QUOVADISLABS

QVL ESPIAL
OVERVIEW DOCUMENT

RELEVANT INDUSTRY SECTORS

• SECURITY SERVICE • MILITARY • AEROSPACE
• AUTOMOTIVE • MEDICAL • COMMUNICATIONS
• FAILURE ANALYSIS • ELECTRONIC METERS • E-COMMERCE
• BANKING • ELECTRONIC GAMING • HARDWARE SECURITY

OVERVIEW

The QVL Espial is a significantly new approach to sensor technology aimed at precision measurements with considerably higher sensitivity and lower noise than can be achieved with current technology.

When applied to side-channel analysis the QVL Espial allows 20dB–100dB gain over existing equipment or sensors and allows an improvement of x100–x1,000,000 over existing attacks in terms of time, and x10–x10,000 improvement in cost.

The technique can be uni-dimensional and multi-dimensional thus enabling the sensor to look at several parameters simultaneously, resulting in an unprecedented attack time, such as milliseconds for encryption key extraction. Conventional systems such as CRI DPA Workstation™ have an attack time of minutes or hours.

The first evaluation board, QVL-E, is an entirely non-invasive device which is built as a hybrid module onto a PCB which in turn connects to the chip to be analysed.

The next generation Espial, Pandora (already under development), can be made into a single piece of silicon to perform the same task, thereby reducing development time and costs.

The technology behind the QVL and Pandora Espials is patented and owned by Quo Vadis Labs Ltd.

CURRENT CAPABILITIES

When applied to any semiconductor chip, the QVL Espial can:

- extract cryptographic keys from a device through side-channel leakage. These keys include, but are not limited to AES, DES, TDES, RSA, ECC, SHA-1 and MD5
- extract passwords used for access to secret data
- reverse engineer the algorithm flow in chips
- reverse engineer the instruction flow for CPUs
- monitor device activity to spot any abnormalities caused by faults, trojans, backdoors or even the attachment of an unexpected or unauthorised device to the chip.

CURRENT APPLICATIONS

- Failure analysis to spot any faults in the operation of a given chip.
- Against security in microcontrollers, smartcards, FPGAs and ASICs to get access to keys and passwords.
- Reverse engineering of design in microcontrollers, smartcards and FPGAs.
- Analysis of ASICs and custom chips.
- Health monitoring of chip operation.
- Scanning for trojans and backdoors inserted by third parties.

COLLABORATION OPPORTUNITIES

- Quo Vadis Labs Ltd act as consultants to the semiconductor industry to highlight security issues on manufacturers' silicon, deliver reports, perform hardware evaluation and advice to fix any security issues.
- Develop a benchmark standard where other chips' performance can be rated against the QVL Espial to test whether they can withstand the sensor.
- Develop a silicon version of the sensor to be placed in the mass market.
- Lease or sell the sensor technology or particular design to a chip manufacturer on an exclusive basis.
- Sign a Non Disclosure Agreement on the Quo Vadis Labs' research findings, specific to a particular chip manufacturer.
- Sign an agreement not to make our findings public until the specific chip manufacturer has implemented proper and sufficient countermeasures.

info@quovadislabs.com
WWW.QUOVADISLABS.COM