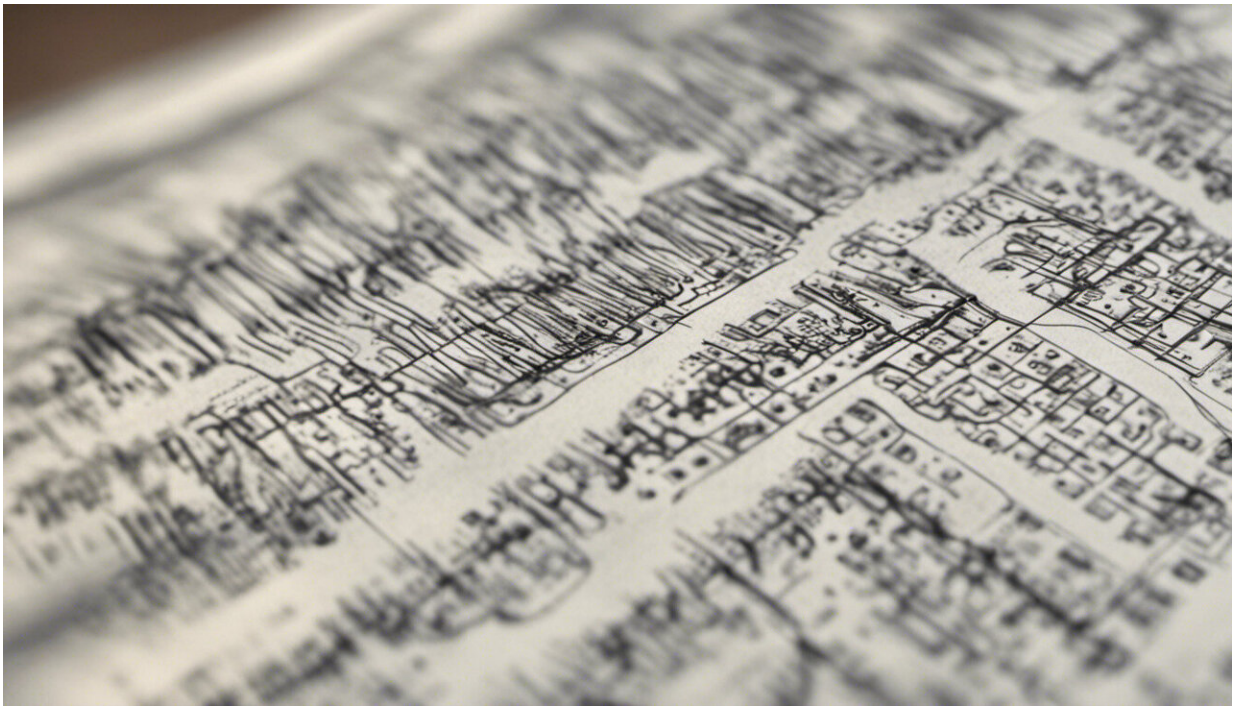
How to counterfeit quantum money

March 17 2017



Credit: AI-generated image (disclaimer)

A Polish/Czech research team has demonstrated how even a seemingly ultrasecure form of money, designed using quantum mechanics can have a potentially important security loophole putting it at risk of forgery. But this highlights not the shortcomings of this exciting new technology, but rather its continuing potential to transform human society in the 21st century.

Quantum technologies are without a doubt currently in vogue in the scientific and technological communities. As the theory becomes reality, these exciting technologies promise to transform our societies over the coming decades.

The technology of tomorrow

As noted in this week's edition of *The Economist*: 'A bathing cap that can watch individual neurons, allowing others to monitor the wearer's mind. A sensor that can spot hidden nuclear submarines. A computer that can discover new drugs, revolutionise securities trading and design new materials. A global network of communication links whose security is underwritten by unbreakable physical laws. Such - and more - is the promise of quantum technology.'

The EU has also jumped on the quantum bandwagon, with funding of around EUR 550 million through Horizon 2020 to ensure that Europe maintains its role as one of the global powerhouses for quantum research (for more on the EU's efforts in this field, see the CORDIS Results Pack on quantum technologies.

Moreover, as with all developing technologies, scientists will not only have to push forward what works but also find solutions to existing weaknesses. A Polish and Czech team of scientists have done exactly this through developing what should be – in theory – ultrasecure 'quantum money' but then immediately found a serious flaw leaving it at risk of forgery. The research has been published in the journal 'npj Quantum Information'.

Forging the unforgeable

Under ideal conditions, quantum currency is impossible to counterfeit.

But thanks to the messiness of reality, a forger with access to sophisticated equipment could skirt that quantum security if banks don't take appropriate precautions. The concept of quantum money has been around since the 1970s, first proposed by then-Columbia University grad student Stephen Wiesner, but this is the first time anyone has created and counterfeited quantum cash.

Instead of paper or plastic banknotes, the research team's quantum bills were minted in light. To transfer funds, a series of photons would be transmitted to a bank using the photons' polarisations, the orientation of their electromagnetic waves, to encode information.

To illustrate their technique in a fun way, the researchers transmitted a pixelated picture of a banknote—an old pre-euro Austrian schilling bill – using photons' polarisations to stand for grayscale shades. In a real quantum money system, each bill would be different and the photon polarisations would be distributed randomly, rather than forming a picture. The polarisations would create a serial number–like code the bank could check to verify that the funds are legitimate.

Crucially, a criminal intercepting the photons couldn't copy them accurately because quantum information can't be perfectly duplicated. 'This is actually the cornerstone of security of quantum money,' says Karel Lemr, study co-author from the Palacký University Olomouc in the Czech Republic.

However, the system would not be as secure as it first appears. Because single photons are easily lost or garbled during transmission, banks would have to accept partial quantum bills, analogous to a paper banknote with a corner torn off. This gives an opportunity for criminals to make forgeries that aren't perfect, but are arguably good enough to be verified by the bank.

Lemr and his colleagues used an optimal cloner, a device that comes as close as possible to copying quantum information (the technology to instigate a real money system based on quantum technologies does not physically exist yet), to attempt a forgery. The team showed that a bank would accept a forged bill if the standard for accuracy wasn't high enough—more than about 84 % of the received photons' polarisations must match the original.

Previously, this vulnerability 'wasn't explicitly pointed out, but it's not surprising,' says theoretical computer scientist Thomas Vidick of Caltech, who was not involved in the research. The result, he says, indicates that banks must be stringent enough in their standards to prove the bills they receive are real.

So whilst this experiment highlights not only the great potential of quantum technologies, it also exposes significant security challenges that still need to be overcome. This isn't just confined to the concept of quantum money, but also many of the other revolutionary products the human harnessing of quantum mechanics promises.

However, as 'The Economist' summarises, the remaining challenges are mostly engineering ones, rather than scientific, and what is most exciting about quantum technology is its as yet untapped potential.

Provided by CORDIS