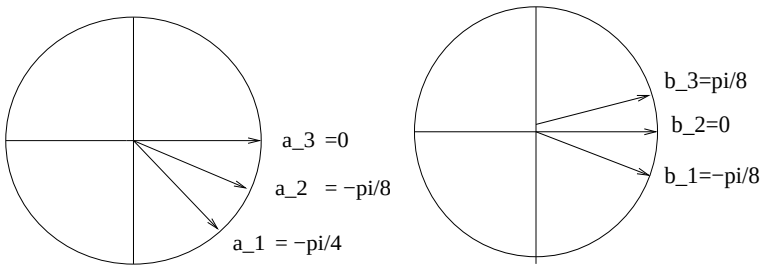

Figure 0.1 Alice and Bob's random choices of analyzers

0.1 Ekert protocol for quantum key distribution

A nice application of the CHSH inequality is a protocol for the generation of a secret key by two parties. We assume that a localized source of EPR particles delivers entangled Qbits to Alice and Bob at each time instant n in the state

$$|B_{00}\rangle = \frac{1}{2}(|00\rangle + |11\rangle) = \frac{1}{2}(|\theta\theta\rangle + |\theta_\perp\theta_\perp\rangle)$$

Moreover they have also established a noiseless communication channel.

The protocol:

- Alice has analyzers oriented in directions $\mathbf{a}_1$, $\mathbf{a}_2$, $\mathbf{a}_3$ and records the results of measurements, at each time instant, for the observables

  $$A(\mathbf{a}) = (+1)|\mathbf{a}\rangle\langle\mathbf{a}| + (-1)|\mathbf{a}_\perp\rangle\langle\mathbf{a}_\perp|$$

  where she chooses $\mathbf{a}$ randomly among $\mathbf{a}_1$, $\mathbf{a}_2$, $\mathbf{a}_3$ (figure 0.1).
- Bob has three analyzers oriented along $\mathbf{b}_1$, $\mathbf{b}_2$, $\mathbf{b}_3$ and records the results of measurements, at each time instant, for the observables

  $$B(\mathbf{b}) = (+1)|\mathbf{b}\rangle\langle\mathbf{b}| + (-1)|\mathbf{b}_\perp\rangle\langle\mathbf{b}_\perp|$$

  where he chooses $\mathbf{b}$ randomly among $\mathbf{b}_1$, $\mathbf{b}_2$, $\mathbf{b}_3$ (figure 0.1).
- Alice and Bob start a public discussion over the communication channel: they inform each other on what vectors they used at each time instant.
- They do a security check to ensure that no eavesdropper is present. Alice and Bob select the time instants when the basis choices were

  $$(\mathbf{a}_3, \mathbf{b}_3),\ (\mathbf{a}_3, \mathbf{b}_1),\ (\mathbf{a}_1, \mathbf{b}_1),\ (\mathbf{a}_1, \mathbf{b}_3)$$

  Note that these are the same four analyzer arrangements used for the Bell-CHSH inequalities (figure **??**). For such configurations and only for such ones they exchange their measurement results. Each party computes an empirical correlation coefficient

  $$X_{\text{exp}} = Av[a_n(\mathbf{a}_3)b_n(\mathbf{b}_3)] + Av[a_n(\mathbf{a}_3)b_n(\mathbf{b}_1)] - Av[a_n(\mathbf{a}_1)b_n(\mathbf{b}_3)] + Av[a_n(\mathbf{a}_1)b_n(\mathbf{b}_1)]$$

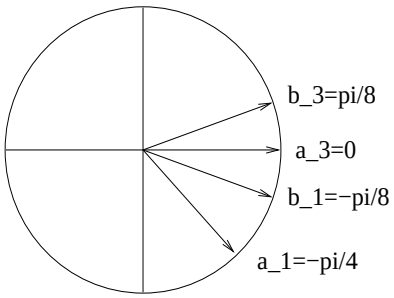

Figure 0.2 CHSH configuration

where Av is the empirical average. In a perfect world they should find $X_{exp} = 2\sqrt{2}$. We will see later that when an eavesdropper is present they will certainly find $X_{exp} \leq 2$ because the effect of the eavesdropper is to destroy the entanglement of the EPR pair and the system then behaves "classically". The security check thus consists in checking that

$$X_{exp} > 2$$

If the test passes they conclude there is no eavesdropper and generate the key, if not they stop communication.

- The key generation process is as follows. For every time n such that they used the same basis - that is $(\mathbf{a}_3, \mathbf{b}_2)$ or $(\mathbf{a}_2, \mathbf{b}_1)$ - they know for sure that

$$a_n = b_n = 1, \qquad \text{or} \qquad a_n = b_n = -1$$

(one can also check that in this case $\langle B_{00}|A \otimes B|B_{00}\rangle = \cos 2\widehat{(\mathbf{a}, \mathbf{b})} = 1$). Thus they have a common subsequence of ± 1's that they keep secret and forms their shared secret key.

Attacks from Eve. Let us consider the simplest measurement attack in which Eve captures each photon of the EPR pair and makes a measurement (figure 0.3). Then she sends each photon (in the resulting state) to Alice and Bob. She measures Alice's photon in the basis $\{\mathbf{e}_a, \mathbf{e}_a^\perp\}$ and Bob's photon in the basis $\{\mathbf{e}_b, \mathbf{e}_b^\perp\}$. Her strategy for the successive choices of basis at each time instant is described by a probability distribution

$$\rho(\mathbf{e}_a, \mathbf{e}_b) \geq 0, \qquad \int\int d^2\mathbf{e}_a d^2\mathbf{e}_b \, \rho(\mathbf{e}_a, \mathbf{e}_b) = 1$$

After Eve's measurement the pair of photons is left in one of the four tensor product states

$$|\mathbf{e}_a, \mathbf{e}_b\rangle, \ |\mathbf{e}_a, \mathbf{e}_b^\perp\rangle, \ |\mathbf{e}_a^\perp, \mathbf{e}_b\rangle, \ |\mathbf{e}_a^\perp, \mathbf{e}_b^\perp\rangle$$

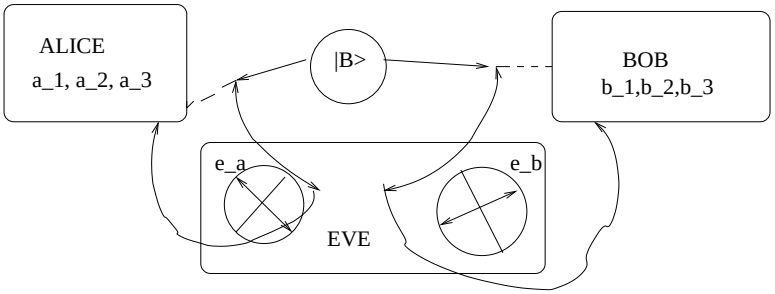

Figure 0.3 Eve collapses the pair in a tensor product state

with corresponding probabilities

$$|\langle \mathbf{e}_a, \mathbf{e}_b | B_{00}\rangle|^2 = \frac{1}{2}\cos^2(\widehat{\mathbf{e}_a, \mathbf{e}_b}), \qquad |\langle \mathbf{e}_a, \mathbf{e}_b^\perp | B_{00}\rangle|^2 = \frac{1}{2}\sin^2(\widehat{\mathbf{e}_a, \mathbf{e}_b})$$

$$|\langle \mathbf{e}_a^\perp, \mathbf{e}_b | B_{00}\rangle|^2 = \frac{1}{2}\sin^2(\widehat{\mathbf{e}_a, \mathbf{e}_b}), \qquad |\langle \mathbf{e}_a^\perp, \mathbf{e}_b^\perp | B_{00}\rangle|^2 = \frac{1}{2}\cos^2(\widehat{\mathbf{e}_a, \mathbf{e}_b})$$

Let us compute the correlation coefficient that Alice and Bob would find during the security test. Given Eve's choice $(\mathbf{e}_a, \mathbf{e}_b)$ we have

$$\begin{aligned} X(\mathbf{e}_a, \mathbf{e}_b) \; &= \tfrac{1}{2}\cos^2(\widehat{\mathbf{e}_a, \mathbf{e}_b}) S(\mathbf{e}_a, \mathbf{e}_b) + \tfrac{1}{2}\sin^2(\widehat{\mathbf{e}_a, \mathbf{e}_b^\perp}) S(\mathbf{e}_a, \mathbf{e}_b^\perp) \\ &+ \tfrac{1}{2}\sin^2(\widehat{\mathbf{e}_a^\perp, \mathbf{e}_b}) S(\mathbf{e}_a^\perp, \mathbf{e}_b) + \tfrac{1}{2}\cos^2(\widehat{\mathbf{e}_a^\perp, \mathbf{e}_b^\perp}) S(\mathbf{e}_a^\perp, \mathbf{e}_b^\perp) \end{aligned}$$

where $S(\mathbf{v}, \mathbf{w})$ is the correlation coefficient for a pair of photons in the state $|\mathbf{v}, \mathbf{w}\rangle$ resulting from Eve's measurement,

$$S(\mathbf{v}, \mathbf{w}) = \langle \mathbf{v}, \mathbf{w} | A(\mathbf{a}_3) \otimes B(\mathbf{b}_3) + A(\mathbf{a}_3) \otimes B(\mathbf{b}_1) - A(\mathbf{a}_1) \otimes B(\mathbf{b}_3) + A(\mathbf{a}_1) \otimes B(\mathbf{b}_1) | \mathbf{v}, \mathbf{w}\rangle$$

The average correlation coefficient found by Alice and Bob when Eve operates is

$$X = \int\int d^2\mathbf{e}_a d^2\mathbf{e}_b \, \rho(\mathbf{e}_a, \mathbf{e}_b) X(\mathbf{e}_a, \mathbf{e}_b)$$

We leave it as an exercise to check that $|S(\mathbf{v}, \mathbf{w})| \leq 2$. This is not too surprising since $|\mathbf{v}, \mathbf{w}\rangle$ is a tensor product state. This immediately leads to,

$$|X| \leq 2.$$

Thus Alice and Bob notice the presence of Eve. Note that Eve could manipulate (unitarily) the pair after her measurements in order to send other photon states to Alice and Bob. However if she re-entangles the photons she behaves as a new source for Alice and Bob, and she gets no information from their measurements!

Finally let us note that if Eve copies the EPR pair (this can be done with a machine that copies the four orthogonal Bell states) and waits for the public discussion before doing the measurements, she gets no information about the secret key. Indeed her measurements operate on a different pair and thus she

gets the same result than Alice and Bob only half of the time. This is equivalent to flip a coin at each time instant and cannot yield information.

Experiments. see in Review of Modern Physics **74** p 145-190 (2002) the extensive article "Quantum cryptography" by N. Gisin, G. Ribordy, W. Tittel, H. Zbinden.