# Wax Tablets to Quantum Mechanics

## UT Physics and 21st Century Cryptography

September 14, 2015

**Read the UT Press Release (http://tntoday.utk.edu/2015/10/13/physicists-developing-solutions-digital-information-safe-sea/)**

*For thousands of years, kings, queens and generals have relied on efficient communication in order to govern their countries and command their armies. At the same time, they have all been aware of the consequences of their messages falling into the wrong hands, revealing precious secrets to rival nations and betraying vital information to opposing forces. It was the threat of enemy interception that motivated the development of codes and ciphers: techniques for disguising a message so that only the intended recipient can read it.*

*—From The Code Book, by Simon Singh*

In the 5th Century an exiled citizen named Demaratus covered wooden tablets with wax to hide a message warning the Greeks of a Persian attack. In the 1500s Mary Queen of Scots sent ciphered messages to co-conspirators in a plot to dispatch the Queen of England. People have long looked for ways to guard information, especially with the advent of the digital age where bits and bytes carry data about national security and personal bank accounts. And as long as information has been protected, people have been trying to crack the codes concealing it. Three UT physicists: Associate Professor Bing Qi, Assistant Professor Raphael Pooser (both UT-ORNL Joint Faculty), and Professor George Siopsis are drawing on their expertise in quantum information to be part of that tradition as it unfolds in the 21st Century. Working with colleagues Professor Hoi-Kwong Lo (University of Toronto) and Assistant Professor Eric Chitambar (Southern Illinois University), they've won a $1.1 million award from the Office of Naval Research to keep information safe on the seas.

## Alice, Bob, and Eve

Coding a message has historically involved a sender encrypting information and the receiver translating the message by using a shared key—a string of secret bits. Qi delved into this world of code making and breaking in 2003. He explained that "the security of today's cryptographic system is largely dependent on the secrecy of the keys. The 'key' refers to a long train of random numbers shared between two authenticated users (conventionally named 'Alice' and 'Bob'). Alice can use her copy of the key to encrypt her message and send the generated ciphertext to Bob through an insecure communication channel. Once Bob receives the ciphertext, he can use his copy of the same key to decode Alice's original message."

While an eavesdropper (Eve) may intercept the message, the information is useless without the key, and the longer the key (and the more often it's refreshed), the stronger the security. In what's called a "one-time-pad" scheme, the key can be as long as the message it protects, and is used only once. For this method to work, Qi said, "Alice and Bob need a key distribution scheme to generate new keys. So far, the only key distribution scheme with proven security is QKD."

QKD (or quantum key distribution) has been around for a couple of decades. It's a little bit like Snapchat —there is no transcript of the quantum transmission once it's completed, so Eve can't simply hold on to an unreadable message and wait for better technology to come along and crack the code. And if Eve attempts to intercept a message by wiretapping into the channel, she'll automatically introduce "noise"

and give herself away, so Alice and Bob can simply drop all the data and start over. Qi noted that because "all the data transmitted in the QKD process are just random numbers, Eve won't gain any useful information."

Qi was introduced to QKD while working at the University of Toronto with Lo, whom he described as a "world-leading expert in quantum information science." Together with Siopsis, Pooser, and Chitambar, their plan is to build on the strengths of QKD to develop a multi-faceted and flexible network for the demands of the maritime environment.

## Security through Quantum Physics

While QKD works well over long-distance fibers and free space links, the vastness and turbulence of the high seas present their own challenges. The communication channels have a higher loss. Strong ambient light requires a sophisticated filtering scheme to selectively detect signal photons, and the mobility of the platforms (e.g., ships) requires the communication network to be highly reconfigurable. Eve may also derail key distribution by making the network unavailable, or try to hijack the message as it's encoded by Alice or decoded by Bob. To mitigate these obstacles the research team proposed a design with multiple options for transmitting data securely, including measurement-device-independent quantum key distribution (MDI-QKD).

It sounds obvious that in order to generate a secure key, the QKD protocol should be carried out properly. But how can Alice and Bob assure this in practice? Recent quantum hacking studies suggest that in conventional QKD, the security can be compromised due to imperfections in implementation, especially those associated with the measurement device (which has been regarded as an Achilles' heel for QKD). Fortunately, in MDI-QKD, Qi explained that the physics means the measurement device need not be trustworthy to be secure.

"The protocol explores one of the strangest features of quantum physics—entanglement," he said. "Roughly speaking, if two photons are in a maximally entangled state, their global property can be well defined and precisely determined, while the property of each (individual) photon is undefined (or loosely speaking, doesn't exist). So, the only thing Eve can determine faithfully is the correlation between Alice's and Bob's photon. That's why in MDI-QKD, we don't need to trust the measurement device. If Eve does follow the protocol, she gains no information of the key; if she doesn't follow the protocol, she will destroy the expected entanglement and can always be detected by Alice and Bob."

This device-independent option fits nicely into the kind of flexible, multi-user network required in a maritime environment. MDI-QKD offers high security in a untrusted scenario, whereas the more standard QKD protocol offers greater efficiency where any third parties involved are trusted and are privy to the secure key. The system can also be operated in a classical communication mode, where Bob and Alice deliver insensitive messages via strong light pulses.

"By allowing the system to be operated at different modes, we hope the proposed solution can be easily adapted to different applications," Qi said.

A position-based element allows a party (e.g., a ship) to use its geographical coordinates as the sole credential to establish an authenticated channel—an especially useful approach in ship-to-ship quantum key distribution.

The three-year grant begins in January 2016 with a potential second phase lasting two years.

Qi, who completed a Ph.D. in experimental optics in 1996, recognizes how far cryptography has come since the days of Demaratus and how physics research and applications continually evolve to meet society's needs.

"It's amazing to me that by exploring the quantum nature of light, we can achieve mission impossible in classical physics," he said, "even with practical devices we use in an optical lab every day."