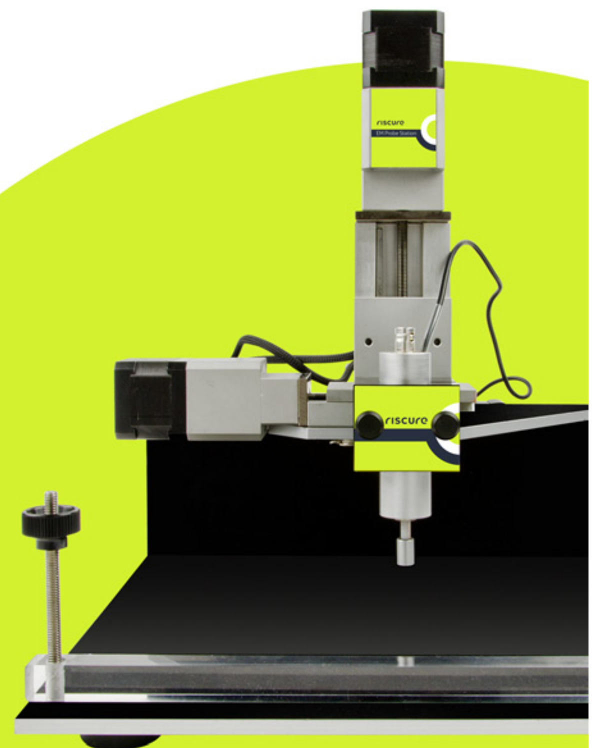
riscure

Challenge your security



EM Probe Station

Complete electromagnetic analysis solution for precise localised side channel measurements on a wide range of targets including embedded devices, contactless cards and conventional smart cards.

Introduction

Inspector's EM Probe Station provides a complete solution for EM analysis. It consists of three hardware components, two EM probes and a motorized XYZ table, which are integrated with the Inspector software for configuration, taking measurements and subsequently performing cryptanalysis.

Electronic devices draw current through their internal wires while functioning. Variations of these currents result in electromagnetic emanations related to the processing being performed by the device.

Due to this relationship, EM emanations can be used for Side Channel Analysis of smart cards and embedded devices. However, a high quality (i.e. low noise and large bandwidth) measurement device is important to achieve good results with a limited number of traces. Further, the quality of the acquired signal for Side Channel Analysis depends on the location of the probe with respect to the analyzed device.

The EM Probe is especially designed for side channel analysis. Top end differential amplifiers provide low noise and high bandwidth measurements of the EM signal. The high sensitivity probe is capable of measuring weak emanations from small current loops in the chip and will typically generate a signal with 1V amplitude for a state-of-the-art smart card. The low sensitivity probe is designed for analysis of contactless cards and embedded processors with strong emanations.

When used in conjunction with the XYZ table, it is possible to automate a scan of the complete chip surface in order to find the best measurement location. The small step size of the XYZ table combined with the high spatial resolution of the EM probe provides a very accurate way of measuring the signal intensity on different parts of the target device.

How to use the EM Probe Station?

In order to find the best measurement location, a user should perform the following steps:

- Use the XYZ table to automatically measure the EM emanations at different locations above the chip surface
- Use the sliders shown in Figure 1 to select a specific frequency band
- Identify hot spots for the selected frequency band
- Move the probe to a hot spot and acquire multiple measurements at this location

Key features

- High sensitivity probe for weak EM emanations and a low sensitivity probe for strong EM emanations.
- Measurement of high quality EM signals to reduce required number of traces.
- High spatial resolution for focusing on interesting areas.
- Completely automated scan over the chip surface.
- Small step size and little repositioning error of the XYZ table allow to profit from the spatial resolution provided by the EM probe.
- Integration with Inspector SCA software environment.

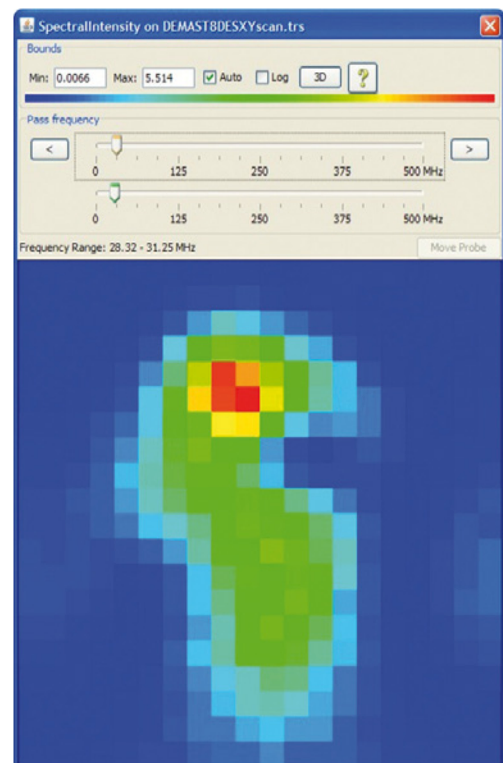
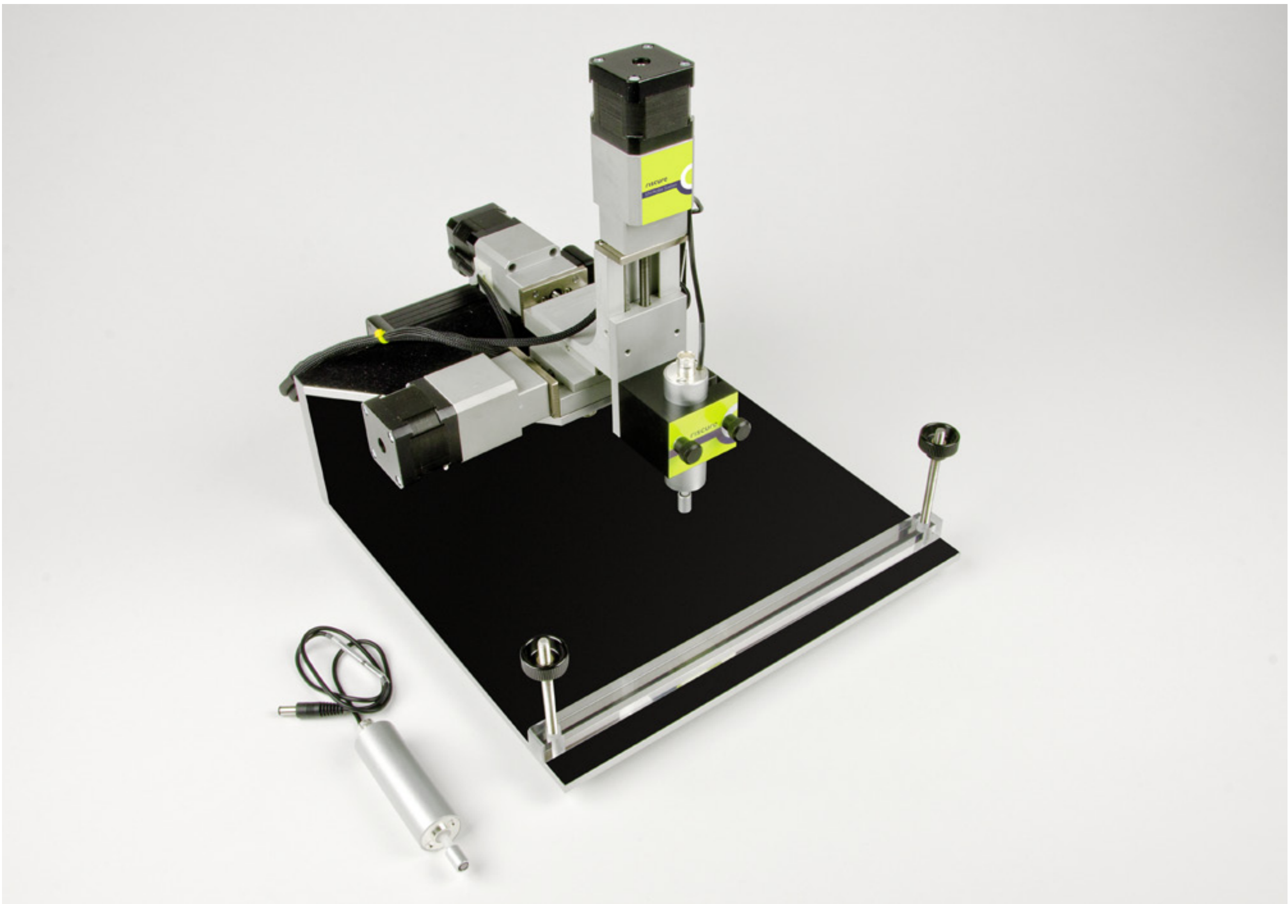
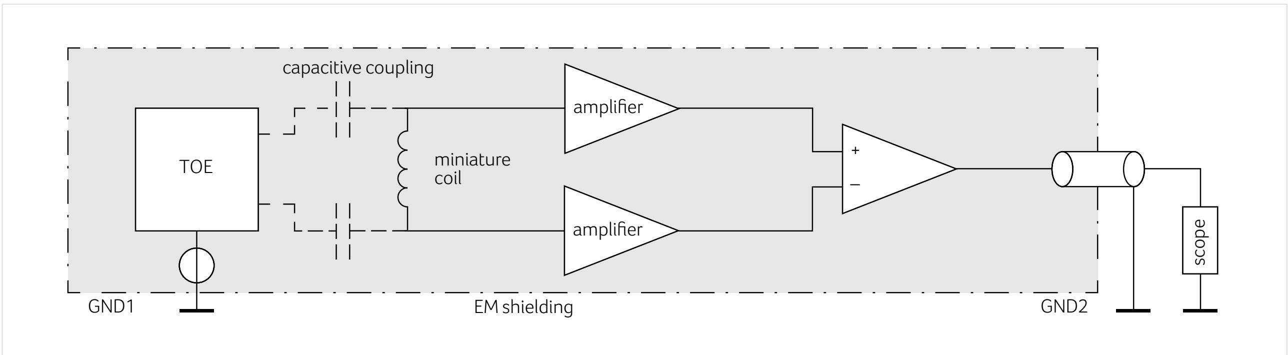


Figure 1 Module that shows the intensity of the specified frequencies for different locations above the chip surface (scan area 2 x 2 mm)





Conceptual overview of EM Probe

Inspector integration

For embedded crypto processors, the EM Probe Station can be used on its own for SEMA/DEMA measurements. For analyzing contact smart cards it is used in conjunction with the Power Tracer. For contactless smart card analysis, it works in conjunction with the MP300 TCL1/TCL2 and the CleanWave analog filter.

EM Probe Station SDK

The EM Probe Station can be operated without using Inspector. A Software Development Kit (SDK) is provided for integrating EM Probe Station in your custom tools. It contains a documented standard C API (Application Programmers Interface) and a simple example program that shows how to use the API functions.

Technical specifications

The EM Probe Station meets the following specifications:

- Low noise differential amplifier with 15pT/√Hz@1MHz noise for high sensitivity probe and 3pT/√Hz@1MHz noise for low sensitivity probe
- EMI shielding and choking of power line to further reduce noise
- 3 stage amplification providing sensitivity of 100mV/1µT@1MHz for high sensitivity probe and 20mV/ 1µT@1MHz for low sensitivity probe
- Amplifier bandwidth of 1 GHz
- 50Ω output impedance to avoid reflections and allow use of BNC in-line analogue filters
- Sensitive to EM field pointing out of die surface
- High spatial resolution: Coil inner area 1 mm^2 and outer area 2 mm^2
- 5V Power supply
- XYZ table step size of 2.5 µm
- XYZ table repetition error smaller than 50 µm to allow repeatability

riscure

Riscure BV

Frontier Building
Delftechpark 49
2628 XJ Delft
The Netherlands

Phone: +31 (0)15 251 4090
Fax: +31 (0)15 251 4099

E-mail: inforequest@riscure.com
www.riscure.com

EMPS 11.09.2011

Riscure provides these specifications for information only.
No rights can be obtained from these specifications.