Scientific advance leads to a new tool in the fight against hackers

April 28 2022

Using the laws of quantum physics, the researchers developed a new security protocol that uses a person's geographical location to guarantee that they are communicating with the right person. Position-based quantum encryption, as it is called, can be used to ensure that a person is speaking with an actual bank representative when the bank calls and asks a customer to make changes to their account. This is an artistic representation of the security protocol. Credit: Alex Bols, University of Copenhagen, The Quantum for Life Centre.

A new form of security identification could soon see the light of day and help us protect our data from hackers and cybercriminals. Quantum mathematicians at the University of Copenhagen have solved a mathematical riddle that allows for a person's geographical location to be used as a personal ID that is secure against even the most advanced cyber attacks.

People have used codes and encryption to protect information from falling into the wrong hands for thousands of years. Today, encryption is widely used to protect our digital activity from hackers and cybercriminals who assume false identities and exploit the internet and our increasing number of digital devices to steal from us.

As such, there is an ever-growing need for new security measures to detect hackers posing as our banks or other trusted institutions. Within this realm, researchers from the University of Copenhagen's Department of Mathematical Sciences have just made a giant leap.

"There is a constant battle in cryptography between those who want to protect information and those seeking to crack it. New security keys are being developed and later broken and so the cycle continues. Until, that is, a completely different type of key has been found," says Professor Matthias Christandl.

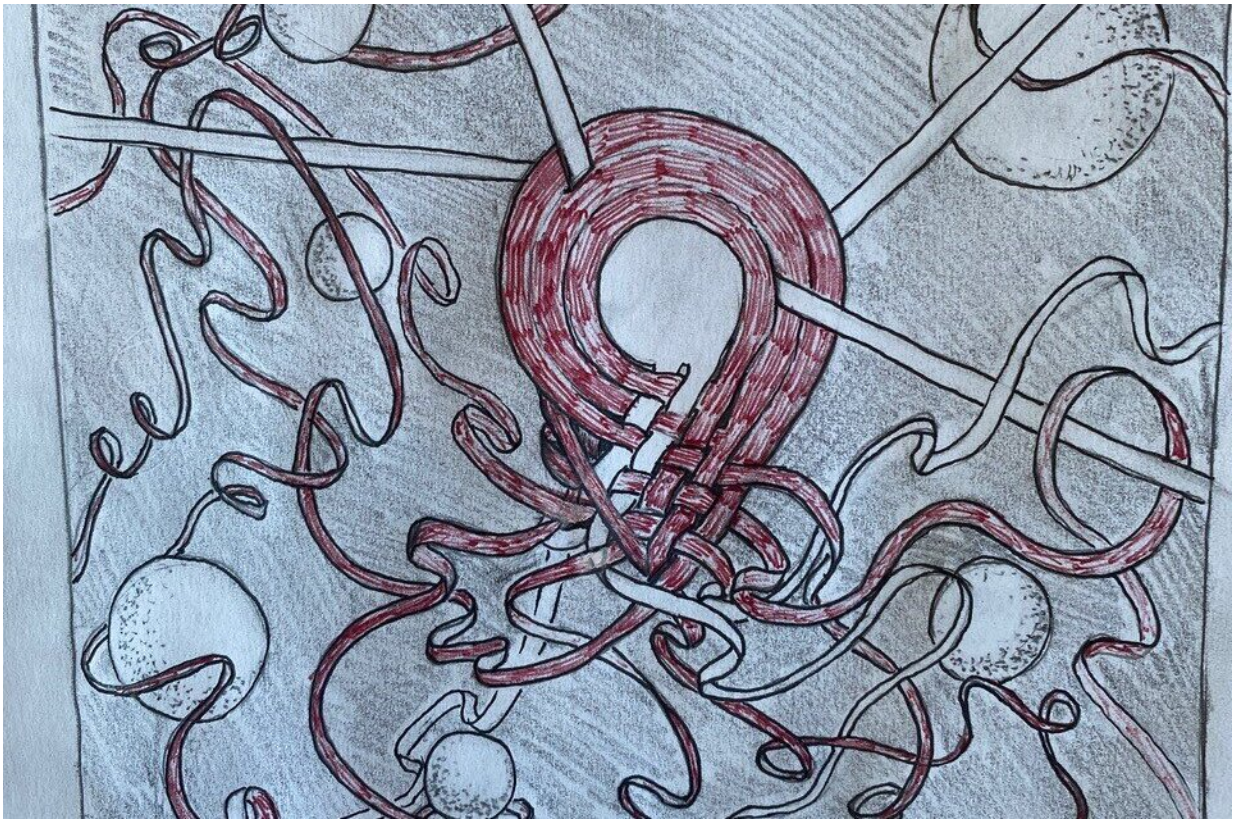
For nearly twenty years, researchers around the world have been trying to solve the riddle of how to securely determine a person's geographical location and use it as a secure ID. Until now, this had not been possible by way of normal methods like GPS tracking.

"Today, there are no traditional ways, whether by internet or radio signals for example, to determine where another person is situated geographically with one hundred percent accuracy. Current methods are not unbreakable, and hackers can impersonate someone you trust even

when they are far far away. However, quantum physics opens up a few entirely different possibilities," says Matthias Christandl.

Quantum physics makes hacking impossible

Using the laws of quantum physics, the researchers developed a new security protocol that uses a person's geographical location to guarantee that they are communicating with the right person. Position-based quantum encryption, as it is called, can be used to ensure that a person is speaking with an actual bank representative when the bank calls and asks a customer to make changes to their account.



Using the laws of quantum physics, the researchers developed a new security protocol that uses a person's geographical location to guarantee that they are

communicating with the right person. Position-based quantum encryption, as it is called, can be used to ensure that a person is speaking with an actual bank representative when the bank calls and asks a customer to make changes to their account. Credit: Alex Bols , University of Copenhagen, The Quantum For Life Centre

"Ask yourself, why do I trust an employee at the bank counter? Because they're in a bank. Their location creates trust. This explains the principle behind position-based cryptography, where physical location is used to identify oneself," explains postdoc Andreas Bluhm.

The researchers' recipe for securing a person's location combines the information in a single quantum bit—a qubit—followed by classical bits, consisting of the ones and zeroes that we are familiar with from ordinary computers.

Both types of bits are needed to send a message that is impossible for cybercriminals to read, hack or manipulate, and which can confirm whether a person is in your bank's office or in some far-off country.

The quantum bit serves as a kind of lock on the message, due to the role of Heisenberg's Uncertainty Principle in quantum physics, which causes quantum information to be disrupted and impossible to decode when trying to measure it. It is also due to what is known as the "no-cloning theorem," which makes quantum information impossible to intercept and secretly copy. This will remain the case for quite some time.

"Until a full-fledged quantum computer is built and hackers gain access to one, our method is completely secure and impossible to hack," says Andreas Bluhm.

Could soon be a reality

The researchers highlight the fact that the new method is particularly handy because only a single quantum bit is needed for position verification. So, unlike many other quantum technologies that require further development, this new discovery can be put to use today. Suitable quantum sources that can send a quantum bit of light already exist.

"The particular strength of our technique is that it is relatively straightforward to implement. We're already able to send individual quantum bits, which is all this technique requires," says Matthias Christandl.

The security ID needs to be developed commercially, by a company for example, before it can be widely adopted. However, its quantum foundation is in place.

The new research result is particularly useful in contexts where communications between two parties need to be extremely secure. This could be payments on the internet or transmission of sensitive personal data.

"Secure communication is a key element of our daily lives. Whenever we communicate with public authorities, our banks or any party that manages our personal data and information, we need to know that the people we're dealing with are those who we expect them to be—and not criminals," says Andreas Bluhm.

The research has just been published in *Nature Physics* and was presented at the QCrypt 2021 conference.

More information: Andreas Bluhm, A single-qubit position verification protocol that is secure against multi-qubit attacks, *Nature*

Physics (2022). DOI: 10.1038/s41567-022-01577-0