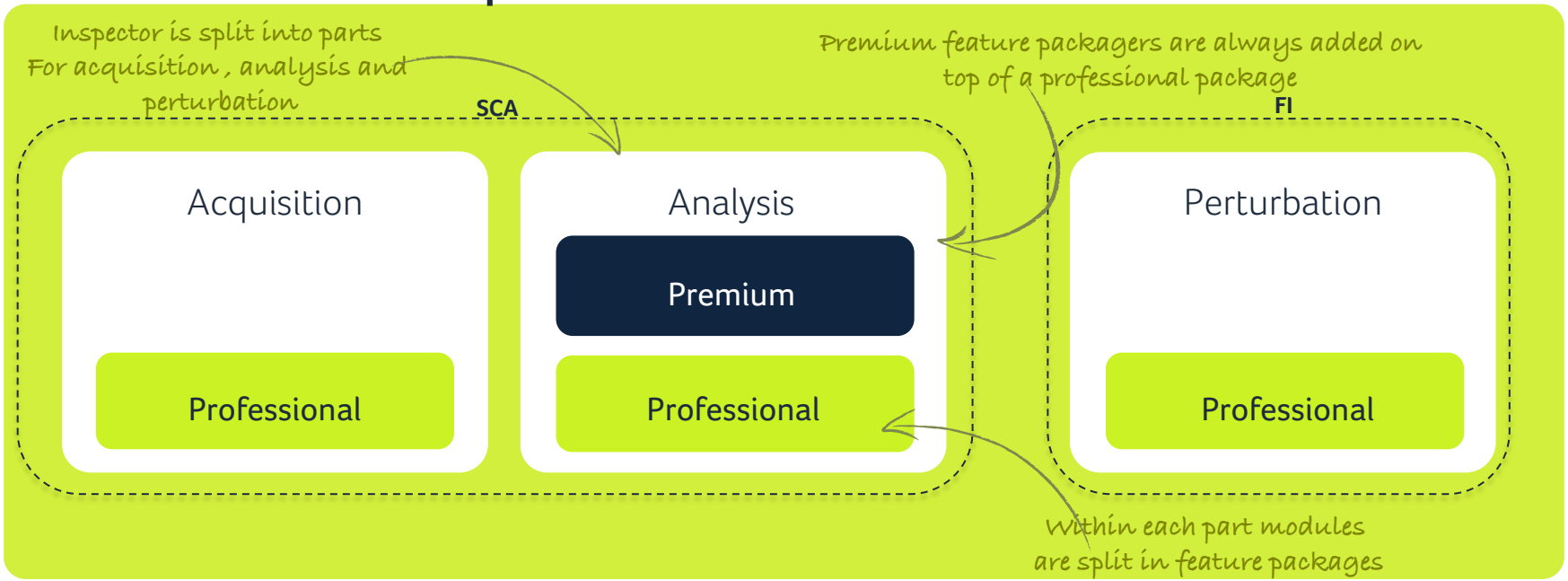
riscure

Overview feature packages

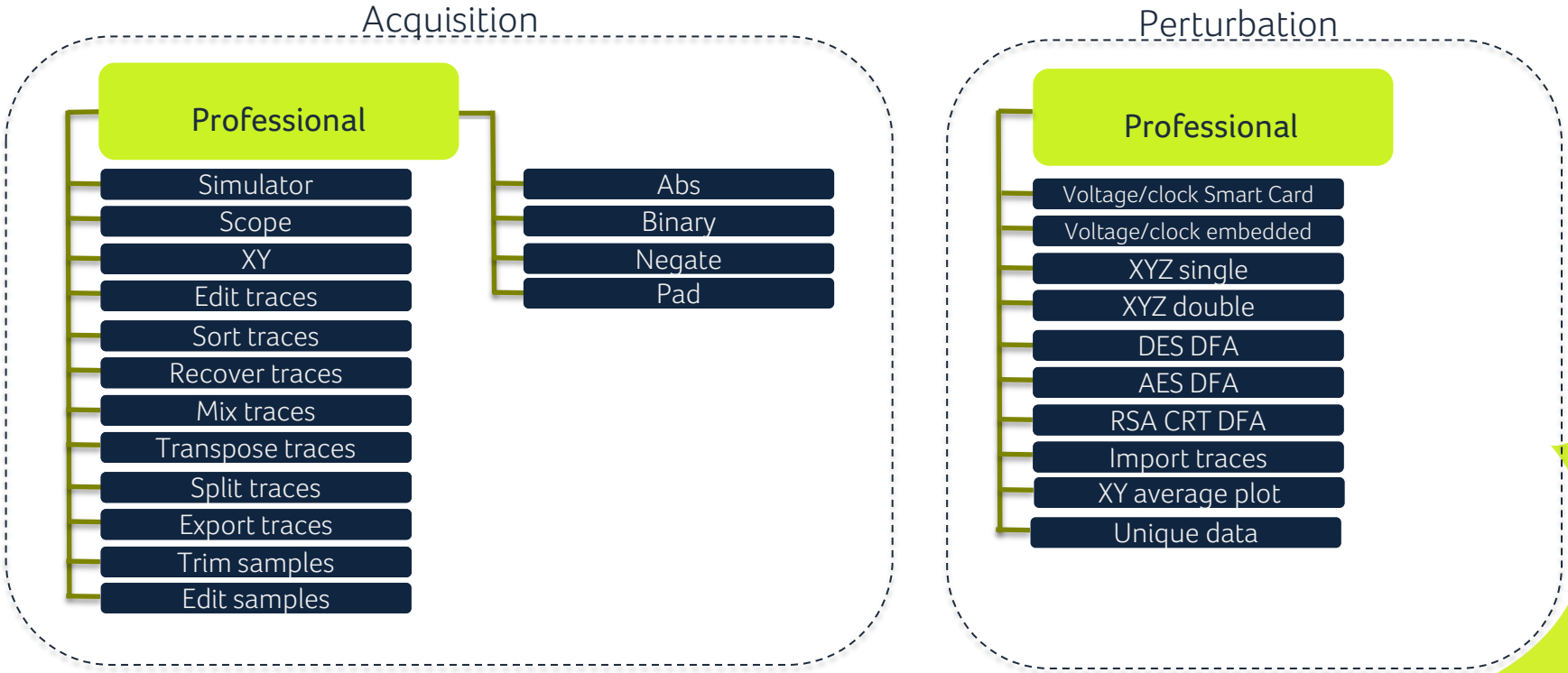
v 1.1

Contents

Overview Inspector software

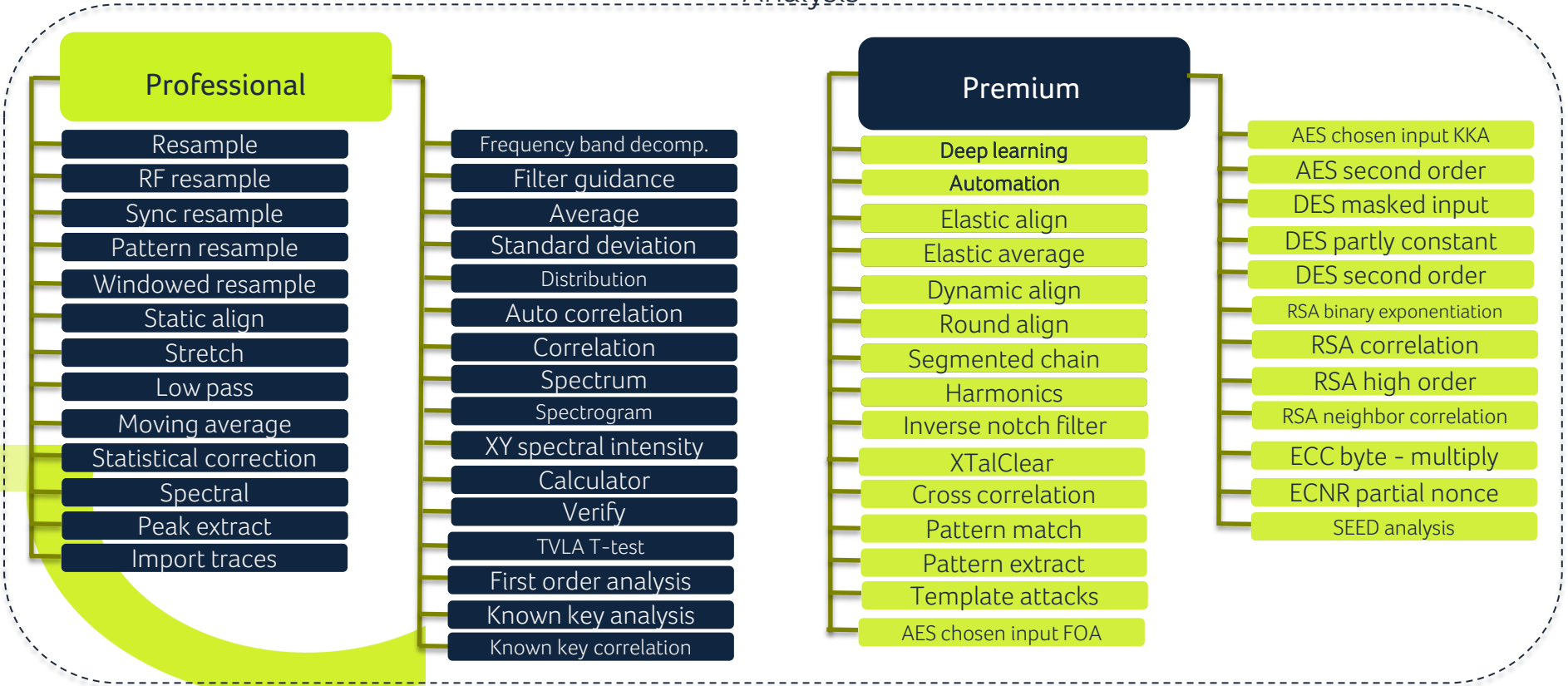


Overview Inspector software



Overview Inspector software

Analysis



RE PACKAGES

Acquisition professional

Modules

Acquisition

Acquisition Simulator

Simulator used to produce power traces for a model crypto target and leaking all selected leakage models

Acquisition Scope

Collect multiple measurements from a target within a single session

Acquisition XY

Collect multiple measurements from a target within a single session using a probe that is automatically moved over an XY grid.

Trace manipulation

Edit traces

Manipulate data stored in a trace set by changing values of data bytes within a specific range

Sort traces

Sort traces in a specific order based on a selection of samples

Select traces

Extract an arbitrary subset of traces from a trace set

Recover traces

Repair a corrupted trace set

Mix traces

Mix a selection of traces (Add, Subtract, Multiply, Divide, Convolute or Correlate) with a single selectable reference trace

Transpose traces

Swap samples and traces. As a result the first result traces will be the concatenation of the first samples of all traces, etc.

Split traces

Split a trace set with interleaved traces for example when traces in a trace set result from a different signal operation or are acquired from different sources (scope channels)

Export traces

Export a trace set to a text file with a comma-separated format, MAT file format version 5 or CRI format

Trim Samples

Trim traces with a selectable number of samples that are longer then needed

Edit samples

Add or delete samples from a trace set with an option to use the clipboard

Operations on samples

Abs

Rectify an AC signal relative to a selectable offset. The module can also compute an average value and use this value as a reference offset

Binary

Convert traces into a binary representation. Every sample will be compared to a threshold and based on this set to 0 or 1

Negate

Mirror the samples in a trace over the x-axis

Pad

Pad samples after or before a pattern match with a constant value. Useful as a preprocessing step before elastic alignment

Analysis professional

Modules

Resampling

Resample

Resample a trace set with a lower frequency. When used properly this module enables to strongly reduce the trace size without losing valuable information.

RF resample

This module can be used to resample a Radio Frequency Analysis signal after passing through the sample and hold demodulator. The sample and hold demodulator takes two samples for each period of the RF carrier wave, hence at a frequency of 27.12 MHz, equal to twice the carrier wave. The RFResample module synchronizes to the RFA demodulated signal and resamples the signal to a 27.12 MHz.

Sync resample

Resample traces to a lower frequency while each sample period is dynamically tuned to the wave shape.

Pattern resample

Find pattern matches and compress them. The module has two phases: 'Correlate', for detecting pattern occurrences and 'Filter', for extracting the patterns.

Windowed resample

To do a window based compression. Rather than converting from one frequency to another, this module simply compresses N samples into 1 (where N is the window size). Additionally, the compression may use overlapping windows.

Alignment

Static align

Align traces based on a single shift per trace based on a reference trace

Stretch

Scale traces which previously were statically aligned. This function enables unstable clocks or random process interrupts to be corrected

Low Pass

The module applies a fast bidirectional filter to each trace, making each sample a weighted average of the previous sample and the current sample

Moving average

Average samples within a trace and reduce noise

Statistical correction

Improve the statistical quality of a trace set by rejecting outlying traces and optionally correcting small divergences of the average values

Spectral

Efficient filtering on specific, configurable frequency ranges from a trace set

Peak extract

To extract positive peaks repeating in a trace set. The peaks need not be exactly evenly spaced. Instead, they are found within a specified interval.

Frequency band decomposition

The module first applies a set of band-pass filters on original traces, secondly takes the absolute values, and finally applies a low-pass filter on these traces. The bandwidth of band-pass filter is B and that of low-pass filter is B/2. The slopes of these applied filters are infinitely steep. In the end, the processed trace set will be produced. The new traces present the specified number of frequency components

Filter guidance

This module gives suggestions on the choice of appropriate frequency filters for side channel signals. It automatically constructs multi band-pass filters based on cross-correlation between narrow-band side-channel traces. It should be applied to the output trace of Frequency Band Decomposition or Spectrogram.

Statistics

Average

Compute an average trace from a set of multiple traces.

Standard deviation

Compute the standard deviation of a trace set. The result can be used to judge the need for alignment or verify the quality of an aligned trace set, because non-alignment causes a significant standard deviation.

Distribution

To compute the value distribution of samples per trace, or for a trace set. This analysis can be useful to observe noise or to distinguish separate coding paths.

Analysis

Auto correlation

Visualize repeating processes in a single trace by computing an auto-correlation graph. This analysis can be useful to recognize known program structures, such as permutations.

Correlation

To investigate an implementation's susceptibility to side channel analysis. It is possible to establish whether sensitive (crypto) data leaks from the implementation based on correlation.

Spectrum

Analyze the frequency spectrum of a trace. By observing the spectrum, the analyst can verify the clock frequency and its stability.

Spectogram

Present and analyze the evolution of the spectrum over time for a trace.

XY Spectral intensity

The SpectralIntensity module can be used to present and analyze the resulting trace set of an EM scan of a chip area which is performed using XYAcquisiton. The module presents the Intensity of the measured signal at the X x Y grid positions and calculated for a selected frequency range. High intensity is indicated by a red square and low intensity is indicated by a blue square, with intermediate values indicated by the rainbow colors in between blue and red.

Calculator

Calculate crypto output and intermediates given input and key.

Verify

Verify if input/ouput data of traces are correct given a key and algorithm.

TVLA T-test

This module performs Welch T-test using the Random set against all the semi-constant sets from the input trace set, and it produces the T-value trace set, and, when enabled, produces the T-value evolution plot trace set.

First order analysis

Retrieve the key of a supported crypto algorithm using sophisticated statistical analysis methods.

Known key analysis

Find the strongest locations of leakage and see as a result the strength of the leakage related to every key byte at each data point of the input trace.

Known key correlation

Find correlation with intermediate values for different leakage models. A trace set is returned for each intermediate value and each leakage model gives a correlation trace.

Import traces

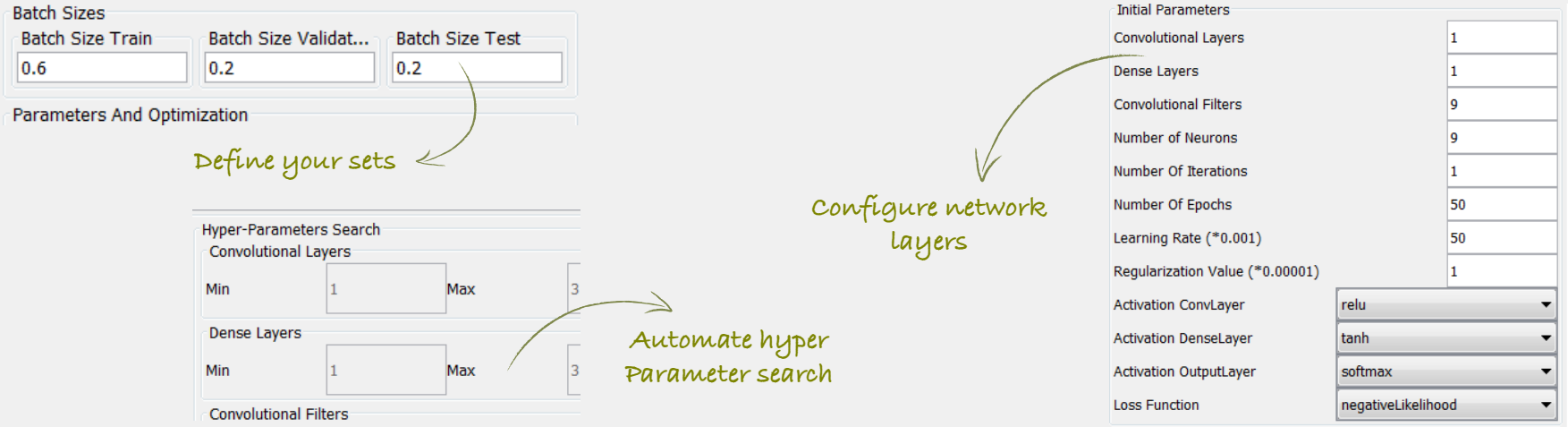
Import a trace set from a text file in comma-separated format or produced by the CRI tool, DPAWS or from a Version 5 Mat-file compliant .mat file.

Analysis premium

Deep Learning

The Deep Learning module uses a convolutional neural network to make side channel analysis more efficient. Best results can be achieved with alignment, Point of Interest Selection, classification of data and Key Recovery. The network that can be trained on part of a trace set and applied to the full trace set. The module will assist the user to choose the best configuration of hyper parameters

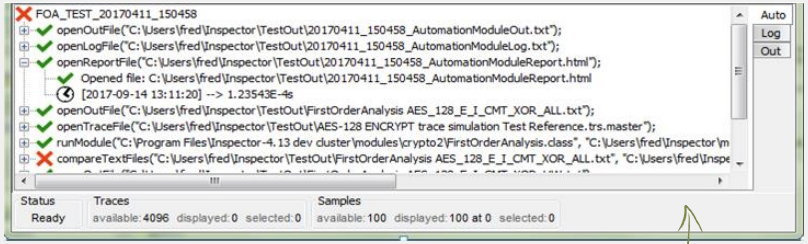
- ✓ Boosts your SCA template analysis capabilities and rely on a neural network next to the expertise of your analyst to be successful.
- ✓ It is easy to train the network to the unique quirks of your trace acquisition process
- ✓ Extend 'human' research effort with processing power
- ✓ Be compliant : evaluation using Deep Learning algorithms has recently become a requirement for a number of common certification schemes.



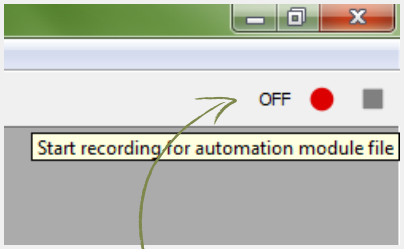
Automation

This new module enables you to reduce manual work and perform side channel analysis faster then ever before. Use record and playback functions to create a test scenario once and run it multiple times without the need for repetitive actions. The module enables regression testing and archives everything used in a scenario : parameters, templates, intermediate results, reference traces, etc.

- ✓ Generates a programmable user module
- ✓ Build loops to run a automation scenario with multiple settings
- ✓ Works with all modules
- ✓ Integrates perfectly with Inspector High Performance Analysis (HPA)
- ✓ Uses known Inspector principles to guarantee a steep learning curve for users



Progress of the automation scenario is shown in new "auto' tab



Buttons enable 'macro like' recording of automation scripts

Modules

Elastic align

Elastic alignment differs from static and dynamic alignment by using local compression and stretching of traces to perform the synchronization, and the absence of the necessity to select a reference pattern. The trace set output is elastically aligned to the specified reference trace. Normally, the output trace set has the same number of samples as the input trace set. However, if the action is align and an external reference trace is selected, this external trace set determines the number of samples in the output trace set.

Elastic average

Produce an average trace for a trace set by performing repeated elastic alignment and averaging of trace pairs. The resulting average is not biased with respect to a single trace and can therefore be used as reference trace to elastically align a larger set. Intermediate results can be saved based on a setting in the module

Dynamic align

This process starts by performing a Static Alignment. After static alignment has completed, it performs repeated shifts to achieve continuous alignment with the reference trace

Round align

This module can be used to align multiple misaligned rounds in a trace set by inserting pauses at the right moments. Rounds are detected by a pattern match.

Segmented chain

Similar to the Chain module, this module repeats a chain of operations to subsets of traces as if they are separate trace sets. This is especially useful for traces acquired in a XY scan, where multiple traces are acquired at the same location and the same analysis, e.g. correlation, is to be applied to traces from the same spot to determine the best measurement spot.

Harmonics

With this module it is possible to perform a special form of spectral filtering of a trace. A filter can be configured to facilitate efficient filtering of specific frequencies and their harmonics from a trace set. An analyst can estimate the filter frequency, and the module will center the filter on the strongest frequency in the neighborhood of the estimated filter frequency.

Inverse notch filter

This module inverts the EMA-RF signal after passing the multi-notch filter of the CleanWave. The CleanWave attenuates the RF carrier together with 2nd, 3rd and 4th harmonics and amplifies the signal-frequency range in between these harmonics. The frequency characteristic of this filter is not flat. The Inverse Notch Filter module has an inverted frequency characteristic. The combination of the CleanWave and the Inverse Notch Filter module gives a flat frequency characteristic while preserving the higher resolution in the analog-to digital conversion process. Additionally the Inverse Notch Filter has the option to block the RF carrier and its higher harmonics, similar to the Harmonics filter tuned to 13.56 MHz and a window of 2%.

XTalClear

The XTalClear filter is designed to filter all the external clock sub- and higher harmonics that appear in the power or EM frequency spectrum without the need to define them. It searches for all the peaks in the spectrum with a maximum frequency band width and a minimum peak level relative to the background level, and filters out those frequencies from the input traces. This module requires as input an averaged frequency spectrum, which can be generated by the Spectrum and Average modules.

Cross correlation

This module helps to visualize correlation between samples in a trace set. The module considers the input trace set as a matrix where each column represents the same sample in different traces, so It is important that the traces are well aligned. Subsequently, correlation coefficients are computed between all pairs of columns. These correlation coefficients are represented in a square matrix, where the value corresponds to the intensity of the representing dots. A positive correlation is shown in green, and a negative correlation is shown in red.

Pattern match

This module compares different segments within the traces and look for similarities. It can be used to search for repetitive patterns within a long operation, such as repeated rounds in block cipher computation or squares and multiplies in RSA exponentiation. The result of this module is especially useful for Pattern extract module.

Pattern extract

This module performs pattern match as the Pattern match module does, and in addition it extracts the matching patterns and forms a new trace set. This process is especially useful as a preparation step prior to attacks on RSA and ECC, or on block ciphers with dummy rounds as countermeasures.

Template attacks

POI selection

This module is used to select samples in traces that are likely to give the best result for differential side-channel analysis and in particular DPA-like Template attacks. These samples are typically referred to as points of interest (POI). The module selects POI by analyzing the traces based on statistical tests over the leakage models input by the user, and choosing samples in traces that give the best statistical test results.

TA DPA Known key

The concept of DPA-like template attack is similar to DPA. It aims to find the key of a cipher by exploiting the leakage of an intermediate result which is dependent on the key and a known variable. For example, exploiting the leakage of the first-round S-box output of an AES encryption in order to recover the first round key.

In this type of Template attacks, the templates are built for the intermediate result during the Learn (a.k.a. profiling) phase. During the Apply (a.k.a. exploitation) phase, the templates are used to validate the hypothetical intermediate values predicted based on all possible values for the key, and thereby differentiate the correct key hypothesis from the others.

TA DPA unknown key

This module works similar compared to template analysis with a known key with the exception that the key in this case is not known.

TA key loading known key

This module can be used to perform key loading type of Template attacks. In such an SPA-like attack, the leakage of the target e.g. keys is exploited directly as opposed to DPA-like attacks where the leakage being exploited is from a key-dependent intermediates value. The typically targeted operations for this attack include transfer of the key between memories or registers, hence the name -- key loading Template attacks.

During the Learn (a.k.a. profiling) phase, the templates are built for every possible value of the targeted key; during the Apply (a.k.a. exploitation) phase, the templates are applied to the corresponding key hypotheses in order to differentiate the correct hypothesis from the rest. Traces for the Learn phase must be for different key values so that templates can be built for all possible key values. The value of the key must be written into the data field of the trace for every trace during the Learn phase. The module builds templates for the data it reads from the data field and is unware of the cipher which the targeted key is for.

TA key loading unknown key

This module works similar compared to template analysis with a known key with the exception that the key in this case is not known.

TA DES key scheduling known key

This module can be used to perform DES Key Scheduling Template Analysis, it is based on the paper (pending publication) by Mathias Wagner. In this attack, leakages in the DES key scheduling function are exploited to recover the key. These XOR operations are grouped together in rings with a total length of 56 bits, so that almost all key bits may be recovered. The module can only be applied to DES, Triple DES is not supported.

During the Learn (a.k.a. profiling) phase, the templates are built for every possible value of a subset of the ring; during the Apply (a.k.a. exploitation) phase, the best matching templates are used to determine how much key entropy is left. The traces for the Learn phase must be for different random keys so that templates can be built for all possible key values.

Visualize templates

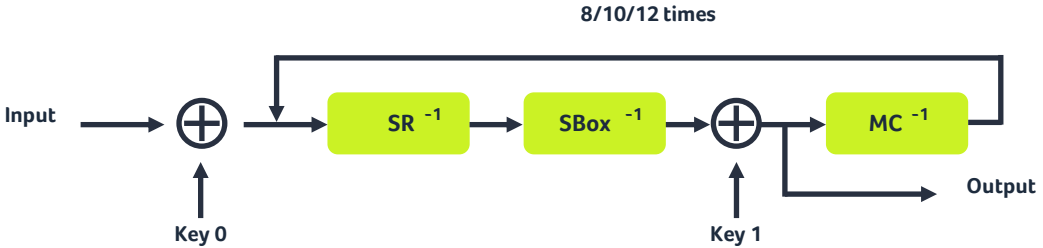
This module is used to visualize templates as generated and stored by the template analysis modules during the learn phase of a template attack. This applies to all types of Template attacks: DPA-Like Template Analysis Known Key, Key Loading Template Analysis Known Key and key scheduling Template analysis. The module return textual outputs and optionally traces representing the templates.

AES

AES chosen input FOA

This module targets a particular type of chosen-input side channel attack on AES, where the output of the MixColumns (or the inverse MixColumns) of an encryption (respectively decryption) is exploited to recover the first round key. This attack is in particular inspired by a hardware design of AES implementation as illustrated in the diagram on the right (decryption).

In this design, the output of the inverse MixColumns are written into a register, which previously contains either the result of the first AddRoundKey (only for the first round) or the output of the inverse MixColumns from the previous round. This write may cause the value of the inverse MixColumns, and/or the XOR of the first AddRoundKey output and the first inverse MixColumns output, to leak through side channels. Since these intermediate values depend on the first round key, their leakages may be used in Side Channel Analysis to recover the first round key.



AES chosen input known key analysis

Perform DPA on AES-128 decryption with chosen input data. The attack targets hardware AES implementations where the leakage lies in the first inverse MixColumns operation, which can only be exploited with partial constant input data. The module requires the key to be known for testing purposes.

AES second order analysis

To investigate a masked AES (Advanced Encryption Standard) implementation's susceptibility to second order side channel analysis. The module can work with different key and block sizes

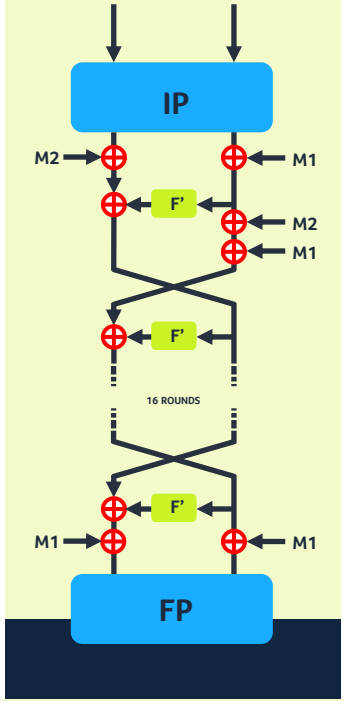
DES

DES masked input analysis

The standard Inspector DES modules assume the analyst knows the full plain text. This module is for use in situations where part of the plain text is unknown, for example when the input is an XOR of known data and partially unknown data. The attack targets four rounds of DES and retrieves both the input and key.

DES partly constant analysis

The standard Inspector DES modules assume the analyst has full control over the plain text and can make it random. This module is for use in situations where the full plain text is known, but part of it is constant (for example, with DES in counter mode), causing the usual correlation attack to fail. How many and which inputs bits are constant is variable: the module assumes only that the analyst knows the full input and has stored it as the first 8 bytes of data with each trace.
The module normally runs twice: the first run determines which input bits are constant and also their values, and performs standard DPA on 1st round S-boxes with 3 or more varying inputs. The second run performs DPA on 2nd round S-boxes, using hypotheses built from the constant bits and key candidates supplied by the 1st run and bit functions for the rest, resulting in a correlation list of function choices for each 2nd round S-box. These and the 1st run results are then used to calculate possible key values.



DES second order analysis

The DesSecondOrderAnalysis module provides a basis for second order differential side channel analysis experiments on DES to retrieve a DES key used in a masked implementation. The module extends Advanced Differential Analysis The masking scheme of a single round is represented in the image on the left.

The module operates by trying to guess the XOR-ed value of the R input of two consecutive rounds. Since both of the inputs are XOR-ed with the same mask M1, the result of their XOR will remove the mask. A drawback of this method is that any R byte is influenced by all of the S-Boxes, therefore since the module still tries to guess one sub key at a time, the resulting noise will be higher, thus requiring a higher amount of traces to yield the same results as the first order DES Analysis module on non-masked implementations.

RSA

RSA binary exponentiation analysis

This module can be used to perform attack on conventional bit-wise exponentiation in RSA. Both left-to-right and right-to-left exponentiation can be targeted.. The analysis method must be invoked repeatedly to retrieve the exponent bit by bit. For long RSA keys this method is not very efficient, but it may be serve well for proving the principle of RSA key extraction. At each round a comparison is made between a square and a multiply operation, and depending on the correlation results the key exponent is updated with a zero or one. The most likely operation is determined by comparing correlation values of two different intermediate data values, whose occurrence is dependent on the actual exponent.

RSA correlation

With this module the exponentiation scheme used for a specific implementation of the RSA algorithm can be explored, for example binary exponentiation or k-ary exponentiation. The analysis method can serve to demonstrate side channel leakage of an RSA implementation. The resulting traces show the correlation computed between the hamming weights of the bits for each unit with the samples.

RSA high order analysis

Perform attacks on k-ary exponentiation in RSA by cross-correlating different segments of side channel traces. The module detects the multiplier used in each round and retrieves the private exponent.

RSA neighbor correlation analysis

With this module recovering the private exponent used in a binary exponentiation implementation of the RSA algorithm by doing cross correlation is possible. This could be used to verify if a vulnerable 'multiply-always' implementation is used. In this case adjacent multiply and square operations would share an argument if the multiply result was discarded. Shared operands may result in detectable correlation.

Miscellaneous

ECC byte – multiply analysis

Perform DPA on ECC signature algorithms, such as ECDSA and ECNR, where the first part of the output signature is multiplied by the private key to obtain the second part of the signature. This module assumes that the multiplication is performed byte-wise and retrieves the private key using differential analysis on the multiplication.

ECNR partial nonce analysis

ECNR partial nonce analysis implements private key recovery using partially known nonces extracted from an ECNR signature implementation. The partial nonces in each trace represent the most significant bits of the nonce as used in the calculation of the ECNR signature. This module must be used in the final phase of an SPA attack on the ECNR signature scheme.

SEED analysis

The Seed Analysis module provides a basis for sophisticated differential side channel analysis experiments on SEED, a symmetric encryption algorithm used in Korea. The module extends Advanced Differential Analysis.

FI professional

Modules

Perturbation voltage/clock

The "Perturbation, Voltage/Clock" module offers three categories:

• Smart Card modules
The module "SC Perturbation" performs a glitch attack after sending the APDU command to the card. The goal is to influence the process triggered by the command, for instance a cryptographic operation. When the response of the card does not match the expected output (either a wrong crypto result or an abnormal status word) it is considered a successful perturbation attempt.

The module "SC Perturbation after reset" aims at the initialization phase of the target. The smart card will always send an Answer-To-Reset (ATR) message. When a voltage or
clock glitch is successful it can cause the target to release more data than the ATR message.
These two modules work with the standard behaviour of the VC Glitcher, in combination with the GUI.
The module "SC Perturbation with Glitch Program" is used when more detailed control is required. The user can write a custom glitch program, where for example multiple glitches based on the actual timing of the device can be specified.
The module "SC Perturbation after RST with Glitch Program" is a combination of the previous two.

• Embedded modules
There are two system modules shipped with Inspector that support embedded targets:
The "EP Perturbation" performs a glitch at a certain moment after sending the command to the target device.

The module named "EP Perturbation after Reset" performs an attack at the start-up stage of the target. After the reset line is asserted an embedded device will typically send a boot sequence message to indicate its status. This module enables the user to perform a glitch attack on this initialization stage.

• Advanced modules
Just like in the smart card category the embedded category offers the user has the option to specify a custom glitch program for the VC Glitcher.

Perturbation XYZ single

Apart from VCC/clock glitching, which works via the power/clock line, fault injection can also be applied via an electromagnetic or laser pulse. This type of fault injection has the advantage that it can be applied locally on a die; the disadvantage is that finding "the right spot" requires testing a wide range of locations. Currently, Inspector ships with two XYZ devices: The EM Probe Station for EM-FI (and EM Acquisition), and the Laser Station for optical perturbation. The Inspector UI is transparent for the actual XYZ device, meaning that EM-FI and laser glitching can be performed using this module.

Perturbation XYZ double

The XYZ double module offers the same functionality as the XYZ single module with the addition that two laser sources can be controlled instead of one. This function is used to control multiple laser sources in combination with the Twin Scan add on for the Laser Station II.

Differential fault analysis

DES DFA

To recover a DES key by analyzing fault-injected outputs this module can be used. This module performs a Differential Fault Analysis on a trace set using output data to retrieve the key. For the attack to work, at least one trace must contain the original, not fault-injected DES output, while the other traces must contain the same input with an injected fault.

AES DFA

This module performs a Differential Fault Analysis on a trace set using output data to retrieve the key. For the attack to work, at least one trace must contain the original, not fault-injected AES output, while the other traces must contain the same input with an injected fault.

RSA CRT DFA

Being able to recover a RSA private key by analyzing fault-injected outputs, this module performs a Differential Fault Analysis on a trace set targeting the re-combination step to retrieve private primes. For the attack to work, at least one trace must contain the original, not fault-injected RSA output, while the other traces must contain the same input with an injected fault.

Import traces

Import a trace set from a text file in comma-separated format, produced by the CRI tool DPAWS or from a Version 5 Mat-file compliant .mat file.

XY average plot

The Average plot module can be used to analyze spatially obtained measurements. It plots for each spatial measurement the average value of the samples of the selected samples. An example application is visualizing a chip surface by stimulating different locations with a laser pulse. The chip's power usage is affected differently depending on the location. A trace set with power measurements can be input to this module

Unique data

UniqueData is used to visualize different data responses of an optical FI log on the XY plane. This module is used in combination with the XY average plot to visualize the XY scan.

riscure

Please contact Riscure for more information
You can reach us by email : inforequest@riscure.com,
by phone : +31 15 251 4090 US: +1 650 646 9979
Or on the web: riscure.com.