E91 Quantum Key Distribution Protocol - a step by step proof

Dariusz Lasecki

1 Quantum Key Distribution (E91 protocol)

The E91 protocol [Eke91], proposed by Ekert, is one of the first important applications of quantum entanglement. It allows Alice and Bob to establish a secret key or detect the presence of an adversary. Such a provably secret key can be then used for provably secure communication using the so called one-time pad method. The E91 protocol is the modification of the well-known BB84 protocol [BB84] which accomplishes the same task. The main difference between them is that the BB84 protocol requires quantum communication between Alice and Bob and for the E91 protocol it is enough for Alice and Bob to have shared entanglement.

E91 protocol [Eke91]

Input:
Alice and Bob: supplied n quantum states claimed to be maximally entangled states $\left|\Psi_2^-\right\rangle_{AB}$ (singlets)
Resources:
Shared by Alice and Bob: a public classical communication channel.
Goal: Alice and Bob establish a shared secret key
Protocol:

1. Suppose Alice and Bob can measure a qubit along one of the vectors $\{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3\}$ and $\{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\}$ respectively, which correspond to measurements in a computational basis $\{|0\rangle, |1\rangle\}$ rotated by angles $\left\{0, \frac{\pi}{4}, \frac{\pi}{2}\right\}$ and $\left\{\frac{\pi}{4}, \frac{\pi}{2}, \frac{3\pi}{4}\right\}$ respectively. Alice and Bob measure their share of maximally entangled states along one of the vectors uniformly at random and independently of each other.

2. Alice and Bob publicly announce their measurement vectors. They keep measurement results of qubits for which they used the same basis, i.e., along $(\mathbf{a}_2, \mathbf{b}_1)$ and $(\mathbf{a}_3, \mathbf{b}_2)$, as a potential secret key.

3. The rest of the measurement results are announced publicly and analyzed to detect a potential adversary. Alice and Bob calculate the empirical value of the correlation coefficient

$$S = E(\mathbf{a}_1, \mathbf{b}_1) - E(\mathbf{a}_1, \mathbf{b}_3) + E(\mathbf{a}_3, \mathbf{b}_1) + E(\mathbf{a}_3, \mathbf{b}_3),$$

where $E(\mathbf{a}_i, \mathbf{b}_j) = P_{++}(\mathbf{a}_i, \mathbf{b}_j) + P_{--}(\mathbf{a}_i, \mathbf{b}_j) - P_{+-}(\mathbf{a}_i, \mathbf{b}_j) - P_{-+}(\mathbf{a}_i, \mathbf{b}_j)$ and $P_{\pm\pm}(\mathbf{a}_i, \mathbf{b}_j)$ means the probability of obtaining results ± 1 and ± 1 when measuring along $\mathbf{a}_i$ and $\mathbf{b}_j$.

4. If Alice and Bob obtain $S \approx 2\sqrt{2}$, they use perfectly anti-correlated (and secret) results of measurements along $(\mathbf{a}_2, \mathbf{b}_1)$ and $(\mathbf{a}_3, \mathbf{b}_2)$ as their secret key. Otherwise, they assume that an eavesdropper tempered with singlets and they abort the protocol.

Theorem 1.1. *E91 protocol establishes a secret key of length about $\frac{n}{3}$ or provides statistical evidence for the presence of an adversary.*

Proof. This proof follows [Eke91]. We consider the correlation coefficient S from the protocol, $S = E(\mathbf{a}_1, \mathbf{b}_1) - E(\mathbf{a}_1, \mathbf{b}_3) + E(\mathbf{a}_3, \mathbf{b}_1) + E(\mathbf{a}_3, \mathbf{b}_3)$. We now show, that if singlets are not tempered with, the coefficient S has a value $S = -2\sqrt{2}$. Suppose $\mathbf{a}_i$ and $\mathbf{b}_j$ are measurements in a computational basis rotated by angles α and β respectively. We introduce rotation matrices given by

$$S_\alpha = \begin{bmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{bmatrix},$$

$$S_\beta = \begin{bmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{bmatrix}.$$

The spin-$\frac{1}{2}$ measurement of two particles along directions α and β is given by $M_{\alpha,\pm} \otimes M_{\beta,\pm} = \frac{1}{4}(I \pm S_\alpha) \otimes (I \pm S_\beta)$. Since it is a symmetric projection, the probabilities from the protocol can be calculated as follows

$$\begin{aligned} P_{++}(\mathbf{a}_i, \mathbf{b}_j) &= \left\langle \Psi_2^- \right| M_{\alpha,+} \otimes M_{\beta,+} \left| \Psi_2^- \right\rangle, \\ P_{+-}(\mathbf{a}_i, \mathbf{b}_j) &= \left\langle \Psi_2^- \right| M_{\alpha,+} \otimes M_{\beta,-} \left| \Psi_2^- \right\rangle, \\ P_{-+}(\mathbf{a}_i, \mathbf{b}_j) &= \left\langle \Psi_2^- \right| M_{\alpha,-} \otimes M_{\beta,+} \left| \Psi_2^- \right\rangle, \\ P_{--}(\mathbf{a}_i, \mathbf{b}_j) &= \left\langle \Psi_2^- \right| M_{\alpha,-} \otimes M_{\beta,-} \left| \Psi_2^- \right\rangle. \end{aligned}$$

Using the results above, we obtain

$$E(\mathbf{a}_i, \mathbf{b}_j) = P_{++}(\mathbf{a}_i, \mathbf{b}_j) - P_{+-}(\mathbf{a}_i, \mathbf{b}_j) - P_{-+}(\mathbf{a}_i, \mathbf{b}_j) + P_{--}(\mathbf{a}_i, \mathbf{b}_j) = -\cos(\alpha - \beta) = -\mathbf{a}_i \cdot \mathbf{b}_j.$$

Therefore, using the actual angles of measurements and remembering that we deal with unit vectors, we obtain

$$S = -(\mathbf{a}_1 \cdot \mathbf{b}_1 - \mathbf{a}_1 \cdot \mathbf{b}_3 + \mathbf{a}_3 \cdot \mathbf{b}_1 + \mathbf{a}_3 \cdot \mathbf{b}_3) = -\cos\left(0 - \frac{\pi}{4}\right) + \cos\left(0 - \frac{3\pi}{4}\right) -$$

$$-\cos\left(\frac{\pi}{2} - \frac{\pi}{4}\right) - \cos\left(\frac{\pi}{2} - \frac{3\pi}{4}\right) = -3\cos\left(\frac{\pi}{4}\right) + \cos\left(\frac{3\pi}{4}\right) = -2\sqrt{2}.$$

Let us now consider the case in which an eavesdropper interferes with singlets to later obtain some information about the secret key. All the eavesdropper can do is to try measuring qubits that form a singlet along a certain direction which may vary from pair to pair, depending on whatever malicious strategy the eavesdropper may have. In this scenario, the correlation coefficient is of the form

$$S = \int \rho(\mathbf{n}_a, \mathbf{n}_b) d\mathbf{n}_a d\mathbf{n}_b [(\mathbf{a}_1 \cdot \mathbf{n}_a)(\mathbf{b}_1 \cdot \mathbf{n}_b) - (\mathbf{a}_1 \cdot \mathbf{n}_a)(\mathbf{b}_3 \cdot \mathbf{n}_b) +$$

$$+(\mathbf{a}_3 \cdot \mathbf{n}_a)(\mathbf{b}_1 \cdot \mathbf{n}_b) + (\mathbf{a}_3 \cdot \mathbf{n}_a)(\mathbf{b}_3 \cdot \mathbf{n}_b)],$$

where $\mathbf{n}_a, \mathbf{n}_b$ are directions along which measurements were performed by an eavesdropper on Alice's and Bob's particles respectively. In our protocol, it can be further simplified by substituting the actual values for measurement directions. Suppose that measurements along $\mathbf{n}_a$ and $\mathbf{n}_b$ are parametrized by angles α and β respectively. Remembering that we deal with unit vectors, we have

$$S = \int \rho(\mathbf{n}_a, \mathbf{n}_b) d\mathbf{n}_a d\mathbf{n}_b \left[\cos(\alpha - 0) \cos\Big(\beta - \frac{\pi}{4}\Big) - \cos(\alpha - 0) \cos\Big(\beta - \frac{3\pi}{4}\Big) + \right.$$

$$\left. + \cos\Big(\alpha - \frac{\pi}{2}\Big) \cos\Big(\beta - \frac{\pi}{4}\Big) + \cos\Big(\alpha - \frac{\pi}{2}\Big) \cos\Big(\beta - \frac{3\pi}{4}\Big) \right] =$$

$$= \int \rho(\mathbf{n}_a, \mathbf{n}_b) d\mathbf{n}_a d\mathbf{n}_b \left[\sqrt{2} \cos(\alpha - \beta) \right] = \int \rho(\mathbf{n}_a, \mathbf{n}_b) d\mathbf{n}_a d\mathbf{n}_b \left[\sqrt{2} \mathbf{n}_a \cdot \mathbf{n}_b \right] =$$

$$= \sqrt{2} \int \rho(\mathbf{n}_a, \mathbf{n}_b) d\mathbf{n}_a d\mathbf{n}_b \left[\mathbf{n}_a \cdot \mathbf{n}_b \right].$$

By examining the integral, we see that it is lower and upper bounded by -1 and 1 respectively. Thus, the coefficient S can take values from the range

$$-\sqrt{2} \leq S \leq \sqrt{2}.$$

Therefore, we showed that based on the value of S that Alice and Bob calculate empirically, they can obtain the statistical evidence of the presence of an eavesdropper. If they are convinced that they are not present, they can use their secret results from measurements along the same direction to establish a secret binary key. We notice that if Alice and Bob were sent n singlet pairs and performed n measurements on them, on average one third of their measurements should happen in the same basis. Therefore, the number of bits that can constitute for a secret key is roughly $\frac{n}{3}$. □

References

[BB84] Charles Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: vol. 560. Jan. 1984, pp. 175–179. DOI: 10.1016/j.tcs.2011.08.039.

[Eke91] Artur K. Ekert. "Quantum cryptography based on Bell's theorem". In: *Phys. Rev. Lett.* 67 (6 Aug. 1991), pp. 661–663. DOI: 10.1103/PhysRevLett.67.661. URL: https://link.aps.org/doi/10.1103/PhysRevLett.67.661.