Department of Electrical and Information Technology, Lund University
Presented 2021-10-18
Masters Thesis Power analysis on FPGA implementation of Classic McEliece
Student Andreas Johansson
Supervisor Qian Guo
Examiner Thomas Johansson

Revealing encrypted information by monitoring power consumption

Popular science summary.

So, you came up with a strong password used when signing into government websites. Well, then you don't need to worry that anyone else can get access to your data, or should you worry? In this work, it is shown that strong passwords alone do not guarantee that personal data will be kept confidential.

More and more of our daily activities such as work, social interaction, and contact with authorizes are performed with an ever-increasing number of electronic devices around us all connected to the Internet. Often we transmit sensitive data, like bank account numbers, private messages over some social platform, or images from our home security camera over the Internet. Many people do not concern themselves about security when they transmit sensitive data over the Internet, and why should they? After all, they used a strong password to authorize themselves before sending any sensitive information over the Internet.

National authorities also handle a lot of information that needs to be kept confidential, both for keeping the integrity of citizens and for national safety. Authorities might be more aware of how to keep sensitive data secure while it sent over the Internet. But, both authorizes and ordinary people rely on that their sensitive data is encrypted before it is sent over the Internet. This is possible since serval cryptosystems have been developed throughout the years where a private key is used to encrypt sensitive data. In an ideal cryptosystem, only the holder of the private key should be able to retrieve the original data that was encrypted.

However, now and then some cryptosystems are reported as broken as someone has figured out how to get their hands on sensitive encrypted data without having access to the private key. Typically, cryptographic systems rely on that some mathematical problems that take a long time to solve without knowledge of the private key. When a cryptosystem is broken, someone has typically found a flaw in the used mathematical problem that allows them to solve the problem in a short time. And by solving the problem the encrypted data can be decrypted without access to the private key.

A big concern for many of today's cryptosystems is the increased research and development of quantum computers. If or when a sufficiently powerful quantum computer becomes a reality, many of the mathematical problems used in today's cryptosystems will be easily solved. This is a well-known fact in the research community, and in an attempt to fuel the development of new quantum computer resistant cryptosystems, the US agency National Institute of Standards and Technology launched a competition for finding new cryptosystems. Currently, the competition is in its last round and one of the finalists is called Classic McEliece.

Since Classic McEliece made it to the final there is a high hope that this cryptosystem is quantum computer resistant. However, as a cryptosystem is implemented on an electronic device another possible threat opens up. Since 1996 it has been known that by measuring the power consumption of an electronic device it is sometimes possible to retrieve the private key of a cryptosystem. Thereby, an attacker can bypass the tedious work of solving the underlying mathematical problem of the cryptosystem. Therefore, it is important to assess if potential future cryptosystems can be broken by observing the power consumption of the device where the cryptosystem is implemented.

Since Classic McEliece is a possible future standard cryptosystem there is an interest to evaluate this system in multiple ways. In this thesis, the power consumption of Classic McEliece was measured while decryptions were executed. It turned out that a straightforward implementation of Classic McEliece suffers from a lot of information leakage that potentially could be exploited by an attacker, even without a quantum computer.