Electrodynamics Notes

1 Recap/Intro

Recall what oracles do and how quantum algorithms work. Recall further that the takeaway from Deutsch-Josa is that oracles change the computational question from find an answer to confirm an answer. Today we're talking about how to make and break encryption.

2 Today's stuff

We consider two kinds of encryption - symmetric and asymmetric. Considering a message, the sender encrypts the message, sends it, and the receiver decrypts it. Symmetric encryption is when the same thing is used to encrypt and decrypt - asymmetric is not.

We'll start with **XOR masks**. Let's make a message,

$$M = 10011$$

and an encryption key,

$$K = 01100$$

All we do is we take the XOR of these two, giving us a cipher:

$$C = 11111$$

Alice then sends this message to Bob, who decodes the message by XORing it with his key, giving him the original message. XOR masks like this are used in current encryption protocols.

Today, our goal is to, given an input message and a cipher, to find the key. That's what we call Simon's algorithm, which is similar to the Deutsch-Josa algorithm - it's just that instead of 1 ancilla bit, we have N ancilla bits. Also, only the computational bits go through the Hadamard gates each time, and all of them get measured - other than that, same thing. This oracle, though, has a different job - it needs to find the collision. Also, the starting state is:

$$|0\rangle^n \otimes |0\rangle^n$$

where the first group is the computational bits and the second is the ancilla bits. The state after the Hadamards will become:

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}} |x\rangle \otimes |0\rangle$$

Now, we apply the oracle:

$$\hat{O}\,|x\rangle\,|y\rangle = |x\rangle\,|y \oplus f(x)\rangle$$

making our state:

$$\frac{1}{\sqrt{2^n}} \sum_{x} |x\rangle\,|f(x)\rangle$$

where $f(x)$ is our XOR mask, containing the key. Now, we move up the measurement of the ancilla bits and we measure them before applying the Hadamard to the computational bits, making the system collapse:

$$f(x) = f(x \oplus x)$$

$$\frac{1}{\sqrt{2}} \left[|x\rangle + |x \oplus s\rangle\right] |f(x)\rangle$$

Next we apply the Hadamard to the computational bits:

$$\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\sum\left[(-1)^{x\cdot z}+(-1)^{(x\oplus s)\cdot z}\right]\cdot|z\rangle$$

$$\frac{1}{\sqrt{2^N+1}}\sum(-1)^{x\cdot z}\left[1+(-1)^{s\cdot z}\right]|z\rangle$$

3 What's next