HyperSpace Security, Inc.'s Blog Post #2: Quantum Computing

Welcome Again

Your interest in HyperSpace Security, Inc.'s blog is appreciated!

Some background information follows:

HyperSpace offers a radical breakthrough in data security by eliminating the need to store a cryptographic master key, which is vulnerable to today's computers and social engineering. With HyperSpace's technology, master keys are never persistently stored and therefore cannot be hacked or stolen resulting in a "keyless" system. The technology not only protects against attacks based on quantum computing, it also provides unique benefits by securing payment systems, enhancing enterprise key management, bolstering multi-factor authentication, and securing blockchains and private key infrastructure.

In this forum, we will discuss issues related to data security, advances in mathematics and quantum computing, vulnerabilities of blockchains and other security technologies to attack, hacks that have harmed real people in the real world, and more. Some of these posts will get a little deep into some math. That said, we will try to make the content understandable to anyone interested in these fields.

Please feel free to provide comments and feedback. We value your input!

Today's Topic

The topic of today's blog post is quantum computing. A lot of people including security professionals do not think this is a real or a true threat vector. To be blunt, they are wrong.

Sorry, we will get into some math again, but most of this blog post should be easily understood by people without a math background. Warning: I will get into some deep math at a few points scattered throughout.

What is Quantum Computing?

Let's start with the basic idea of what is called "classical computing." This type of computing is used by everything people think of as computers: smart watches, mobile phones, laptop computers, desktop computers, the very large computers used by big companies, and more. Classical computing is very good at running though a lot of things in sequence and even sometimes in parallel to solve some tough math problems, processes information, and basically make the digital world work.

But classical computing cannot solve some problems. For example, classical computing is completely incapable of solving an NP Complete Problem. See https://en.wikipedia.org/wiki/NP-completeness.

Most classical computing represents information as groups of binary bits, namely 1's or 0's. For example, the decimal number 14 is represented in binary as 1110 and the decimal number 10 is represented in binary as 1010. Pretty cool and very effective for a lot of things.

Quantum computing is different. It represents information using **qbits that can be both 1's and 0's at the same time**. For example, a 4 qbit number can represent all decimal numbers from 0 to 15 **at the same time.**

Now what's that mean? Let's take a simple example.

Factor a big or even small number. We'll start with the number 15. The factors of 15 are 3 and 5 because 3 times 5 equals 15. Easy, right? But it gets harder if the numbers are very big. Per our last blog post, the difficulty of factoring big numbers is the basis for a lot of the data security people rely upon for communicating with banks and utility companies, online shopping such as Amazon and eBay, and almost everything else online.

For a classical computer to factor a big number, it has to try each potential factor in turn. Now, we can develop math that can simplify the approach, but's it is all still a repetitive one. A quantum computer? It can try many of them at once using qbits.

That's a game changer.

Quantum computing has other applications besides factoring big numbers. (By the way, there are some good theories that say this is how your own brain works.)

Is Quantum Computing Real?

Short answer is yes. See https://www.research.ibm.com/ibm-q/learn/what-is-quantum-computing/ (IBM), https://ai.google/research/teams/applied-science/quantum-ai/ (Google), and https://quantumcurriculum.mit.edu (MIT). Pretty sure they know what's real or not.

Some Math

Actually applying quantum computing to real problems presents some difficulties that are beyond the scope of this blog post. That said, some very smart people have developed ways to do so. A couple examples are Shore's and Grover's algorithms. Decent explanations of these can be found at https://en.wikipedia.org/wiki/Shor%27s_algorithm and https://en.wikipedia.org/wiki/Grover%27s_algorithm. The algorithms actually exist, are peer reviewed, and have significant implications for data security.

Our Approach

What we created was specifically designed to be immune to attacks based on quantum computing including use of Shore's, Grover's, and related algorithms. It is even immune to our own prime spiral factoring attack.

About the Author

Dane C. Butzer is the inventor of HyperSpace Security, Inc.'s Key Shadowing technology. He holds a Bachelor of Science in Electrical Engineering, a Master of Science, and a Juris Doctor, all from the Ohio State University. Mr. Butzer also has been published in Applied Optics and in the Appendix of the first edition of Bruce Schneier's seminal work *Applied Cryptography*. He has held several patents including currently issued U.S. Patent No. 9,634,836 for "Key Shadowing."

For More Information

Questions can be posted on this blog. We will try to answer those questions. You can also follow us on Twitter @keyshadowing or contact the author at dbutzer@keyshadowing.com.