A police woman fights quantum hacking and cracking

July 30 2009

This is Dr. Julia Kempe of Tel Aviv University's Blavatnik School of Computer Science. Credit: AFTAU

The first desktop computers changed the way we managed data forever. Three decades after their introduction, we rely on them to manage our time, social life and finances -- and to keep this information safe from prying eyes and online predators.

So far, so good, despite an occasional breach. But our security and our data could be compromised overnight when the first quantum computer is built, says Dr. Julia Kempe of Tel Aviv University's Blavatnik School of Computer Science. These new computers, still in the theoretical stage, will be many times more powerful than the computers that protect our data now.

Laying the groundwork to keep governments, companies and individuals safe, Dr. Kempe is working to understand the power of quantum computers by designing algorithms that fit them. At the same time, she is figuring out the limits of quantum computers, something especially important so we can build safety systems against quantum hackers.

"If a very rich person worked secretly to fund the building of a quantum computer, there is no reason in principle that it couldn't be used for malevolent power within the next decade," she says. "Governments, large corporations, entrepreneurs and common everyday people will have no ability to protect themselves. So we have to plan ahead."

What quanta can't do

"If we know what quantum computers will not be able to do, we can find 'windows' of protection for data," says Dr. Kempe, who is working on future programs that could keep data in quantum computers safe. Dr. Kempe recently published papers in *Computational Complexity*, the SIAM Journal on Computing and Communications in Mathematical Physics.

Quantum mechanics allows a computer built on these principles, a so-called quantum computer, to perform tasks that are currently thought impossible to do efficiently on a normal computer, such as breaking current encryption standards.

Adding it all up

Although the most powerful quantum computer today barely has the computational capacity of a 4-bit calculator, it's just a matter of time until they are as powerful as physicists and mathematicians suspect they can be, Dr. Kempe says.

Today's computer operates by manipulating 0s and 1s — that is, a piece of data can be in one state or the other, but cannot be in both states simultaneously. In quantum computing, however, photons can be in the states 0 and 1 at the same time. This will give people and institutions phenomenally more computing power, but at the same time leave their data held in binary computers vulnerable to attack.

"Today if you use a credit card it's encrypted. No matter who intercepts the data it would take forever to decode the numbers -- even if all the computers we have today were wired together for the job," Dr. Kempe explains. A quantum computer, however, could crack the code quickly and efficiently.

"My basic research helps us better plan for the future when quantum computing is a reality," says Dr. Kempe, one of 23 new handpicked faculty recruits to Tel Aviv University.

Source: Tel Aviv University (news : web)

Citation: A police woman fights quantum hacking and cracking (2009, July 30) retrieved 17 April 2024 from https://phys.org/news/2009-07-police-woman-quantum-hacking.html