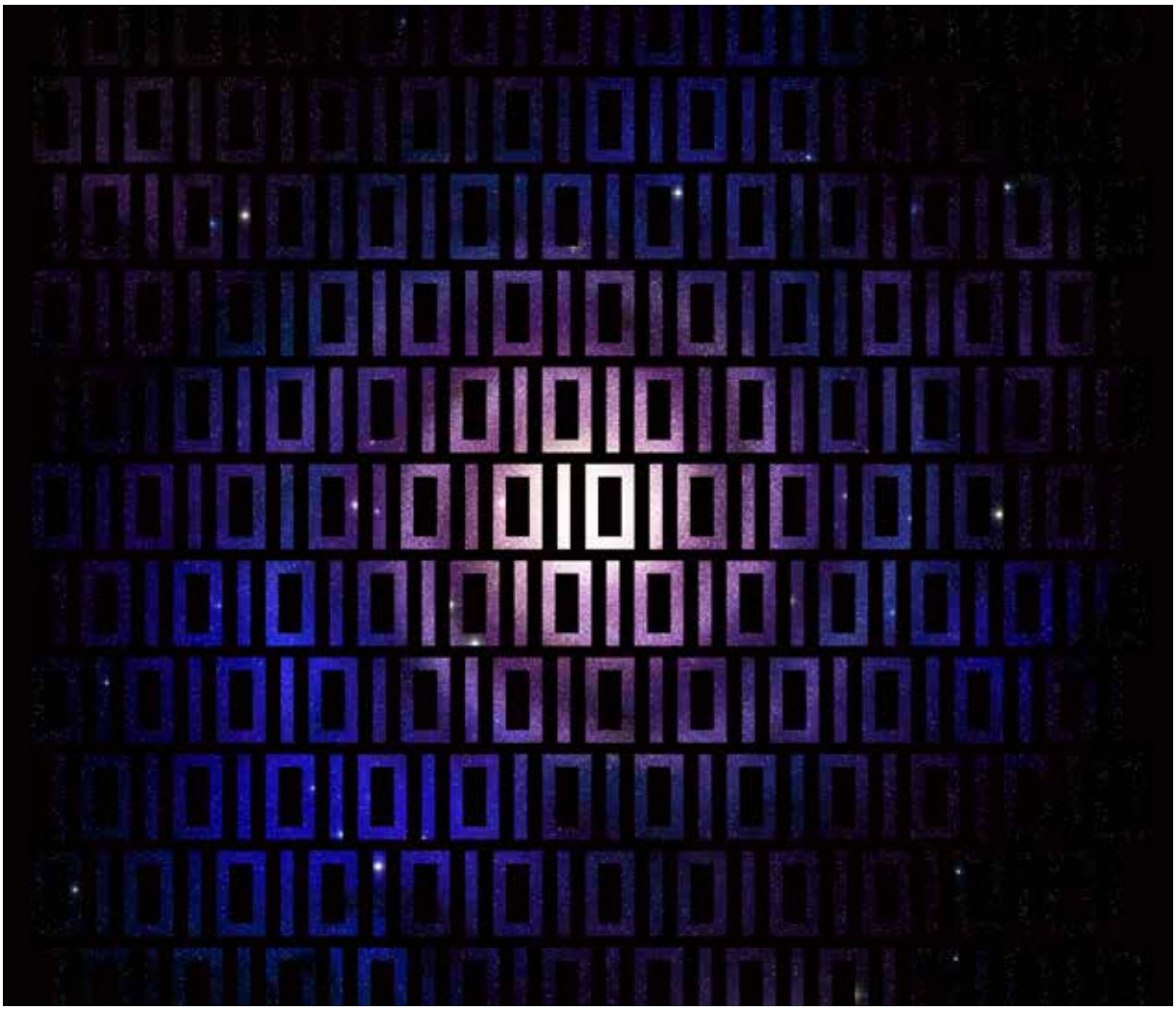

The Big Bang Theory of Security

BY FLEMING FREE

Look for more investment into computer security technology that relies on quantum theories of computing.

Quantum computing and encryption, qubits, and superposition — words that sound like the basis of a plot on the hit CBS sitcom The Big Bang Theory. These complex scientific terms are concepts that are core to the next quantum leap in data security — pun intended. According to a Ponemon Institute study, each data breach in the United States in 2013 cost an estimated $3.5 million. With several more high-profile data security issues in 2014, the growing costs for companies and global economies may bring more serious investment in a next-generation solution.

Current standard encryption techniques make use of public and private keys. Even with today's fastest computers, the encryption algorithms are complex enough that standard computing techniques take quite a long time to run code-breaking calculations, reducing the probability of a breach to near zero. It simply takes too long to try enough possibilities to determine the encryption key.

THROUGH THE ODDITIES OF QUANTUM THEORY, QUBITS CAN BE 0 OR 1 AT THE SAME TIME BECAUSE OF SUPERPOSITION.

That's where quantum computing comes in. Quantum computers, in theory, can use certain quantum effects to perform calculations much faster through the use of qubits, or quantum bits. Through the oddities of quantum theory, qubits can be 0 or 1 at the same time because of superposition. This is in contrast to standard computers using regular bits, which can only be 0 or 1. Using qubits means quantum computers can evaluate a staggeringly high number of encryption key combinations simultaneously, making them incredibly efficient and fast at breaking keys generated by today's standards.

While it seems quantum computing will effectively bring an end to secure data, quantum theories bring more to the table. Some quantum properties dictate that data values are simultaneously all possible values until they are measured. The famous thought experiment of Schrödinger's Cat, popularized by "The Tangerine Factor" episode of The Big Bang Theory, illustrates the notion.

Assume a cat is placed in a box with a possible radioactive quantum event that would trigger a poisoning mechanism to kill the cat. The idea is that the cat can be thought of as both alive and dead simultaneously until the box is opened (i.e., the measuring event), which then defines the cat's state. The same superposition idea allows quantum key distribution (QKD) to work. Simply stated, if two parties have established encrypted quantum-based communications, anyone eavesdropping to try to discover the data or the key will have to measure the data, thus changing it. The unwanted and ill-timed measurement will alert the receiver of an attempted breach, ensuring security through awareness.

Given that quantum computers can theoretically hack through encryption codes generated by today's standard routines, new routines will be required. Those encryption routines will need to be complicated enough to render the computing power of the quantum computer useless. Several new candidates, all viable, have been proposed, and all of them involve ridiculously complicated algorithms. Options include everything from purposely corrupting data, making it unreadable, to finding the nearest points in space to other points in space. Agreeing on a standard will likely take time; no recognized leader or quantum standards organization yet exists.

A few startup companies have cropped up to turn this apparent science fiction into reality, and a few large technology corporations, such as Toshiba, have created research divisions around quantum security. Swiss company ID Quantique has even implemented a short-hop private network in Ohio, secured by quantum key distribution, for the science/technology firm Battelle.

Universities and governments support the remainder of the research. Thanks to Edward Snowden and WikiLeaks, we learned that the National Security Agency is spending significant money to be at the forefront of the quantum computing revolution. However, there is one sure-fire indicator that quantum computing has truly become mainstream: When The Big Bang Theory dedicates an episode to QKD, we'll know we are late to the party.

FLEMING FREE
fleming.free@jabian.com

Fleming is a Director with expertise in program and project management, architectural solutioning, and business data and metrics.