riscure

inspector

Riscure

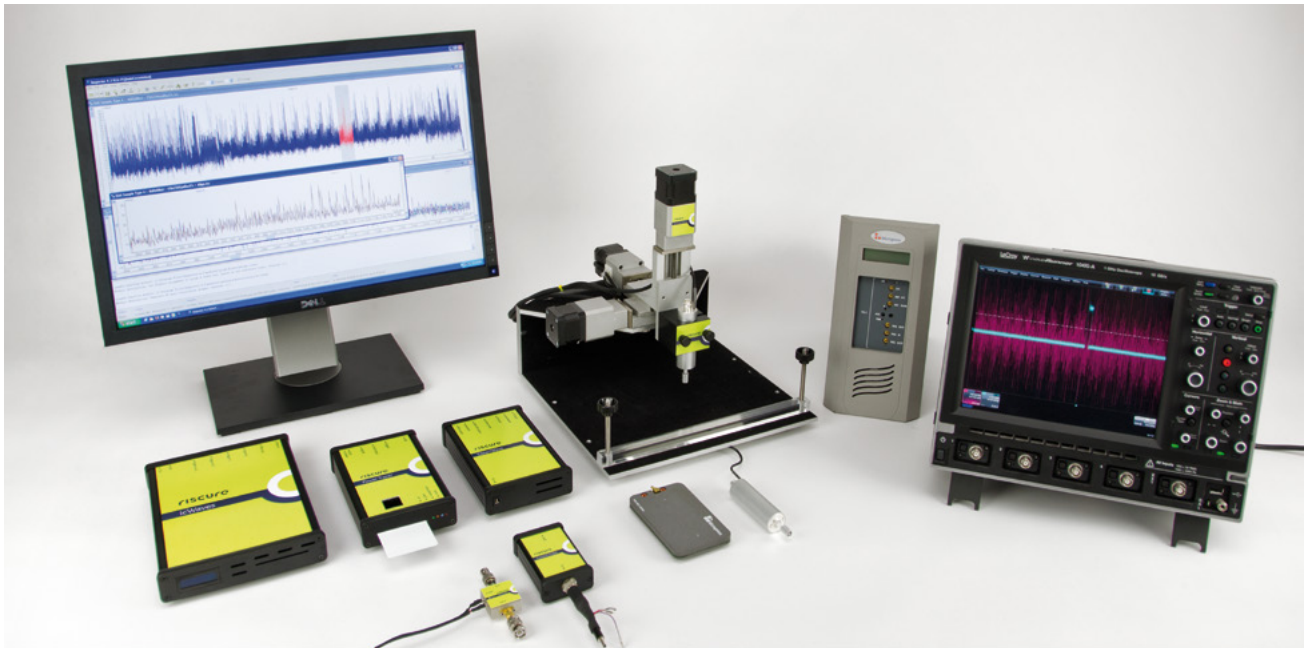
Riscure is an independent security test laboratory specialising in security testing of products based on smart card and embedded technology.
Riscure's specialists work with industry leaders worldwide to create products that require strong security to operate safely in a hostile environment.
Riscure was amongst the first to apply side channel analysis techniques to smart cards, and pioneered Differential Power Analysis attack techniques.

We support security evaluation laboratories, government agencies, manufacturers, and card issuers by conducting security evaluations and by providing and maintaining the Inspector Side Channel Test Tool.
Riscure is an EMVco-accredited security evaluation laboratory.

Inspector is an advanced integrated tool for side channel analysis and fault injection. Designed to meet the highest standards of security research teams, certification labs and businesses around the world, Inspector excels in time-efficient analysis and perturbation of evaluation targets with the latest attack techniques and methods. Inspector is open for extension and modification, user-friendly, and designed for accuracy and reliability, guaranteeing clear and reproducible results.

Over the past decade, unintentional data leakage and program flow manipulation through side channels have emerged as methods for attackers to retrieve secrets or perform other unauthorised actions. Traditional attack methods can be costly in terms of knowledge, time, and computing power. Side channel attacks on the other hand can be more easily mounted and are non-invasive as they observe or manipulate physical properties available during normal operation. By using statistical methods on side channel measurements, or by injecting faults into a secure chip, an attacker can gain access to its secrets within a matter of hours.

High flexibility, strong capabilities



Inspector SCA with Power Tracer, EM Probe Station, icWaves, CleanWave and Current Probe.

Signal processing functions can be applied real-time during data acquisition

With over 5,000 million smart cards being issued every year, and embedded cryptographic technologies emerging in new markets, there is a growing need for security to protect business models and privacy. Cryptographic protection of sensitive data in hostile environments is vital to safeguard intellectual property and business models, user privacy and safety, and regulatory or statutory compliance. Inspector provides test and research labs as well as manufacturers with a highly efficient means of identifying threats in the implementation of a security model.

Inspector supports side channel analysis methods such as power, timing, radio frequency, and electromagnetic analysis, and perturbation attacks such as voltage glitching, clock glitching, and laser manipulation.
Inspector features built-in support for numerous cryptographic algorithms, application protocols, interfaces, and measuring devices. Inspector can be extended by using the integrated development environment or Eclipse. Inspector lets you easily develop and research new test techniques and test proprietary implementations.

Mature testing tool

Inspector has become the side channel and fault injection test tool of choice for many organisations around the world including government agencies, manufacturers and commercial laboratories. With a broad user base in North America, Europe and Asia, Inspector is a mature solution that offers the best possible means of determining a device's side channel security and fault resistance.

Key features

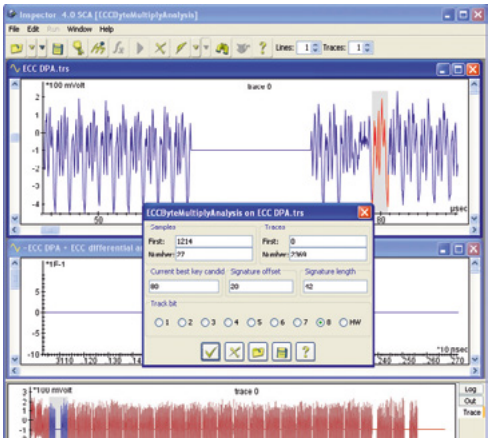
- Single integrated tool for side channel analysis and fault injection testing
- Inspector meets the side channel test requirements of Common Criteria, EMVco, and CMVP certifications
- Open environment includes source code of modules, allowing existing techniques to be modified and new test methods to be developed from within Inspector
- Stable and mature, tightly integrated software and hardware enables high-speed acquisition of millions of traces
- Comprehensive tutorials with configurable training test objects, up-to-date user documentation, and training programs
- Six-month software release cycle keeps users up-to-date about the latest side channel test techniques in the field
- Service contract provides access to a dedicated support desk

Inspector is released in different versions to suit different testing needs. All variants use the same core software, which can be used separately or integrated in a single multifunctional platform.

- **Inspector SCA** offers complete side channel analysis functionality
- **Inspector FI** offers complete fault injection functionality (perturbation attacks) as well as Differential Fault Analysis (DFA)
- **Inspector Core and SP** – Signal Processing offers basic SCA functionality, cut to size to provide an accessible software package suitable for acquisition or post-processing.

Different needs, same platform

Inspector SCA



Performing DPA on an ECC implementation

Inspector SCA – Side Channel Analysis – offers all the necessary options to conduct side channel analysis, such as DPA and EMA. Different hardware components address the form factors that we nowadays find in high-security products: contact smart cards, contactless smart cards, and crypto processors in embedded technology. Once the measurements have been taken, a wide variety of signal processing methods is available to establish a high signal and low noise trace set. The signal processing features are designed to deal with the subtle differences between the signal processing of an electromagnetic trace, a power trace, and an RF trace. Inspector's strong graphical trace representation enables users to perform timing analysis or trace inspection on e.g. SPA vulnerabilities.

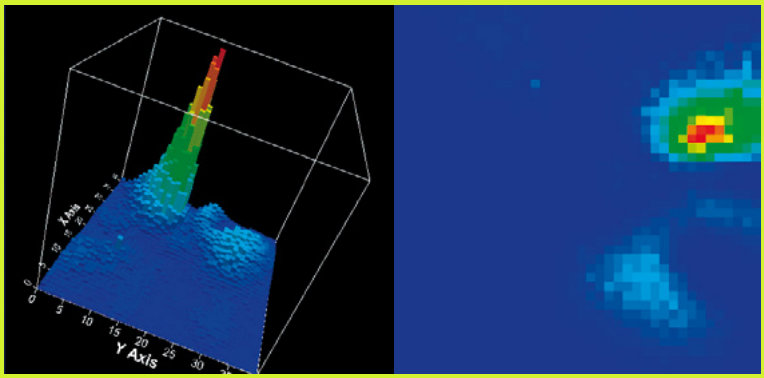
With many secure implementations nowadays being SPA-resistant, the focus of testing typically lies on differential test methods (i.e. DPA/CPA). For this purpose Inspector offers an extensive set of configurable methods covering a large number of cryptographic algorithms, and such established algorithms as (3)DES, AES, RSA, and ECC.

"The EMA capabilities of Inspector take an important place in our security evaluations for our customers of secure system-on-chip technologies that are deployed in embedded devices."

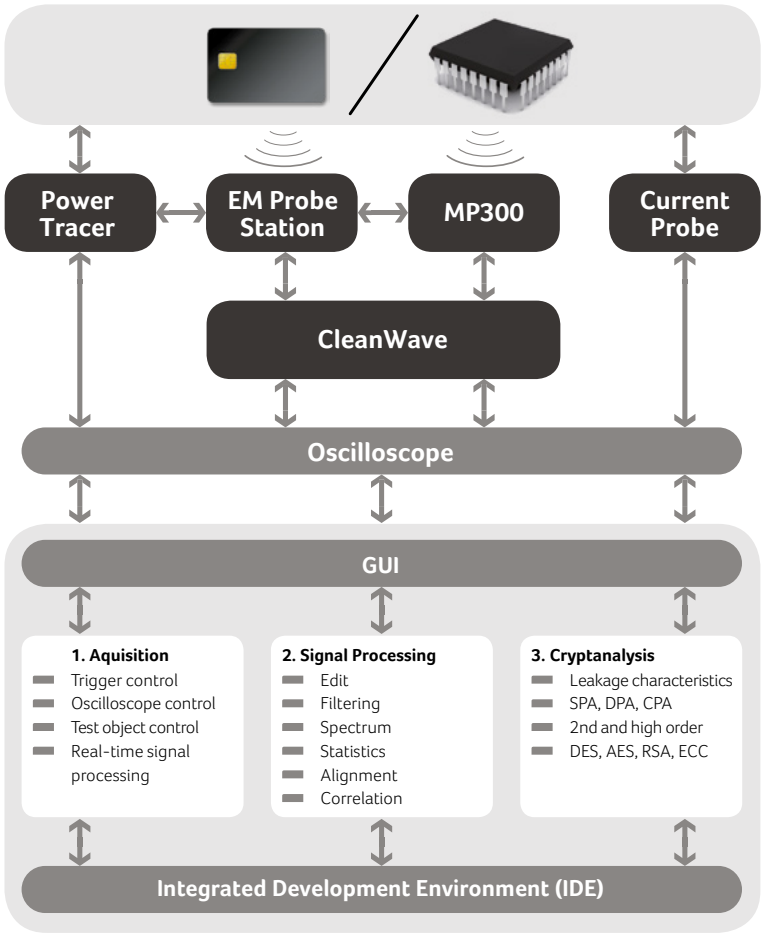
Job de Haas, Director Embedded Technology

Key features

- Single solution for power (SPA/DPA/CPA), electromagnetic (SEMA/DEMA/EMA-RF), and contactless (RFA) testing methods
- Fast analysis and processing using application-specific custom measuring hardware
- Time-efficient thanks to automated real-time signal processing during data acquisition
- Tight oscilloscope integration for full acquisition settings configuration from within Inspector, significantly boosting acquisition speed
- Advanced alignment methods to overcome clock jitter and randomisation countermeasures
- Highly configurable cryptanalysis modules supporting first-order and high-order attacks on all major algorithms such as (3)DES, AES, RSA and ECC
- Extensive region-specific algorithm support includes SEED, MISTY1, DSA and Camellia among others



EM emanations of a chip to find the best location to perform DEMA



Inspector SCA

Hardware

In addition to a PC workstation, Inspector SCA uses hardware optimised for side channel data and signal acquisition.

- Power Tracer for SPA/DPA/CPA on smartcards
- EM Probe Station for SEMA/DEMA/EMA RF
- Current Probe for SPA/DPA/CPA on embedded devices
- CleanWave with Microprocess MP300 TCL1/2 for RFA and EMA-RF
- LeCroy WaveRunner 104Xi-A or IVI-compatible oscilloscope

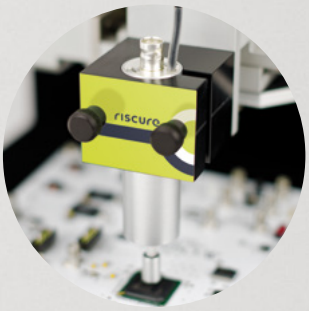
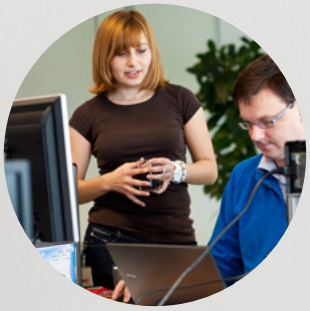
The target under evaluation will often dictate the measuring, triggering, and control hardware needed to perform SCA. Inspector's flexible hardware manager, open development environment, and broad interfacing options provide a solid foundation for high-quality measurements using custom hardware.

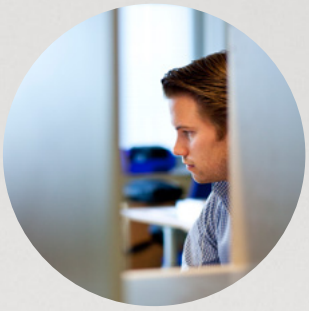
John Connor, Principal Security Engineer from INSIDE Secure says:

> “Inspector has revolutionized the way we evaluate our products’ DPA resistance. Its strength lies in the way it integrates the acquisition and analysis processes allowing us to quickly determine the effectiveness of new cryptographic hardware designs.
>
> Further, its excellent graphical interface allows the user to visualise the power signatures of discrete acquisitions individually or simultaneously - invaluable when preparing data for DPA during an attack – while its powerful analysis libraries support most commercially used encryption algorithms.
>
> With comprehensive software updates and technical support from Riscure it helps us keep our products secure.”

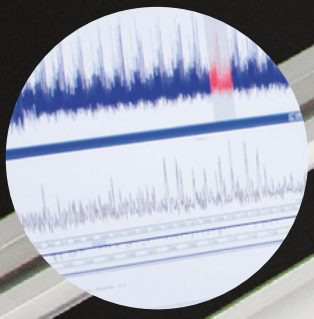
riscure inspector

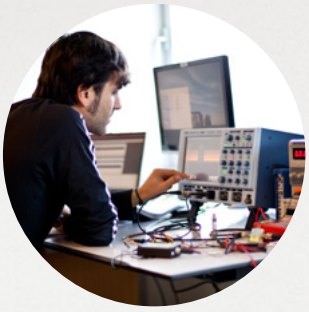


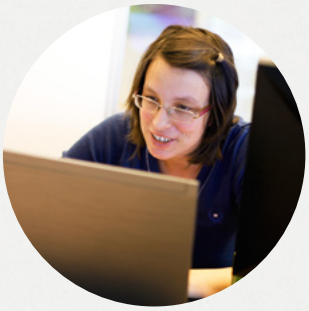













Inspector FI

Inspector FI – Fault Injection – offers a comprehensive set of features to perform fault injection testing on smart card technology and embedded devices. Supported test methods include clock glitching, voltage glitching, and optical attacks with purpose-built laser equipment. Fault injection attacks – also known as perturbation attacks – change the behaviour of a chip by inducing an exploitable fault. With Inspector FI users can test whether they can extract a key by inducing faults in a chip's cryptographic operations, bypass a check such as an authentication or a lifecycle state, or change the program flow on a chip.

Extensive configuration options

Inspector FI includes highly customisable software-controlled trigger and perturbation parameters such as glitch and pulse length, pulse repetition, and voltage level. The software presents the results by showing expected behaviour, card resets, and unexpected behaviour, along with a detailed log. DFA attack modules are available for major encryption algorithms. Using a wizard, users can also create a custom perturbation program with the API.

Key features

- Unparalleled and easily reproduced accuracy and timing for all glitching hardware
- Design attack scenarios using a powerful instruction set and Inspector's integrated IDE
- Extensive configuration options from Inspector to automate fault injection testing
- Back- and front-side multi-glitching laser equipment, custom-designed for fault injection testing
- DFA modules for implementations of popular encryption algorithms, including RSA, AES, and 3DES
- Multi-location laser upgrade provides the option to target multiple locations at once.
- Operation-dependent timing using icWaves to defeat countermeasures and prevent sample loss

Testing the effectiveness of counter-measures is essential when improving the security design of a product

Hardware

Inspector FI can be used with the following hardware components to perform attacks:

- VC Glitcher with optional Glitch Amplifier
- Diode Laser Station with optional Multi-Area upgrade
- PicoScope 5203 or IVI-compatible oscilloscope

The VC Glitcher forms the core of Inspector's fault injection architecture. Using ultra-fast FPGA technology, it can generate faults that are only two nanoseconds long. The hardware features a user-friendly programming interface. The glitch program created by the user is loaded on the FPGA before a test run. The VC Glitcher includes integrated circuitry for performing voltage and clock glitching, and an output channel for controlling the Diode Laser Station.

The Diode Laser Station consists of a special set of powerful diode lasers with custom-designed optics controlled by the fast and flexible VC Glitcher. The equipment takes optical testing to a new level by offering effective multi-glitching, precise power control, and fast and predictable response to trigger pulses. With the Multi-Area Diode Laser Station upgrade multiple area's on the chip can be target using different timing and power parameters.

Waveform-based triggering using icWaves

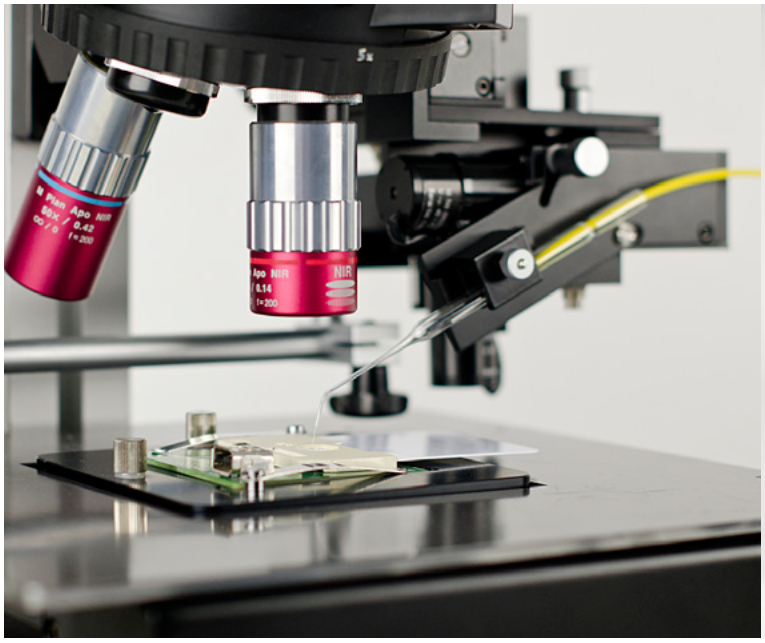
Clock jitter, random process interrupts, and data-dependent process duration require flexible triggering of fault injection and side channel acquisition. Inspector's icWaves component generates a trigger pulse in response to the real-time detection of a distinctive pattern in a chip's power or EM signal. The device includes a special narrow band-pass filter to enable the detection of matching patterns even in noisy signals. The reference trace used for the pattern match inside this FPGA-based device can be modified using Inspector's signal processing features.

A smart card detecting a fault injection may initiate a protection mechanism to delete secret data or mute the card. The icWaves component can also be used to trigger the powering down of a card whenever the power or EM profile deviates from the standard operation.

"Efficiency and thoroughness are the cornerstones of our design philosophy. Inspector enables us to perform high-end security evaluations on the one hand and train engineering staff on the other hand".

Marc Witteman, Chief Technology Officer

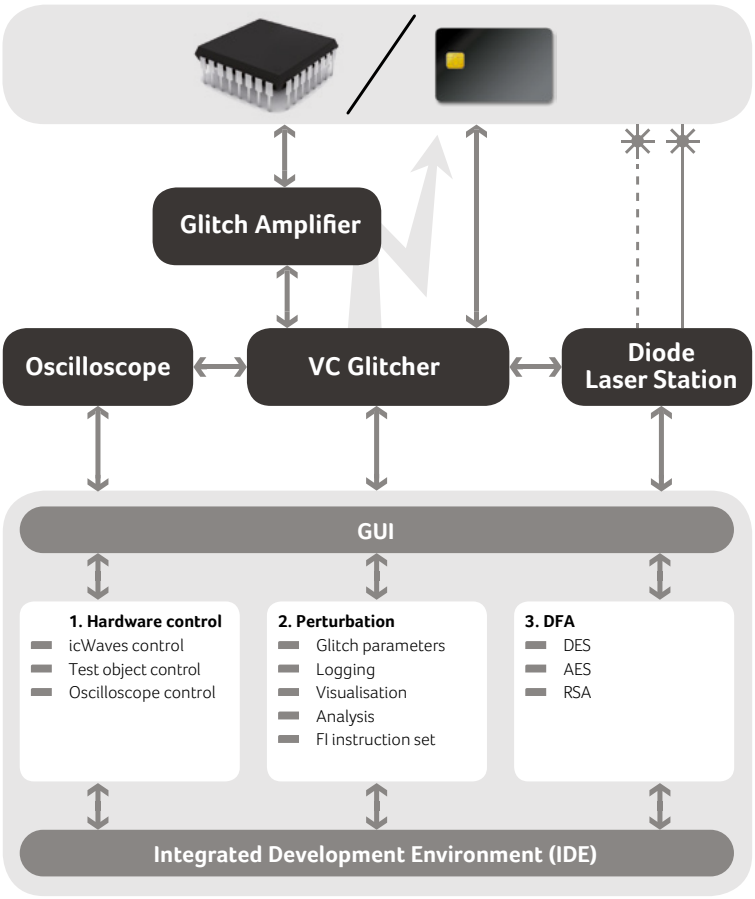
Inspector FI with VC Glitcher, icWaves, Glitch Amplifier and Diode Laser Station.



Diode Laser Station with Multi-Area upgrade option.

Diode Laser Station (DLS) with Microscope and XY Stage

Inspector combines fault injection and side channel analysis techniques in one high-end package



Inspector FI

Integrated development environment (IDE)

The development environment in Inspector is designed to offer maximum flexibility to the user, allowing SCA and FI on any target.

- Open API: Facilitates the implementation of new modules
- Source code: Each module is supplied with its source code so modules can be tailored as required or used as starting points for new modules

Service & Product support

User training

Inspector SCA and Inspector FI include a multi-day training course by two Riscure side channel specialists. Participants gain hands-on experience with Inspector and perform tests on training chips. Depending on the options purchased, a subset of the following topics is covered:

- Introduction to side channel analysis and fault injection methodology
- Inspector functions and user interface
- Hardware components
- Signal processing features
- Cryptanalysis on common algorithms (SPA, DPA, CPA)
- Perturbation attacks and DFA
- Tuning modules and developing new techniques
- Step-by-step analysis of training chips

State of the art

Internal R&D and feedback from our customers are used to ensure that Inspector remains a state-of-the-art product. Our specialists use Inspector to perform side channel evaluations for customers all over the world. Riscure is an EMVco-accredited security evaluation laboratory. By using and evaluating Inspector on a daily basis, we make sure that our product always incorporates the latest side channel test techniques.

Service contract

The field of side channel attacks is rapidly evolving, with new research results being published every year, are gaining popularity or made obligatory by certification schemes and standards. Inspector enables users to stay up-to-date about developments via regular software updates that implement new techniques. The Inspector service contract includes:

- Software updates with new forms of attack, features, and improvements
- Annual Inspector User Workshop with the latest developments in the field
- Technical support from our help desk

Annual user workshop

Customers are invited to attend the annual two-day technical workshop. At the workshop, which takes place in the Netherlands, we present the latest developments in the field of side channel attacks. New and updated Inspector features are also presented and discussed, as is our product development road map. During the workshop, users can share their Inspector experiences with others. Visit our web site to find out the date and topics for our next workshop.

Did you know that with inspector:

- You stay up-to-date about the latest side channel test techniques
- You use measurement hardware optimised for crypto processors
- You work with a test tool used by EMVco- and Common Criteria-accredited laboratories
- You optimise your R&D thanks to the integrated development environment
- You receive an excellent Return on Investment with improved efficiency and a short learning curve

More information

For more information about Inspector, please contact us by phone at +31 (0)15 251 4090 or by email at inforequest@riscure.com.

Detailed information about Inspector components can be found at www.riscure.com/inspector.

Inspector Hardware Matrix

		Side Channel Analysis			Fault Injection		
		Power	**Electromagnetic**	**Radio Frequency**	**Power**	**Clock**	**Optical**
	Application	SPA, DPA, CPA on embedded processors and smart cards	SEMA, DEMA and EMA-RF on smart cards, contactless cards and embedded processors	RFA on contactless smart cards	Power glitching on embedded processors and smart cards	Clock glitching on smart cards	Optical fault injection on embedded processors and smart cards
	Strengths	Low noise smart card measurements, short acquisition times, advanced filtering and alignment options	Sensitivity and resolution optimised for crypto processors, automated surface scanning, flexible in use	Low noise contactless measurements, integrated triggering and highly configurable device control	Very short pulse generation, flexible glitch program, structured and efficient test approach	Very short pulse generation, flexible glitch program, structured and efficient test approach	Multi-glitching, precise power control, customised optics, diode lasers for front and back side testing
	Standalone options	Power Tracer SDK	EM Probe Station SDK	CleanWave	VC Glitcher SDK	VC Glitcher SDK	DLS SDK VC Glitcher SDK
Embedded Processor	**Measurement / Pertubation**	**Current Probe with amplifier**	**EM Probe Station**	-	**VC Glitcher with Glitch Amplifier**	-	**VC Glitcher with Diode Laser Station**
	Control	Native interface, program on target or RS-232/TCP-IP from software	Native interface, program on target or RS-232/TCP-IP from software	-	Native interface, program on target or RS-232/TCP-IP from software	-	Native interface, program on target or RS-232/TCP-IP from software (optional: Multi-Area upgrade)
	Triggering	icWaves, external, program on target or software	icWaves, external, program on target or software	-	icWaves, external, program on target or software	-	icWaves, external, program on target or software
Smart Card	**Measurement / Pertubation**	**Power Tracer**	**EM Probe Station**	-	**VC Glitcher**	**VC Glitcher**	**Diode Laser Station**
	Control	Integrated	Power Tracer	-	Integrated	Integrated	VC Glitcher (optional: Multi-Area upgrade)
	Triggering	Power Tracer or icWaves	Power Tracer or icWaves	-	VC Glitcher or icWaves	VC Glitcher or icWaves	VC Glitcher or icWaves
Contactless Smart Card	**Measurement / Pertubation**	-	**CleanWave with EM Probe Station**	**CleanWave with MP300 TCL2**	-	-	**Diode Laser Station**
	Control	-	MP300 TCL2	MP300 TCL2	-	-	MP300 TCL2 (optional: Multi-Area upgrade)
	Triggering	-	icWaves or MP300 TCL2	icWaves or MP300 TCL2	-	-	icWaves or MP300 TCL2

	Separate Components		
	icWaves	**CleanWave**	**EM Probe HS/LS**
Application	Real-time trigger generation from filtered power or EM signal	Removes RF carrier wave for high quality RFA/ EMA-RF measurements	Standalone probes to measure EM emanations with high and low sensitivity respectively
Strengths	Real-time trigger pulse generation, tunable digital filter for noisy signals, integrates witch each inspector component	Filters RF signals and demodulates data, optimizes signal-to-noise ratio, greatly reduces the number of traces required	Sensitivity and resolution optimized for different crypto processors with weak or strong emissions
Standalone	SDK	Yes	Yes

riscure

Challenge your security

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

Chamber of Commerce reg. no. 27287509