# Ralph's EPR QKD

Quantum key distribution is provably secure (unlike RSA or elliptical curve cryptography). EPR QKD (entangled quantum key distribution) is one protocol demonstrating QKD security. The protocol is as follows:

1. Ralph (the sender) creates $2n$ EPR pairs in the state $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ or $|\beta_{00}\rangle^{\otimes 2n} = |\beta_{00}\rangle \otimes \cdots \otimes |\beta_{00}\rangle$.

2. Ralph selects a random $2n$-bit string $b$ and performs a Hadamard transformation on the second half of each EPR pair for which $b = 1$.

3. Ralph sends the second half of each EPR pair to Alice (the receiver).

4. Alice announces receipt of the qubits.

5. Ralph selects $n$ of the $2n$ encoded pairs to serve as check bits to test for Eve's interference (indistinguishable from noise in the channel).

6. Ralph announces $b$ and which $n$ EPR pairs serve as check bits.

7. Alice performs Hadamard transforms on the qubits where $b = 1$.

8. Ralph and Alice each measure their halves of the $n$ EPR pairs in the $|0\rangle, |1\rangle$ basis (that is, using observable $Z$) and share their results. If too many of these $\pm 1$ measurements disagree, they abort the protocol and start over.

9. Ralph and Alice measure their remaining $n$ qubits according to the check matrix for a pre-determined $[n, m]$ quantum code (correcting up to $t$ errors). They share their results, compute the syndromes for the errors, and then correct their state obtaining $m$ (nearly perfect) EPR pairs.[1]

10. Ralph and Alice measure the $m$ EPR pairs in the $|0\rangle, |1\rangle$ basis to obtain a shared (randomly generated) secret key $k$.

Suppose Alice and Ralph agree to use a quantum Hamming $[n = 7, m = 4]$ code (capable of correcting one bit flip and/or one phase flip error). The check matrix, measured one row at a time, is

$$\begin{bmatrix} X_1X_5X_6X_7 \\ X_2X_4X_6X_7 \\ X_3X_4X_5X_6 \\ Z_1Z_3Z_4Z_7 \\ Z_2Z_3Z_5Z_7 \\ Z_1Z_2Z_3Z_6 \end{bmatrix}$$

where, for instance, $X_1X_5X_6X_7 = X \otimes I \otimes I \otimes I \otimes X \otimes X \otimes X$. $X$ measures in the $|+\rangle, |-\rangle$ or $H|0\rangle, H|1\rangle$ basis while $Z$ measures in the $|0\rangle, |1\rangle$ basis with eigenvalues (measurement results) $\pm 1$ (eigenvalue $= +1$ corresponds to eigenstate $|+\rangle$ or $|0\rangle$ and binary 0 while eigenvalue $= -1$ corresponds to eigenstate

[1] See Nielsen and Chuang exercise 12.34.

$|-\rangle$ or $|1\rangle$ and binary 1). Alice only cares about bit flips to generate a shared key, therefore only the last three rows of the check matrix are needed.

Suggested:

1. Suppose their is no interference. Apply the protocol to the $n = 7$ EPR pairs (ignore the check qubits) and generate an $m = 4$ random shared private key.

2. Suppose the second qubit (the first qubit delivered to Alice) in the first EPR pair is bit flipped (this transforms $|\beta_{00}\rangle$ to $|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle))$. Apply the protocol to the $n = 7$ EPR pairs (ignore the check qubits) including correcting any errors indicated by syndrome, and generate an $m = 4$ random shared private key.