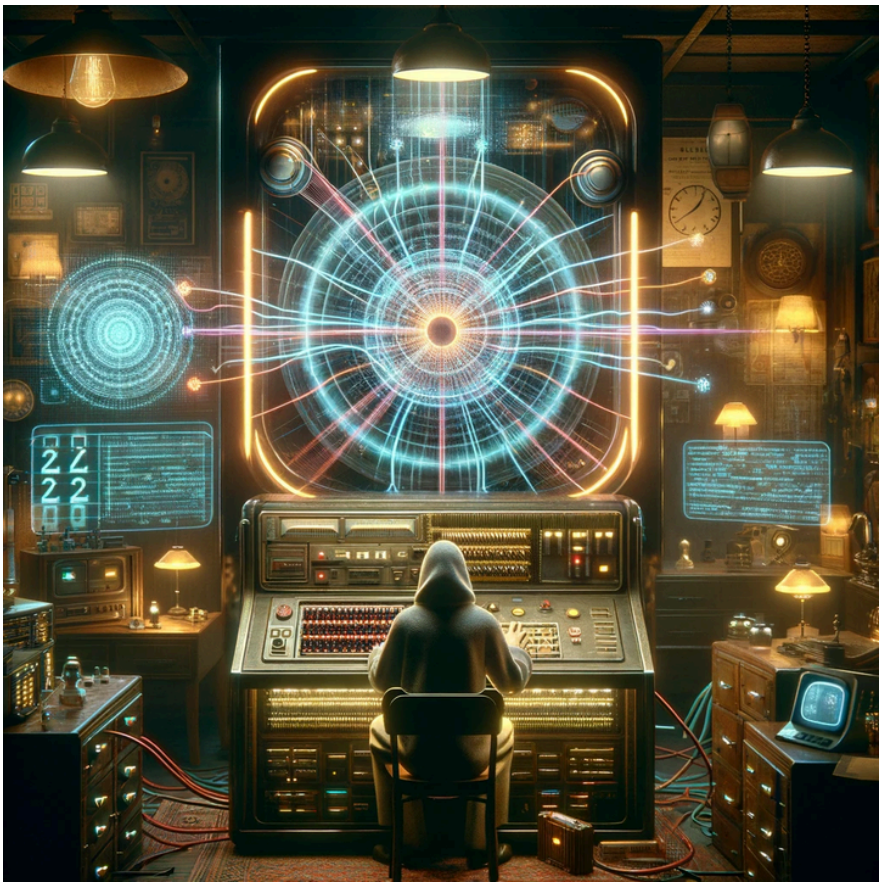
Quantum Vault Hacking:



As the title suggested, why would anyone come to a hackathon and do anything other than hacking.

Rumor has it that IonQ locked up a pool of money to donate to local schools to support education in quantum. Our goal is to hack IonQ's pool of money and use it to buy video games. If you think this is awesome and ready to proceed, please skip the Turquoise contents. But if not, please accept my apology, close your eyes, meditate for 10 minutes, and imagine a new start from the next paragraph.

Rumor has it that IonQ prepared a pool of money to donate to local schools to support education in quantum. But an evil group hacked into the financial system and locked up the money so they can later use it to buy video games. Our goal is to anti-hack the evil group to free up the pool of money.

You may wonder what is the point of us writing and you reading the above two paragraphs of nonsense. Maybe we want to show you the intriguing perspective of the quantum entangled parallel universe. Maybe we just got bored stuck in a meeting. Or maybe we just want to make you say "what the hack?". After all, at a hackathon it's all about hacking.

For security reasons, the money is locked up separately in 13 batches we will refer to as "vaults". Each vault is protected by a "key" – a secret quantum state $|\psi_k\rangle = U_k|0\rangle$. Here $|0\rangle$ represents the initial state which has all qubits in 0. Your goal is to come up with an attack, U_A, which inverts U_k. More formally, you want to find U_A such that $\langle 0|U_A U_k|0\rangle = 1$.

Like what we've been told again and again in cyber security training that most hacks are based on social engineering, via phishing email you established a backdoor that would allow you to probe each one of the 13 keys $|\psi_k\rangle$ up to 20 times (so 13*20 times for all the 13 keys).

Specifically, each probe is a round of circuit submission and result retrieval performed in the following way:

1. You submit a probe circuit U_P to the server.
2. The server simulates the state $|\psi_k'\rangle = U_p U_k |0\rangle$ and measures for 500 shots in the computational basis.
3. The measurement results, as a histogram h_p, are then returned to the participants.

(*Note the returned results are formatted as a histogram, where each element is a big-endian integer representation of measurement outcomes for the measurement key in that repetition.)

Feel free to use the probed information $\{U_p, h_p\}$ anyway you want. The goal is to prepare the attack circuit U_A.

After you send the attack circuit U_A to the server, it will free up a portion of the batch of money in the vault specified exactly by $\alpha\langle 0|U_A U_k|0\rangle$. α is a factor that punishes attacks that involve more resources, because they are more suspicious. It is well known to the hacking industry that $\alpha = n_g * 4/(n_g * 4 + x)$ where x is the number of 2 qubit gates used in the attack. And n_g is the number of two-qubit gates IonQ used in U_k.

Beware each one of the 13 vaults will only allow up to 20 attack attempts before it gets locked up.

Let's see who can free up the most amount of money. Cheers!

Good news! To get a better chance of sharing your “$80M in Swiss Bank” someone at IonQ just responded your phishing email and shared some important information regarding the design of secrete keys $|\psi_k\rangle = U_k|0\rangle$:

1. The key to vault 0 is a test key that can be attacked and probed for double the amount of times. It is just a 3-qubit GHZ state(https://www.quantiki.org/wiki/ghz). There’s no money in vault 0, but we think it’s equally fun to hack!
2. For the rest of the 12 vaults, IonQ used 3 different algorithms to generate secret keys.
3. 4 of the secret keys are generated with parametric quantum circuits made of alternating single-qubit layers and two-qubit entangling layers (https://arxiv.org/abs/1812.08862). These 4 keys involve only small numbers of qubits.
4. 4 of the secret keys are generated as Matrix Product States of quite small bond dimensions(https://tensornetwork.org/mps/).
5. 4 of the secret keys are generated as graph states (https://en.wikipedia.org/wiki/Graph_state).
6. The number of qubits used in each secret key is no larger than 15, for some it could be as small as 2.
7. **There is actually an additional vault —”the holy 14th” that is only accessible after the score(“money”) you obtained in the first 13 vaults exceeds a threshold. This vault is so important that the encryption is running on an actual IonQ QPU. Rumor goes that this vault holds IonQ CEO’s browser history, so the stake is very high so the reward you receive from this vault is 3x more.**

This person at IonQ seems to have a strong faith in you. Maybe send him at least a pair of socks?