Master's thesis internship proposal:

Horizontal Attacks Against ECC Blocks in Authentication Protocols For RFID.

Keywords: Elliptic Curve Cryptography (ECC), side-channel attacks, RFID.

RFID is becoming the reference technology for short distance wireless identification; some example uses are for building or room access, car entry systems and car immobilizers, and valuable items tracking. But securing RFID tags is still a challenge today. Because standard secure RFID cards on the market use symmetric cryptography, the secret key may be stolen, and in some cases like the Myfare Classic cards, it may be stolen just by listening to a legitimate communication.

This is why Elliptic Curve Cryptography (ECC) seems to be a good option since it alleviates the key distribution issues of symmetric cryptography, and is the best available tradeoff in asymmetric cryptography between performance and security.

But implementing secure authentication protocols with ECC for RFID is still a research-level challenge: the limited resources of RFID, and ensuring an implementation secure against side-channel attacks are two of the biggest challenges.

Most studies of side-channel attacks consider so-called vertical attacks, where several trace executions are collected and analyzed to recover a part of, or the whole of, the private key. These attacks, and couter-measures against them, are well-researched and well-documented in the research litterature. There are known countermeasures against those attacks, and they may be used in the context of an authentication protocol.

In contrast, so-called horizontal attacks, where only one execution trace is used for the attack, are less studied; and most countermeasures against vertical attacks are of no use against horizontal attacks.

The objective of this master's internship is to study, theoretically and practically, horizontal attacks on ECC blocks, as they could be used against an RFID tag executing an ECC-based authentication protocol.

Some typical tasks to be done will be:

- research in the litterature the known horizontal attacks and countermeasures against ECC blocks;
- reproduce at least one known horizontal attack;
- try to propose new horizontal attacks, and demonstrate their practical feasibility;
- analyze which horizontal attacks may be carried out in the context of ECC-based authentication protocols;
- propose new countermeasures against either old or new horizontal attacks.

This internship proposal will take place in the context of the research project RATECC, which stands for RFID Authentication Through ECC. It is a joint project with TIMA in Grenoble (Paolo Maistri) and LCIS in Valence (Vincent Beroulle, Yann Kieffer). It

is related to the work being done by a PhD student on using ECC for authentication in RFID, and another master's thesis in Grenoble on a related subjet.

An important part of the work will be carried out in english.

Who should apply:

Applicants must be enrolled in a Master's degree in computer engineering, embedded systems or cybersecurity.
An interest in hardware security and some knowledge of MATLAB will be a plus.

Internship context and conditions:

- Internship duration: 5 or 6 months (starting February 2020)
- Internship location: LCIS laboratory, Valence, France
- Financing: about 550€ per month

For further information, please contact:

Yann Kieffer: `yann.kieffer@lcis.grenoble-inp.fr`
Vinent Beroulle: `vincent.beroulle@lcis.grenoble-inp.fr`