Physical Security of Cryptographic Devices

Cryptography Group, Department of Computer Science, University of Bristol

Motivation

Physical attacks, such as power analysis, are techniques with which one can extract secret data from devices such as smart cards, mobile phones, RFIDs, etc.

Modern devices are hence manufactured with such attacks in mind: a wide and varying range of countermeasures have been deployed, each with their particular pros and cons. No countermeasure can provide protection against all threats, and the continuous development of new and improved attack techniques require constant re-evaluation of cryptographic devices.

Experimental Setup

A De-packaged Circuit Board

We have, in the past, contributed to the development of both attacks and countermeasures for various cryptographic primitives and different kinds of cryptographic devices. Our latest effort has been towards the further analysis of attack techniques that focus on the exploitation of several information leaks per acquired observation for a device.

Using such techniques we were able to completely break a popular and widely used countermeasure called masking: a technique in which an implementation is changed such that it never computes on 'raw' data, but only on data that is concealed by a random value. We showed that all implementations of this method that use pre-computations of table look-ups for efficiency are trivially breakable.

The development of implementations that are resistant to physical attacks is an ongoing process that requires the evaluation of new ideas and re-evaluation of previous work as new threats emerge. In Bristol we have the practical expertise to perform a wide range of attacks, which we share with the community via the OpenSCA toolbox (freely available via Sourceforge). Our future efforts will continue to translate our knowledge about attacks into the conception of secure devices.

Contribution and Outlook

- EPSRC via grant EP/I005226/1 and EP/F039638/1.
- European Commission through the ICT Programme under Contract ICT-2007-216676 ECRYPT II
- Industrial Collaborators:
  - CRI, Infineon, RFI-Global, Si-Venture.

Funding and Collaboration

QR code generated on http://qrcode.littleidiot.be