha = \pi/4$.
  - Similarly for Bob, S: $\beta = \pi/8$, T: $\beta = 3\pi/8$.
- Alice chooses measurement basis randomly between Q and R while Bob chooses between S and T.
- We want to measure the average value $E(\alpha, \beta) = \langle a(\alpha) b(\beta) \rangle$.
  - For example, when Alice obtains $R = +1$ and Bob obtains $S = -1$, we calculate the product $R \cdot S = -1$. Calculate the average of such kind of measurement $E(R \cdot S)$

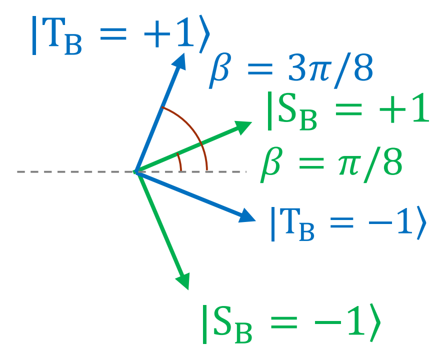




Assume hidden variables exist

No.	Hidden variables				Alice		Bob		Product of meas.			
	q	r	s	t	Q	R	S	T	QS	QT	RS	RT
1	+1	-1	-1	+1	+1		-1		-1			
2	-1	-1	+1	-1		-1	+1				-1	
3	-1	+1	-1	+1	-1			+1		-1		
4	+1	-1	+1	+1	+1		+1		+1			
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
37	+1	-1	-1	+1		-1		+1				-1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
45	+1	-1	-1	+1		-1	-1				+1	
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
82	+1	-1	-1	+1	+1			+1		+1		
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
$4N$	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮





- $E(QS) = (-1 + 1 + \cdots)/N = \sum_{q,r,s,t} p(q,r,s,t)QS$

$q,r,s,t = -1,+1,-1,+1$ $\quad q,r,s,t = +1,-1,-1,+1$ $\quad q,r,s,t = +1,-1,+1,+1$

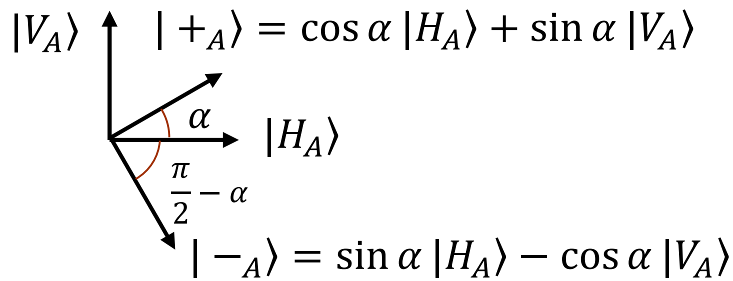
- $E(QT) = (-1 + \cdots + 1 + \cdots)/N = \sum_{q,r,s,t} p(q,r,s,t)QT$
- $S = E(QS) + E(RS) + E(RT) - E(QT)$

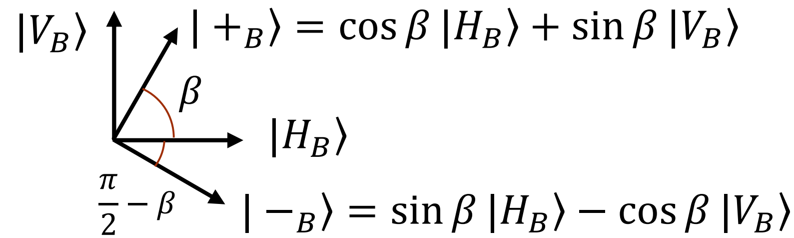
$= \sum_{q,r,s,t} p(q,r,s,t)QS + \sum_{q,r,s,t} p(q,r,s,t)RS + \sum_{q,r,s,t} p(q,r,s,t)RT - \sum_{q,r,s,t} p(q,r,s,t)QT$

$= \sum_{q,r,s,t} p(q,r,s,t)(QS + RS + RT - QT) = \sum_{q,r,s,t} p(q,r,s,t)\big((Q+R)S + (R-Q)T\big)$

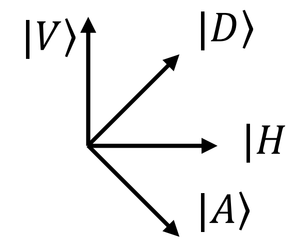
- Because Q, $R = \pm 1$, either $(Q+R)S = 0$ or $(R-Q)T = 0$ ➔ $QS + RS + RT - QT = \pm 2$
- $|S| \leq 2$ for local hidden variable case

Prediction by quantum theory I





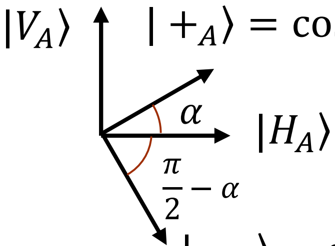
- Recall how we predicted the measurement result in different basis
  - By using basis transform relation,



$$\begin{cases}|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}\\ |A\rangle = (|H\rangle - |V\rangle)/\sqrt{2}\end{cases} \Leftrightarrow \begin{cases}|H\rangle = (|D\rangle + |A\rangle)/\sqrt{2}\\ |V\rangle = (|D\rangle - |A\rangle)/\sqrt{2}\end{cases}$$

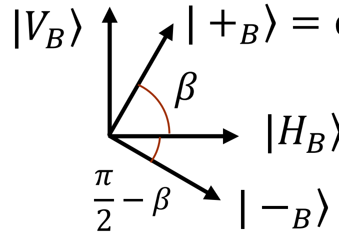
  - $|\psi^-\rangle = [|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B]/\sqrt{2}$
    $= [(|D\rangle + |A\rangle)_A(|D\rangle - |A\rangle)_B - (|D\rangle - |A\rangle)_A(|D\rangle + |A\rangle)_B]/2\sqrt{2}$
    $= [-|D\rangle_A|A\rangle_B + |A\rangle_A|D\rangle_B]/\sqrt{2}$
- Postulate 3
  - If the particle is in a state $|\psi\rangle$, measurement of the variable (corresponding to) Ω will yield one of the eigenvalues ω_i with probability of $P(\omega_i) \propto |\langle\omega_i|\psi\rangle|^2$.
  - Eigenvector corresponding to measurement of +1 by Alice and -1 by Bob is $|+_A\rangle \otimes |-_B\rangle$

Prediction by quantum theory II



$| +_A\rangle = \cos\alpha\, |H_A\rangle + \sin\alpha\, |V_A\rangle$

$| -_A\rangle = \sin\alpha\, |H_A\rangle - \cos\alpha\, |V_A\rangle$



$| +_B\rangle = \cos\beta\, |H_B\rangle + \sin\beta\, |V_B\rangle$

$| -_B\rangle = \sin\beta\, |H_B\rangle - \cos\beta\, |V_B\rangle$

- $|\psi^-\rangle = (|H_A\rangle|V_B\rangle - |V_A\rangle|H_B\rangle)/\sqrt{2}$
- $\langle\psi^-|(| +_A\rangle \otimes | +_B\rangle) = \frac{\langle H_A|\otimes\langle V_B| - \langle V_A|\otimes\langle H_B|}{\sqrt{2}}(\cos\alpha\, |H_A\rangle + \sin\alpha\, |V_A\rangle) \otimes (\cos\beta\, |H_B\rangle + \sin\beta\, |V_B\rangle)$
  $= \frac{\cos\alpha \sin\beta - \sin\alpha \cos\beta}{\sqrt{2}} = \frac{\sin(-\alpha+\beta)}{\sqrt{2}}$
- Similarly, for $| -_A\rangle$, replace α with $-\left(\frac{\pi}{2} - \alpha\right) = \alpha - \frac{\pi}{2}$
  - $\langle\psi^-|(| -_A\rangle \otimes | +_B\rangle) = \frac{\sin\left(-\left(\alpha-\frac{\pi}{2}\right)+\beta\right)}{\sqrt{2}} = \frac{\cos(-\alpha+\beta)}{\sqrt{2}}$
  - $\langle\psi^-|(| +_A\rangle \otimes | -_B\rangle) = \frac{\sin\left(-\alpha+\left(\beta-\frac{\pi}{2}\right)\right)}{\sqrt{2}} = \frac{-\cos(-\alpha+\beta)}{\sqrt{2}}$
  - $\langle\psi^-|(| -_A\rangle \otimes | -_B\rangle) = \frac{\sin\left(-\left(\alpha-\frac{\pi}{2}\right)+\left(\beta-\frac{\pi}{2}\right)\right)}{\sqrt{2}} = \frac{\sin(-\alpha+\beta)}{\sqrt{2}}$
- $E(\alpha,\beta)$

$$= |\langle\psi^-|(| +_A\rangle \otimes | +_B\rangle)|^2 - |\langle\psi^-|(| -_A\rangle \otimes | +_B\rangle)|^2 - |\langle\psi^-|(| +_A\rangle \otimes | -_B\rangle)|^2 + |\langle\psi^-|(| -_A\rangle \otimes | -_B\rangle)|^2$$

$$= \frac{1}{2}[\sin^2(-\alpha+\beta) - \cos^2(-\alpha+\beta) - \cos^2(-\alpha+\beta) + \sin^2(-\alpha+\beta)] = -\cos[2(\alpha-\beta)]$$

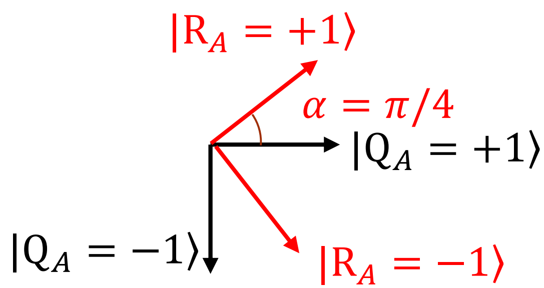
Prediction by quantum theory III

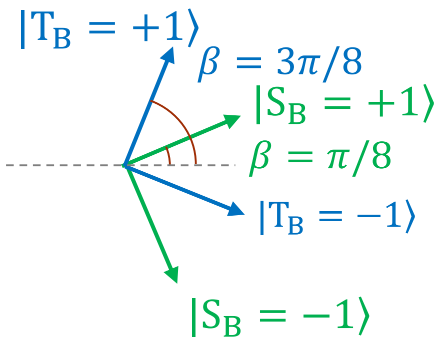
- From the previous page, $E(\alpha,\beta) = -\cos[2(\alpha-\beta)]$
- $S = E(QS) + E(RS) + E(RT) - E(QT)$

$$= E\left(0,\frac{\pi}{8}\right) + E\left(\frac{\pi}{4},\frac{\pi}{8}\right) + E\left(\frac{\pi}{4},\frac{3\pi}{8}\right) - E\left(0,\frac{3\pi}{8}\right)$$

$$= -\cos\left(-\frac{\pi}{4}\right) - \cos\left(-\frac{\pi}{4}\right) - \cos\left(-\frac{\pi}{4}\right) + \cos\left(-\frac{3\pi}{4}\right)$$

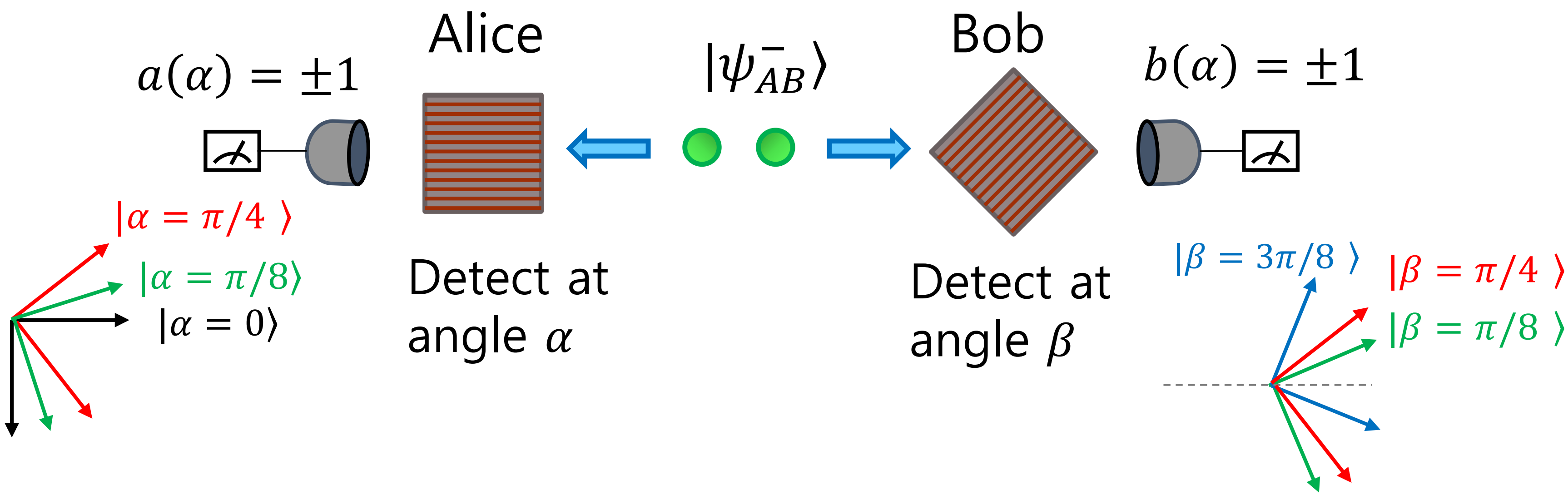
- $= -\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} = 2\sqrt{2} > 2$
- It is called as violation of Bell's inequality in CHSH form.





QKD based on entanglement II

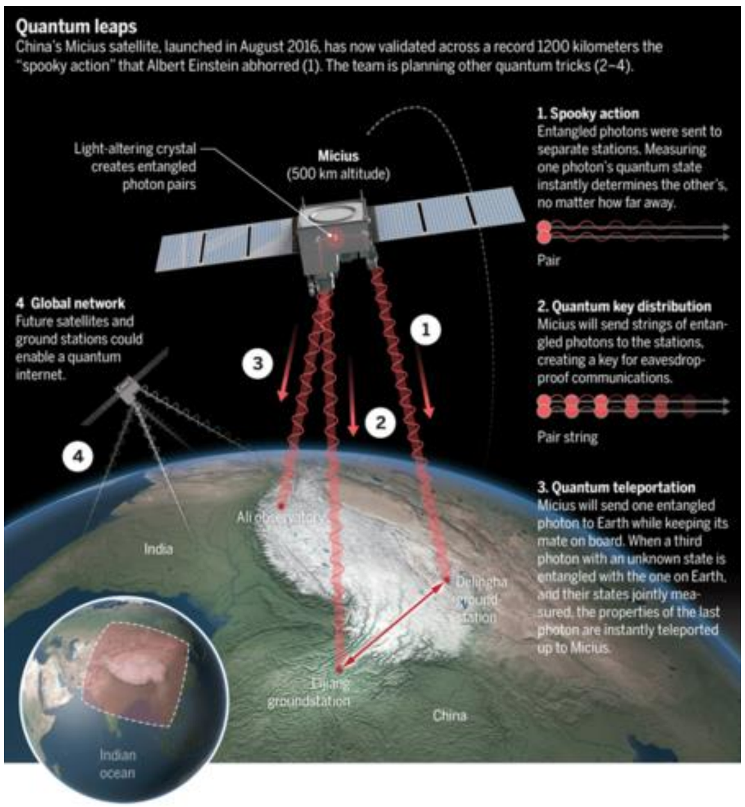
- E91 protocol
  - Developed by A. Ekert in 1991 (Phys. Rev. Lett. 67, 661 (1991))
  - Compared to CHSH measurement, Alice has $\alpha = \pi/8$ choice and Bob has $\beta = \pi/4$ choice.
  - When Alice and Bob use the same bases, they obtain the secure key.
  - When Alice and Bob use different bases, they perform CHSH test and if S is not close to $-2\sqrt{2}$, they conclude that there was eavesdropping attempt.



QKD based on quantum satellite

Yin *et al.*, *Science* **356**, 1140–1144 (2017)   16 June 2017

Satellite-based entanglement distribution over 1200 kilometers



- Mentioned in lecture 12
- News and video
  - https://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance
  - https://science.sciencemag.org/content/356/6343/1140

We used the distributed entangled photons for the Bell test with the Clauser-Horne-Shimony-Holt (CHSH)−type inequality (*30*), which is given by

$$S = |E(\phi_1,\phi_2) - E(\phi_1,\phi_2') + E(\phi_1',\phi_2) + E(\phi_1',\phi_2')| \leq 2$$

where $E(\phi_1,\phi_2)$, $E(\phi_1,\phi_2')$, and so forth are the joint correlations at the two remote locations with respective measurement angles of (ϕ_1,ϕ_2), (ϕ_1,ϕ_2'), and so forth. The angles are randomly selected among $(0, \pi/8)$, $(0, 3\pi/8)$, $(\pi/4, \pi/8)$, and $(\pi/4, 3\pi/8)$, quickly enough to close the locality (*31*) and freedom-of-choice loopholes (**Fig. 5A**). We ran 1167 trials of the Bell test during an effective time of 1059 s. The data observed in the four settings are summarized in **Fig. 5B**, from which we found $S = 2.37 \pm 0.09$, with a violation of the CHSH-type Bell inequality $S \leq 2$ by four standard deviations. The result again confirms the nonlocal feature of entanglement and excludes the models of reality that rest on the notions of locality and realism—on a previously unattained scale of thousands of kilometers.