Master project at NXP Semiconductors
White-box Cryptography

More and more functionality in electronic devices is being implemented in software instead of hardware. Software has the advantage of being less costly, better scalable, easier to personalize, and easier to update. This is also the case for mobile devices, such as smart phones and tablets. Given the increase of security-sensitive applications (e.g. payment) on these devices, a critical question is how to hide secret data and algorithms in software. The main challenge is that the platforms are connected and open. This implies that the most realistic attack model is the so-called white-box attack model: the attacker is assumed to have full access to and full control over the execution environment. A software implementation that is secure under this model is called a white-box implementation.

Mobile devices are increasingly being equipped with NXP's Near-Field Communication (NFC) technology. Recently, Android added Host-Card Emulation (HCE) in order to make NFC accessible to apps.
The end-result of this master project is to realize HCE-based app containing a white-box implementation. If time allows, one can next perform a security and performance analysis of this app.

Your profile:

- Computer science student
- Knowledge of security
- Good C-programming skills

The project will take six months, including the writing of a final thesis report. It will be carried out onsite at the High Tech Campus in Eindhoven, The Netherlands, due to the required high-intensity knowledge transfer and supervision, as well as the availability of specific software tools.

Working in this project at NXP Semiconductors in Eindhoven implies working in a stimulating, multidisciplinary environment at the forefront of technology, with knowledgeable colleagues, and an excellent infrastructure.

Contact information:
Wil Michiels
High Tech Campus 46
5656AE Eindhoven
NXP Semiconductors
Wil.michiels@nxp.com