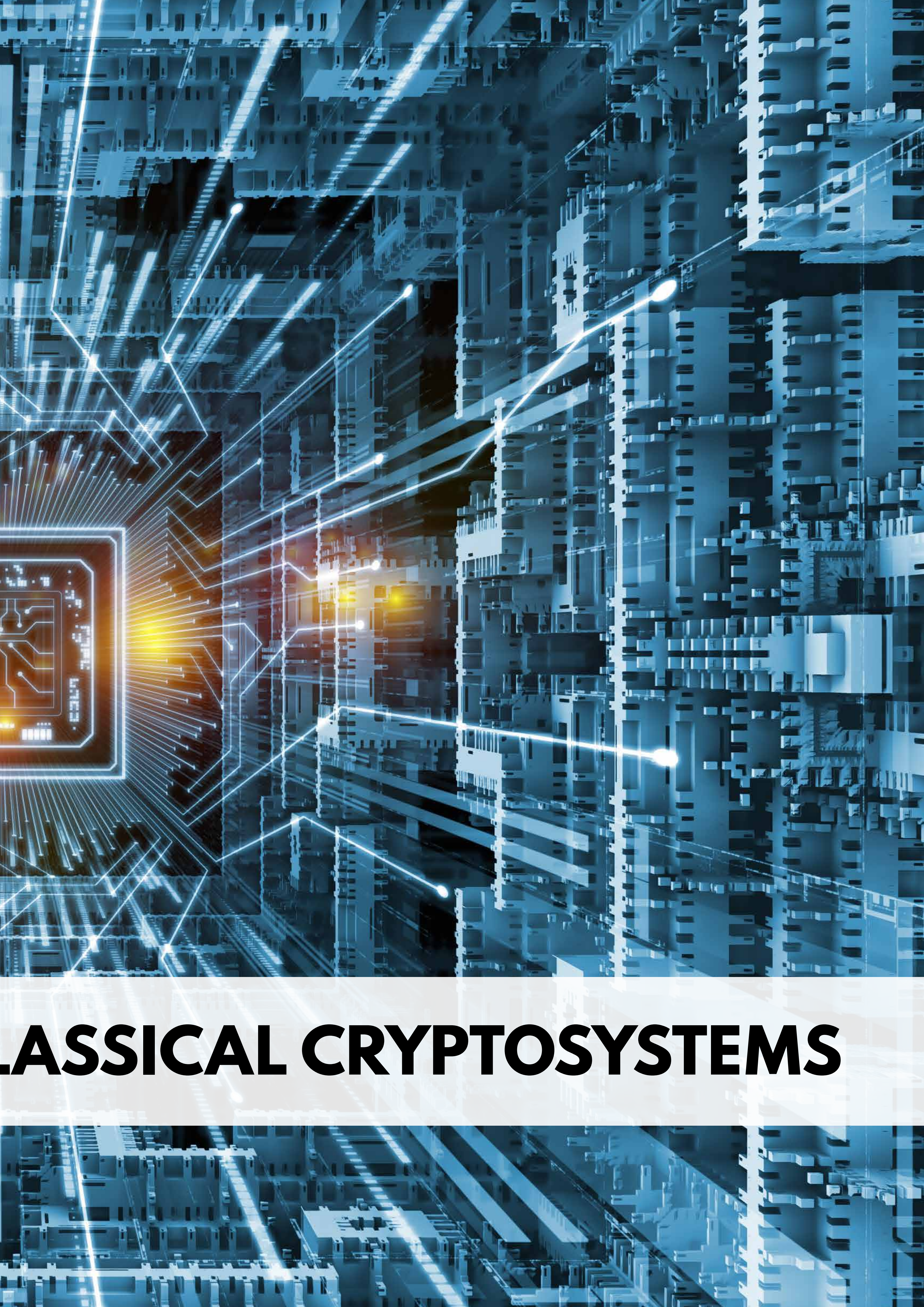
QUANTUM ATTACKS ON CL

Graphic: Andrew Ostrovsky



LASSICAL CRYPTOSYSTEMS

It started as a thought experiment in 1970, when physicist Stephen Wiesner came up with the idea of replacing classical banknote security features with quantum ones. However, the novel idea had to be put on the back burner for a few decades before it could be experimentally tested.

Instead of having unique serial numbers printed on the banknotes and visible to the naked eye, S. Wiesner wanted to use the properties of elementary particles, such as polarisation and spin, for quantum money. Then, it would only be possible to read the printed code with a suitably constructed apparatus. Such money would also be impossible to counterfeit. However, this elegant solution was beyond the capabilities of the technology available at that time.

Nevertheless, the experiments undertaken back then offered some hope that the idea could be put into practice. In the 1980s, the use of single qubits in quantum cryptography was considered (in quantum computing, a qubit is equivalent to a bit in classical computing; unlike a bit, which only takes the value of 1 or 0, a qubit can be in a superposition of two quantum states, which are, in simple terms, 1 and 0 at the same time), and in 1991 Polish scientist Artur Ekert proposed using their entangled states for this purpose. The experiments carried out four years later by a team including Anton Zeilinger – a world authority on quantum information – proved that indeed it could be done. However, before we move on to cryptography, we need to take a closer look at quantum computers themselves.

THE POWER OF QUANTUM COMPUTER

Hardly a day goes by without us coming across a flashy headline while browsing through various websites, proclaiming: *Groundbreaking development in quantum computing!* When asked how much truth there is in the hype generated by the media, Prof. Jerzy Dajka, a physicist from the University of Silesia, replies:

‘We are still a long way from achieving something practical. We are not very good at dealing with decoherence, i.e. the loss of information due to the system’s interaction with the environment. We still don’t have enough cubits. The experiments that we are aware of seem to prove that the quantum advantage has been established for some relatively simple issues. However, the size issue remains. We are indeed able to do some simple things with a qubit faster than with bits, but if there is an issue requiring us to encode something with tens of thousands of classical bits, we don’t yet have enough qubits to contend with that. We are still at a preliminary and more of a theoretical stage when it comes to quantum computing’.

At the moment, the American companies IBM (Quantum) and Google (Quantum AI), as well as Canada’s D-Wave Systems, can boast having quantum computers under constant development. However, it should be noted that the last of these three companies specialises in a certain class of algorithms, capable of solving a rather narrow range of problems.

‘Although D-Wave seems to be the most advanced in terms of technology, it paradoxically poses the least threat to classical cryptography’, asserts the scientist. – And what exactly is this threat about?

UNCOVERING INFORMATION

Let us recall the previously mentioned idea of quantum money by S. Wiesner. After all, we use all sorts of codes and encryptions to protect our data in many different areas. Be it a bank account, a patient’s profile in healthcare information systems, or military or economic secrets – everywhere the security of information is ensured by various types of algorithms used in classical cryptography. We are frequently not sure whether such codes or encryptions cannot be broken. What we do know is that we cannot do it within a period of time shorter than the lifetime of the Universe. Unless someone trying to break through such an algorithm uses a quantum computer.

‘Such a person would be able to break the encryption instantly. The world would become unilaterally transparent, that is, a person with a quantum computer would be able to see all the data encrypted by classical methods, but the other side would not be able to access the data secured by quantum cryptosystems’, explains Prof. Jerzy Dajka.

Weronika Cygan

Prof. Jerzy Dajka
Institute of Physics
Faculty of Science and Technology
University of Silesia
jerzy.dajka@us.edu.pl

A glance at Ukraine ravaged by war is all it takes to realise the huge importance of information. After invading their neighbour, among the first things that Russians destroyed was communications infrastructure, to prevent the enemy from communicating, but also to cut them off from news from the front and stop them from sending their own messages to the outside world.

'The presence of Elon Musk's Starlink in Ukraine is a non-trivial factor. By making his communications satellite system available to the invaded country, the visionary businessman has ensured that Ukraine's military and administration is no longer in any way dependent on Russian interventions for communication', explains the physicist.

It is thus not hard to guess that the first country to develop a quantum computer capable of performing such calculations would have a dangerous weapon at its disposal. This would entail global domination, comparable only to what occurred after the Americans developed the atomic bomb. It lasted until the bomb showed up also on the other side of the Iron Curtain.

POST-QUANTUM ARMOUR

Such a scenario sounds rather threatening, but we already have effective protection against quantum attacks on classical cryptosystems, which does not require a quantum computer!

Post-quantum protocols, which is what we are talking about here, are based on classical infrastructure and have been recommended by the US National Security Agency (NSA) since 2015 as a way of combating potential attacks launched with quantum computers. Such solutions are, in fact, already in use (e.g. for 'mining' bitcoin), and they are highly effective.

In classical cryptography, a certain group of algorithms is based on the factorisation of numbers, i.e. decomposing them into prime factors – even if we know that a number is the product of two prime numbers, we cannot easily identify them in the case of sufficiently large numbers. The established approaches tend to be akin to the trial-and-error method. However, given a sufficiently large number of approaches, we will eventually find the correct answer. In complex cases, it could take millions or billions of years to find the right solution using the classical method. A quantum computer can solve a similar problem in the blink of an eye, so another security measure had to be found. Currently, one quantum algorithm (and its modifications) is recognised as a threat to classical cryptosystems: the Shor algorithm, designed to factorise numbers. Using a classical cryptosystem that does not rely on number factorisation will therefore make it possible to push back the problem into the future, if not solve it altogether. And this is the role of post-quantum cryptography, at least until another algorithm emerges.

HARNESSING THE LAWS OF NATURE

There are also some ideas on how to get around the threat posed by quantum computers. One option is to send a secret key for encryption and decryption using quantum methods and quantum communication channels. We already have considerable achievements in this area; the method itself works brilliantly and is extremely secure.

It seems to have an advantage over the classical method for two particular reasons, both of which draw on fundamental laws of nature. The first is the quantum system issue, which always changes when a measurement is made. This means that with the right tools we would be able to detect someone tampering with the information. The second is that quantum information cannot be copied.

While many publicists are keen on fearmongering with quantum computers as a challenge to data security, we are by no means helpless in the face of this threat. Mathematicians and computer scientists continue to improve the currently used classical cryptosystems, while physicists are working on new quantum solutions. Thus, we should look at quantum computers the way we look at our smartphones or laptops – they are simply tools that can be used for various purposes, both good and bad.