Ralph's CSS QKD

This CSS QKD derives from EPR QKD. We borrow CSS error correction (see Ralph's stabilizer code) to replace explicit usage of entanglement but the key is still effectively randomly generated. CSS error correction is employed for information reconciliation and privacy amplification.

The CSS algorithm for Ralph to privately send a key to Alice with arbitrarily small probability that Eve can intercept and identify the key (without detection by Ralph and Alice) is as follows.

1. Ralph and Alice publicly select their CSS stabilizer code.

2. Ralph creates two random n bit strings x and z.

3. Ralph encodes a random m bit key k via

$$CSS_{z,x}\left(C_1, C_2\right) = \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} (-1)^{z*w} \left|v_k + w + x\right\rangle$$

where v_k is an n bit encoding of k and $|C_2|$ is the number of elements in C_2. Ralph creates n random check bits and randomly assigns the check bits to a $2n$ bit string b with the code assigned to the remaining n bits. These are encoded as qubits $|0\rangle$ or $|1\rangle$. Hadamard transformation is applied to the $|1\rangle$ qubits in b.

4. Ralph sends b to Alice.

5. Alice acknowledges receipt of the qubits.

6. Ralph announces b, x, z, which n cubits provide check bits and their values.

7. Alice performs Hadamards on the qubits where b is one.

8. Alice measure the check qubits in the $|0\rangle, |1\rangle$ basis and publicly shares the results with Ralph. If too many disagree, they abort the protocol and try again.

9. Alice measures and decodes the remaining n qubits from $CSS_{z,x}\left(C_1, C_2\right)$ and recovers Ralph's private key k.[1]

Steps 2 and 3 generate a random seven bit code (like EPR QKD) and x indicates which qubit, if any, are bit flipped to generate a legal code word (this can be determined from the Z portion of the check matrix). While z is important to address phase in quantum error correction, it is not needed for QKD. When Alice receives x it is simplest if she simply bit flips the qubit identified by x prior to determining the syndrome and performing any error correction that may have occurred during transmission.

As the qubits are randomly assigned from Eve's perspective, she cannot keep a copy (quantum information forbids cloning or duplication of information —

[1]Since CSS is a linear code, the m bit string can be recovered from the n bit string by row operations (Gaussian elimination and back-substitution).

information is physical and conserved), and measuring the qubits almost surely changes the state, quantum encryption provably thwarts Eve. Qubits may be garbled during transmission due to Eve or simply noise. The CSS protocol can fix a limited number of errors. Otherwise, the key is discarded and the randomized protocol repeated.

Suggested:

Alice and Ralph use the quantum Hamming $[7, 4]$ code from Ralph's stabilizer code. x and z are each chosen from the following eight possibilities

$$\begin{array}{ccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}$$

w is chosen from C_2

$$\begin{array}{ccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{array}$$

and v_k is chosen from the two legal code words (see Ralph's stabilizer code).

$$|0_L\rangle . = \frac{1}{\sqrt{8}}\{|0000000\rangle + |0011110\rangle + |0101011\rangle + |0110101\rangle$$
$$+ |1000111\rangle + |1011001\rangle + |1101100\rangle + |1110010\rangle\}$$

and

$$|1_L\rangle = \frac{1}{\sqrt{8}}\{|1111111\rangle + |1100001\rangle + |1010100\rangle + |1001010\rangle$$
$$+ |0111000\rangle + |0100110\rangle + |0010011\rangle + |0001101\rangle\}$$

Suppose $k = [0100], z = [0000000]$, the check bits are in the first seven positions, and the code is in the last seven positions of b.

1. Suppose there is no interference and the randomly generated code is [0100110], what is x and do Alice and Ralph share the same key?

2. Repeat 1 where the randomly generated code is [0100111].

3. Suppose everything is as in 2 except the first qubit is bit flipped during transmission. Repeat 1.