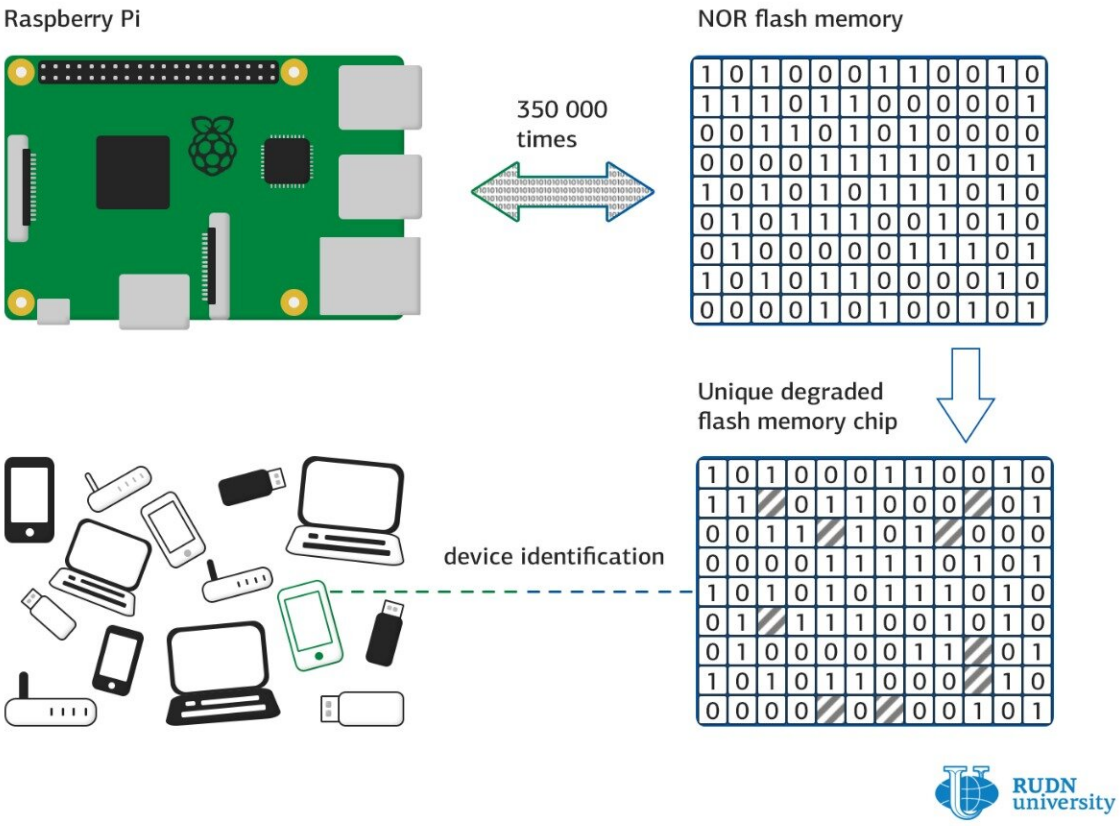
Mathematicians prove that flash-memory 'fingerprints' of electronic devices are truly unique

October 15 2019



Credit: RUDN University

Experts in applied mathematics at RUDN University have experimentally proven that it is possible to accurately identify electronic devices by defects in flash memory cells. It turns out that the distribution and nature of these defects are unique, and they can play the role of "fingerprints" for memory chips. The new method will improve protection against hacker attacks, as it would create electronic flash keys that cannot be faked. The results of the study are published in the journal *IEEE Access*.

As information and communication devices—smartphones, fitness bracelets, Wi-Fi equipment, memory devices—are spreading around the world, the issue of protecting them from theft and tampering becomes more and more relevant. A way to accurately identify each device is needed. Existing identification methods can be divided into two types: virtual and physical. Virtual methods are applied to the software (firmware) of a device. It could be, for example, a unique number that is "hard written" into the device. The problem is that any software can be hacked and data changed. Physical methods deal with hardware. These include the identification of a device by unique fluctuations of its radio frequency. However, radio signals are subject to interference.

One of the new methods of physical identification is based on damaged flash memory cells. Due to microscopic manufacturing defects, damaged cells randomly appear in the memory blocks of a device. The pattern of these microdefects is unique, and that means that one device can be distinguished by it from another. Previously, however, it has not been possible to numerically prove the effectiveness of this method, so the experts from RUDN University undertook to verify the effectiveness of this technology.

For that, they used flash memory chips of configuration NOR, which are used in microcontrollers and microchips for computers. NOR flash memory is a two-dimensional array of low-level memory cells located on

the matrix of the conductor. Each of the cells stores from one to four bits of information. To record or erase information in a cell, you need to change its charge. During the recording process, the cell changes the initial state of the bit (usually "1") to the opposite ("0"). But after each write cycle, irreversible changes accumulate in the cell, and at some point it stops working, that is, it no longer changes its state if writing is attempted. Such a cell is considered corrupted, and the process of the appearance of corrupted cells is called memory chip degradation.

The process of memory cells' "death" is completely random, so the picture of the distribution of non-functional cells within a particular memory sector will be unique for each device. If, before the gadget is sold, this pattern is added to a database, e.g. maintained by the manufacturer, it would become possible to identify the device unambiguously by this corrupted cells pattern. The manufacturer would be able to check a specific sector of memory, compare it with the database and block a stolen smartphone or take other measures.

The researchers from RUDN University decided to prove in practice that the damaged cells pattern is unique for each memory chip. They connected 120 NOR flash memory chips to a custom testbed utilizing Raspberry Pi computer. One of the 512 sectors on each chip was forcibly corrupted by rewriting it 350,000 times. As a result, a map of damaged cells of the first memory sector of each chip was obtained. The number of non-functional cells in the sector for most of the tested chips ranged from 30 to 100.

After that, the researchers compared all the maps of the "bad" cells and none of those matched any other. They also extrapolated the data to a very large number -quadrillions—of devices. Statistical calculations showed that the likelihood of two identical maps of damaged cells is infinitely small.

Of course, new unplanned damaged cells may appear while a chip is in use. But an experiment showed that the map almost does not change over the life of the device: the average number of write cycles before the appearance of a new "bad" cell is 3940. This corresponds to more than 10 years of daily use. However, there remains a possibility that one new damaged cell will make the device identical to another one that differs by just that very cell. RUDN University mathematics also calculated this probability, using a special formula. It turned out that even though such a possibility cannot be excluded completely, it is also infinitely small: about five millionths.

Using all this data, the experts successfully carried out the procedure of mutual identification between two devices: they successfully "recognized" each other.

Thus, the researchers proved both in practice and mathematically that damaged sectors of flash memory can be used as a unique identifier for quadrillions of microprocessors, smartphones, and other devices. This figure is significantly higher than the current number of devices in the world.

More information: Sergey S. Vladimirov et al. Unique Degradation of Flash Memory as an Identifier of ICT Device, *IEEE Access* (2019). DOI: 10.1109/ACCESS.2019.2932804

Provided by RUDN University