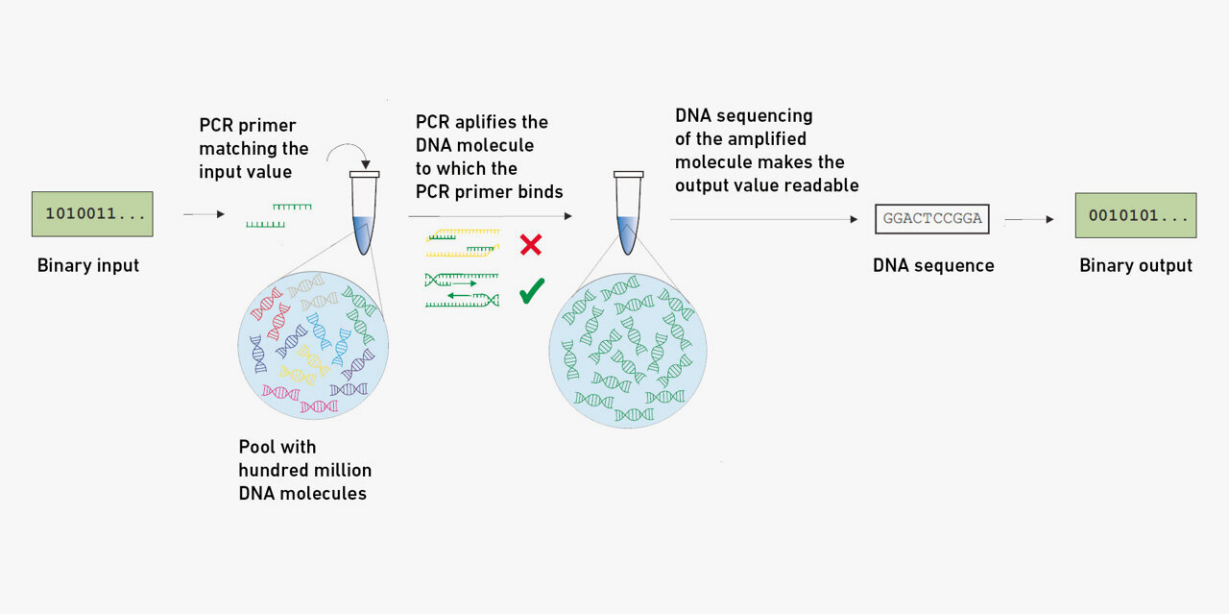
Protecting art and passwords with biochemistry

April 8 2024, by Fabio Bergamin



The language of the DNA world uses the letters A, T, C and G. With suitable rules, however, this can easily be translated into a digital sequence of 0s and 1s. Credit: ETH Zurich

Security experts fear Q-Day, the day when quantum computers become so powerful that they can crack today's passwords. Some experts estimate that this day will come within the next ten years. Password checks are based on cryptographic one-way functions, which calculate an output value from an input value. This makes it possible to check the

validity of a password without transmitting the password itself: the one-way function converts the password into an output value that can then be used to check its validity in, say, online banking.

What makes one-way functions special is that it's impossible to use their output value to deduce the input value—in other words, the password. At least not with today's resources. However, future quantum computers could make this kind of inverse calculation easier.

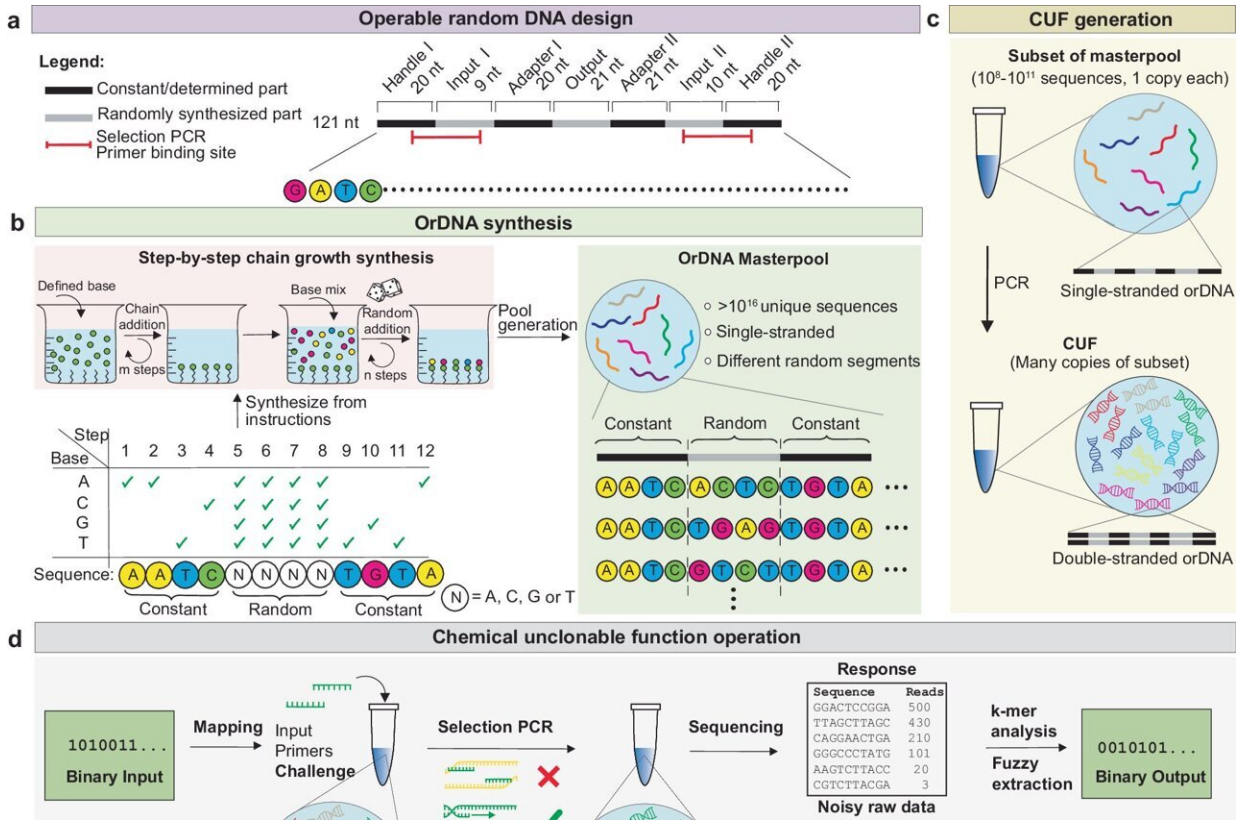
Researchers at ETH Zurich have now presented a cryptographic one-way function that works differently from today's and will also be secure in the future. Rather than processing the data using arithmetic operations, it is stored as a sequence of nucleotides—the chemical building blocks of DNA.

Based on true randomness

"Our system is based on true randomness. The input and output values are physically linked, and it's only possible to get from the input value to the output value, not the other way round," explains Robert Grass, a professor in the Department of Chemistry and Applied Biosciences.

"Since it's a physical system and not a digital one, it can't be decoded by an algorithm, not even by one that runs on a quantum computer," adds Anne Lüscher, a doctoral student in Grass's group. She is the lead author of the paper, which was published in the journal *Nature Communications*.

The researchers' new system can serve as a counterfeit-proof way of certifying the authenticity of valuable objects such as works of art. The technology could also be used to trace raw materials and industrial products.



Design and working principle of DNA-based chemical unclonable functions. Credit: Luescher et al. 2024

How it works

The new biochemical one-way function is based on a pool of one hundred million different DNA molecules. Each of the molecules contains two segments featuring a random sequence of nucleotides: one segment for the input value and one for the output value. There are several hundred identical copies of each of these DNA molecules in the pool, and the pool can also be divided into several pools; these are identical because they contain the same random DNA molecules. The pools can be located in different places, or they can be built into objects.

Anyone in possession of this DNA pool holds the security system's lock. The polymerase chain reaction (PCR) can be used to test a key, or input value, which takes the form of a short sequence of nucleotides. During the PCR, this key searches the pool of hundreds of millions of DNA molecules for the molecule with the matching input value, and the PCR then amplifies the output value located on the same molecule. DNA sequencing is used to make the output value readable.

At first glance, the principle seems complicated. "However, producing DNA molecules with built-in randomness is cheap and easy," Grass says. The production costs for a DNA pool that can be divided up in this way are less than 1 Swiss franc. Using DNA sequencing to read out the output value is more time-consuming and expensive, but many biology laboratories already possess the necessary equipment.

Securing valuable goods and supply chains

ETH Zurich has applied for a patent on this new technology. The researchers now want to optimize and refine it to bring it to market. Because using the method calls for specialized laboratory infrastructure, the scientists think the most likely application for this form of password verification is currently for highly sensitive goods or for access to buildings with restricted access. This technology won't be an option for the broader public to check passwords until DNA sequencing in particular becomes easier.

A little more thought has already gone into the idea of using the technology for the forgery-proof certification of works of art. For instance, if there are ten copies of a picture, the artist can mark them all with the DNA pool—perhaps by mixing the DNA into the paint, spraying it onto the picture or applying it to a specific spot.

If several owners later wish to have the authenticity of these artworks

confirmed, they can get together, agree on a key (i.e. an input value) and carry out the DNA test. All the copies for which the test produces the same output value will have been proven genuine. The new technology could also be used to link crypto-assets such as NFTs, which exist only in the digital world, to an object and thus to the physical world.

Furthermore, it would support counterfeit-proof tracking along supply chains of industrial goods or raw materials. "The aviation industry, for example, has to be able to provide complete proof that it uses only original components. Our technology can guarantee traceability," Grass says. In addition, the method could be used to label the authenticity of original medicines or cosmetics.

More information: Anne M. Luescher et al, Chemical unclonable functions based on operable random DNA pools, *Nature Communications* (2024). DOI: 10.1038/s41467-024-47187-7

Provided by ETH Zurich