Fighting tomorrow's hackers

February 5 2009

One of the themes of Dan Brown's The Da Vinci Code is the need to keep vital and sensitive information secure. Today, we take it for granted that most of our information is safe because it's encrypted. Every time we use a credit card, transfer money from our checking accounts -- or even chat on a cell phone -- our personal information is protected by a cryptographic system.

But the development of quantum computers threatens to shatter the security of current cryptographic systems used by businesses and banks around the world.

"We need to develop a new encryption system now, before our current systems -- such as RSA --becomes instantly obsolete with the advent of the first quantum computer," says Prof. Oded Regev at Tel Aviv University's Blavatnik School of Computer Science. To accomplish that, Prof. Regev has proposed the first safe and efficient system believed to be secure against the massive computational power of quantum computers and backed by a mathematical proof of security.

Secure for Centuries

Prof. Regev stresses it is imperative that a new cryptographic system be developed and implemented as soon as possible. One reason is that current information, encrypted with RSA, could be retroactively hacked in the future, once quantum computers are available. That means that bank and other financial information, medical records, and even digital signatures could instantly become visible.

"You don't want this information to remain secure for just 5 or 10 years until quantum computers are built," says Prof. Regev. "You want it to be safe for the next century. We need to develop alternatives to RSA now, before it's too late."

A New Cryptographic System

Cryptographic systems are used to transmit secure information such as bank and online transactions, and typically rely on the assumption that the factoring problem is difficult to solve. As a simplified example, if the number 3088433 were transmitted, an eavesdropper wouldn't be able to tell that the number is derived from the factors 1583 and 1951. "Quantum computers can 'magically' break all of these factoring-based cryptographic systems, something that would take billions of years for current computers to accomplish," Prof. Regev explains.

The current gold standard in encryption is the universally used RSA cryptosystem, which will be instantly broken once quantum computers are a reality -- an event predicted to happen as early as the next decade. To replace RSA in this new reality, Prof. Regev combined ideas from quantum computation with the research of other leaders in the field to create a system that is efficient enough to be practical for real-world applications.

Prof. Regev's work was first announced in the ACM Symposium on Theory of Computing and will appear in the *Journal of the Association for Computing Machinery*. His work has now become the foundation for several other cryptographic systems developed by researchers from Stanford Research Institute, Stanford University, and MIT. Its potential real-world applications are extensive, ranging from banking transactions to eBay and other online auctions to digital signatures that can remain secure for centuries.

Source: American Friends of Tel Aviv University