INTEGRATED CIRCUIT INVESTIGATION METHOD AND APPARATUS

The present invention relates to a method and apparatus for use to investigate integrated circuit chips (ICs) to discover and/or recover their hidden or lost content. It also relates to investigation and/or presence detection of mechanisms, algorithms and keys which may be held within the IC and which may be deliberately hidden or which may have been lost.

Software is often provided within ICs. While conventionally programmed software in a processor is potentially available for investigation and analysis by scrutiny of the memory in the processor while the processor has the software loaded. When provided within an IC, software is hidden. This is particularly true of encoding and encryption keys and processes. Because of their nature, black box analysis of encryption processes and discovery of keys takes prohibitively long. While governments hold copies of approved encryption keys, there is no practical reason why an individual or organization should not create their own encryption keys which can be embodied in an algorithm on an IC, rendering communications by the individual or organization effectively hidden. It is an aim of the present invention to render investigation of IC keys and data more effective.

The usual way to investigate an IC is by provision of test input instructions and data and by observation of resultant outputs. ICs are now very complex. They can comprise one or more processors operable to perform different tasks based on internally held software. Different processes can be called up by providing different instructions. It is a problem to know when a particular behavior or process has been evoked. The present invention seeks to make detection of IC behavior less uncertain.

Investigation of ICs can involve simultaneous collection of much data and information or subsequent analysis. Plural streams of data and information must be stored and analyzed to provide any hope of successful investigation. It is another aim of the present invention to simplify collection and analysis of simultaneous data and information streams derived from IC investigation.

It is well known to test an IC as art of the overall fabrication process. United States Patent US-B1-7191368 discloses a unitary tester for testing both analog, memory and digital circuits in an IC by injection of appropriate test signals and scrutiny of the resultant outputs. US Patent US-4807161 discloses functional testing of electronic circuits employing a microprocessor in overall control. US Patent Application 2009/0240452-A1 discloses using a coil external to a circuit under test to determine in different stages of fabrication whether the circuit behaves as expected. All of the above documents discloses testing of circuits whose characteristics are known, with

the aim of determining if the circuit is properly working. The present invention is employed to investigate ICs some or all of whose characteristics are unknown. Another aim of the present invention is to enable assessment and analysis of ICs whose characteristics are either unknown or only partly known.

According to a first aspect, the present invention consists in an apparatus for investigating the content of a device under test, the apparatus comprising: means to apply selectable test signals to the device under test; means to receive result signals from the device under test, generated by the device under test in response to application of the selected test signals; one or more analogue sensors, operable to sense analogue qualities of the device under test with the test signals applied thereto, where each of the one or more analogue sensors is operable to provide a respective analogue output signal for each selected test signal; analogue signal analyzing means, operable to analyze the one or more analogue output signals; and test signal modification means, operable to change the selected test signal in response to the analogue signal analysis.

According to a second aspect, the present invention consists in a method for investigating the content of a device under test, the method comprising the steps of: a step of applying selectable test signals to the device under test; a step of receiving result signals from the device under test, generated by the device under test in response to application of the selected test signals; a step of applying one or more analogue sensors to sense analogue qualities of the device under test with the test signals applied thereto, each of the one or more analogue sensors is providing a respective analogue output signal for each selected test signal; a step of analyzing the one or more analogue output signals; and a step of changing the selected test signal in response to the analogue signal analysis.

The invention further provides that the means to apply test signals can successively select and apply different test signals to the device under test, that each selected test signal can be applied for a sampling period, and that the analog signal analyzing means can compare the one or more analogue signals obtained when a first test signal is applied in a first sampling period with the corresponding one or more analogue signals obtained when a previous test signal was applied.

The invention also provides that the analog signal analyzing means can provide, as output, the difference between the one or more analogue signals obtained when a first test signal is applied and the corresponding one or more analogue signals obtained when the previous test signal in the sequence of test signals was applied, and that the previous test signal can be the next previous test signal.

The invention also provides that the one or more analogue sensors can give possible indication of at least one of: the state of the device under test; and changes in type of activity.

The invention also provides that the analogue output signals, from the one or more analogue sensors, can be provided as input to an analogue signal pipeline, and that the output of the analogue signal pipeline can be provided as input to the analogue signal analyzing means.

The invention further provides that the one or more analogue sensors can sense at least one of: timing variation; heat dissipation; temperature; electrical noise, electromagnetic emission, power consumption; and optical or photon emission.
The invention also provides that some or all of the sensing and processing elements of the apparatus can be integrated and embedded in one or more co-operative semiconductor integrated circuits.

It is a further aim of the invention to provide improved measurement of a response from an integrated circuit device under test (DUT 26) by performing analysis on analog signals acquired with measurement probes. That allows significant improvement over existing measurement equipment such as oscilloscopes both in the speed and precision.

The invention is further described and explained, by way of example by the following description, to be read in conjunction with the appended drawings, in which:

Figure 1 is a block diagram showing exemplary constituent parts of the present invention.

Figure 2 is a block diagram of exemplary contents of the device under test module.

Figure 3 is a flow chart illustrating operation of the waveform analyzer.

Figure 4 is a schematic block diagram showing the hardware interface of Figure 1 in greater detail.

Figure 5 is a schematic block diagram of an exemplary integrated circuit implementation of elements of Figure 1.

and

Figure 6 and Figure 7 together show details of the device under test module of Figure 2.

Attention is first drawn to Figure 1, a block diagram showing constituent parts of the present invention, intended to test an IC as a “device under test” (DUT) 26.

An IC investigation apparatus 10 where an IC can be a DUT 26, is controlled by a processor 12 which, in this example, is provided in the form of a personal computer but which may equally be provided in the form of any other computing device capable of performing the same or similar function, having a control interface that can be represented by a personal computer, remote control with embedded processor or other human interface.

The processor 12 provides instructions to and receives data and feedback from a hardware interface 14. The hardware interface 14 comprises a counter 16 which works with a test algorithm store 18 to provide settings and switching for an AC and DC power supply 20 and patterns and instructions (such as clock rate) to a periodic test signal generator 22. The test signal generator 22 produces sets of test patterns according to the programmed algorithm, the signals can be both analog and digital and determined by the DUT 26 specification. One part of the algorithm is fixed while the other is changing.

The test algorithm in the test algorithm store 18 is either present in the hardware interface 14, or can be provided by the processor 12. The processor can change at least part of the test algorithm in sympathy with DUT 26 investigative test results to better investigate the DUT 26 in light of what has been found out about the DUT 26 so far. Each DUT 26 requires its own test algorithm which is a part of a standard device operation and consists of a list of commands to run the DUT 26 in the way required by the tester, for example, to establish an authentication or to decrypt the data.

The power supply of the DUT 26 is provided by the programmable power supply 20 which can produce both DC and AC power sources. The clock of the AC source can be synchronized to the external clock provided by the test signal generator 22 which in turn can be synchronised to the DUT’s internal clock. This is done by injecting the clock signal from the generator 22 into the DUT 26 power supply line. That allows significant improvement over existing measurement equipment setup by significantly reducing the jitter influence on the measurement results.

A device under test module 24 contains the IC which is the Device Under Test (DUT) 26. The power supply 20 provides the DUT 26 with appropriate power supply levels set by the hardware interface 14 and the test signal generator 22 provides the DUT 26 with digital (and optionally, analog) test signals, also under control of the hardware interface 14.

Pins on the DUT 26 are electrically connected in the usual way and signals from individual pins are externalized for recording and analysis. The device under test module also contains numerous analog sensors, described hereafter, used to sense parameters and operational responses in the DUT 26. The outputs of the analog sensors are also externalized. As the DUT 26 performs some requested operation, it leaks some information via side channels. A side-channel is an information emitted as a side effect of the DUT 26 operation. This includes but is not limited to time variations, heat dissipation, noise, electromagnetic emission, power consumption and optical emission. The side-channel responses are measured with dedicated sensors specific for each type of side-channel emission.

Externalized outputs from the device under test module 24 are provided in common to a device response measurement module 28 which accepts plural externalized outputs as plural results 30 and passes the plural results 30 through a plural result signal conditioning module 32 which improves and conditions the plural results 30. The sensors output the signals in analog form which then put through plural results signal conditioning module 32 to amplify the signal or signals and to reduce the noise by applying various filters.

The plural results signal conditioning module 32 provides input to an analog signal pipeline 34 whose data are delayed by one clock period, the clock period being determined by the test signal generator 22. The purpose of the delay is to be able to compare the device side-channel response to different input test data. When the DUT 26 is supplied with test command it performs some operations and the result is leaked through side-channels. Each period the data sent to the device is different; hence there are differences in the side-channel measurements. Characteristic points in the side-channel signal are chosen and the side channel signal is delayed by one period in the pipeline 34.

The pipeline 34 delivers its delayed output to a waveform analyzer 36 which compares the new signal with the delayed signal for the determined number of points and provides an output which is the difference there between. The waveform analyzer 36 then provides the analyzed difference analogue signals to an analyzer output signal conditioner 38 which uses amplifiers and filters to meet the requirement of the acquisition system. The analyzer output signal conditioner 38 provides its inputs to multiplexer and analogue to digital converter 40 which then converts the multiplexer and analogue to digital converter in multiplexed way into digital form.

The output of the multiplexer and analogue to digital converter 40 is then transferred to the hardware interface 14 and then digitized for later analysis. A response

analyzer 42 analyzes the digitized difference result data and produces an overall result which is stored in a status register 44 which is accessible by the processor 12 and/or by the hardware interface 14. The response analyzer 42 makes the decision on the reply based on the predetermined decision making patterns and updates the status register 44. The result of the response analysis influences the next value of data being sent to the DUT 26.

Attention is next drawn to Figure 2, a block diagram illustrating exemplary contents of the device under test module 24.

The device under test module 24 contains the device under test 26 together with a plurality of analog sensors 46 each sensing a different quality of the DUT 26 and each contributing an output to the plural results lines 30.

In the device under test module 24, the DUT 26 may have its external casing stripped, removed or otherwise opened, the better for the analogue sensors 46 to detect conditions in the DUT 26.

Changes in the analog signals 30 can be indicative of the DUT 26 having different functional activities in response to different test signal inputs. This can be of use in discovering potential ways to extract software or data securely contained within a chip. The actual extraction will be done using digital signals, but the analog signals provide clues as to what is going on in the chip. For example, a chip may contain an encryption key which requires to be known in order to decrypt messages or files.

The analog sensors 46 are arrayed in, on and around the DUT 26. They can sense all manner of things. One sensor can sense chip temperature. Another sensor might sense Radio Frequency (RF) noise generated by the chip. Yet another sensor might sense chip feed current power line ripple. Yet another sensor might be an electromagnetic emission sensor. Yet another sensor might sense signals given off by an internal chip clock. Another sensor might be a photon detector/camera for viewing the die of the chip. There is really no limit to the sensors that can be employed. As new approaches are discovered, an appropriate sensor can be added to the one or more analog sensors monitoring the DUT 26 for signals that “leak out” as the DUT operates.

The DUT 26 also has electrical inputs 48 through which it receives power supplies from the programmable AC and DC power supply 20 and test signals from the test signal generator 22. The electrical inputs 48 attached to different pins on the DUT 26, which pins are selected being dependent upon the type of the DUT 26.

The DUT 26 also has electrical outputs 50 communicating digital response signals generated in response to the test signals from the test signal generator 22. The electrical outputs 50 are also attached to different pins on the DUT 26, which pins are selected being dependent upon the type of the DUT 26. The electrical outputs are connected, for example, back to the hardware interface (as shown in Figure 1) for analysis.

Attention is next drawn to Figure 3, a flow chart illustrating operation of the waveform analyzer 36. The waveform analyzer 36 simultaneously performs the same operation for each of the plural results 30 signals, though only one channel is shown in Figure 3.

A first function 52 accepts the incoming signal from the analogue signal pipeline 34. A second function 54 then subtracts the previous analog value from the incoming analog value and a third function 56 outputs the difference between the incoming and previous analog signals to the analyzer output signal conditioner 38.

The skilled man will be aware of different ways in which the functions 52 54 56 of the waveform analyzer 36 can be implemented using electronic hardware utilizing switching signals to replace the previous signal of Figure 3 with the incoming signal of Figure 3 in readiness for receiving the next incoming signal.

An example of operation of the apparatus will now be given.

A DUT 26 requires to be evaluated for information leakage. The DUT 26, for example, performs cryptographic operation using key stored inside without any access to the cryptographic key. From freely available documentation it is known, for example, that in order to force the DUT 26 into cryptographic operation it is necessary first to initialize the DUT 26. After initialization, as many data packets as are desired can be sent to the DUT 26 for encryption.

The hardware interface first powers up the DUT 26 according to the specification, then sends some initialization data to the DUT 26. The hardware interface 14 waits for reply and compares the reply with an error condition. Then the hardware interface 14 starts sending packets consisting of a command followed by some predefined data, and waits for reply from the DUT 26. The data value is determined by software running on a controller 12. The data values are different for each period of test. What value to send next time will depend on the response received from the response analyzer according to the algorithm stored in the hardware interface module 14 with possibility to be configured by the processor 12 through parametric tables, embedded software or FPGA configuration.

In the DUT 26, once the DUT 26 receives the command followed by data, it starts internal computation process. There is no activity on the DUT 26 interface wires during that time. However, the DUT 26 will leak information about its internal processes via side channels such as variable power consumption, electromagnetic emissions, optical emissions, acoustic waves, mechanical vibration etc. These leakages can be determined by the analog sensors 46 and converted into electrical signals 30 forming device response measurement setup. The signal from each analog sensor 46 is then conditioned in order to comply with the analog part of the measurement system. This involves amplification, offsetting, noise reduction, filtering etc. The resulted signal is then delayed for exactly one period to be compared with the signal received from the same DUT 26 operation but with different data. During the execution of the operation, the test signal generator 22 controls the time when the signals must be compared inside the waveform analyser 36. The result of the comparison is then conditioned to comply with the analog-to-digital converter requirements and sent back to the hardware interface 14 where the response analyzer 42 makes a decision about the result and sends it to the algorithm part to form the next set of data.

Different arrangements are possible within the invention. The plural analogue data 30 signals can each be digitized at an early stage in their movement towards the waveform analyzer 36, and the digitized analogue data, instead of being moved along an analogue signal pipeline 34, moved instead along a first in first out process, or stored in successive locations in a memory store, for digital access by the waveform analyzer 36. The waveform analyzer 36, instead of comparing the incoming result signals 30 from the one or more analogue sensors 46 with the previously provided result signal 30, can make a comparison between two, and between any number of different result signals 30. Instead of merely passing on as output the differences between successively provided analogue sensor 46 result signals 30, the waveform analyzer 36 can provide, as output, any one or any combination of mathematical functions derived from any two or more of the result signals 30 derived from the analogue sensors 46. The analogue signal pipeline 34 also can be replaced by one or more successive analogue delay lines, or by any digital emulating process such as one or more bucket brigade devices.

Attention is next drawn to Figure 4, a schematic block diagram showing the hardware interface 14 of Figure 1 in greater detail.

In all figures that follow, each arrow is numbered with the number of the element of the apparatus to which it goes or from whence is originates.

The external control processor 12 has full access to all parts of the hardware interface 14 for updating test algorithms in the test algorithm store 18, for configuring the response analyzer 42, for presetting counters 16 and reading/resetting status registers 44. The test algorithm 18 can be implemented in logic, or can be implemented as software in

microcontroller, or a Field Programmable Gate Array (FPGA) design. The response analyzer 42 looks at particular parameters in the data received from the A/D converter 40 and stores the result in status register or registers 58 as needed, and it also passes the results to the test algorithm 18 and to individual counters 16' so that the next set of data and test signal sequence can be generated. According to the test algorithm 18, the control signals for the power supply 20 and periodic signal generator 22 are sent before each test cycle.

Attention is next drawn to Figure 5, a schematic block diagram of an exemplary integrated circuit implementation of elements of Figure 1.

A signal is picked up from one or more analog sensors 46 placed proximately to the device under test 26 in the device under test module 24. Then signal from each sensor 46 is amplified by an individual amplifier 60 to the required level and filtered by an individual filter 62 to reduce the noise. The amplification level and filter parameters are set through a logic interface 64. Each signal then travels within an individual pipeline delay line 66 with multiple outputs. The delay time for each output is controlled by the logic interface 64. All resulted signals are then fed into multiplexer 68 which allows any combination of the input signal to be sent to one or more comparators 70. The parameters of the comparators 70 are controlled by the logic interface 64. Then the output of each comparator 70 is filtered by a respective final filter 72 according to the settings from the logic interface 64. If necessary, the output can be sent via a further multiplexed 74 to reduce the number of pins.

The invention includes a variant implementation of elements of Figure 1, as one or more silicon integrated circuits, the variant not being shown in Figure 5, the variant including the setup of Figure 5, with one ore more additional embedded analog-to-digital converters after the output of further multiplexer 74.

The invention includes yet another variant implementation which has the logic interface 64 of Figure 5 replaced by an embedded microcontroller with standard external interface or I/O pins. An embedded analog-to-digital converter after the output further multiplexer 74 also be connected to that microcontroller.

The invention also includes another variant implementation where the logic interface 64 of Figure 5 is replaced with an embedded FPGA array with optional a hardware microcontroller and standard external interface or I/O pins. One or more embedded analog-to-digital converters provided after the output further multiplexer 74 can be included and connected to the embedded FPGA. Within the invention, the embedded microcontroller or FPGA can be used to produce the part or full of the test algorithm and the embedded microcontroller or FPGA can be used to replace the hardware interface 14 of the apparatus.

Attention is next drawn to Figures 6 and Figure 7, together showing extra details of the device under test module 24 of Figure 2. The device under test (DUT) 26 is shown in Figure 7 as a die 75 wherefrom the casing has been removed so that optical and infrared emissions can be observed and measured.

For power analysis a current measuring device 76 is used, which can be a simple resistor in the power supply or ground line or can be a more sophisticated sensor. For electro-magnetic analysis H-field 78, E-field 80 or RF antenna sensors 82 can be used with pre-amplifiers 84 and demodulator 86 if necessary. For mechanical emission an ultrasonic sensor 88 can be used with a pre-amplifier 84 and demodulator 86 if necessary. Optical emission, as shown in Figure 7, can be sensed with photo-sensor 90 and pre-amplifier 84 and/or with an infrared camera 92 and an image processing device 94.

The invention can also operate in synchronous mode. By synchronizing the test signal generator 22 with internal DUT 26 signals, the sensitivity of the apparatus in much enhanced. In this example, one or more signals received by the result signal conditioning module 32 are coupled as synchronizing input to the test signal generator 22 to provide enhanced operation.

The invention has been described with reference to extracting data and codes from a DUT 26. The invention forms a very sensitive device which can also be applied to many other applications. For example, whenever there is a need to compare two signals, or whenever it is required to monitor something periodically and to raise an alarm whenever something changes, the invention is applicable. Such tasks can be achieved, at poor resolution, using an oscilloscope, but most oscilloscopes have only something like 6-7 bits (binary digits) of resolution plus high noise. In such situations great precision and resolution are required. By applying the present invention in these circumstances, a resolution of up to 20 bits is possible. As just one example, GPS (Global Positioning by Satellite) signals are very weak and, in previously known applications, have to be averaged over many cycle periods to achieve a reliable and reasonably precise accuracy. If instead, the present invention is applied, and the periodic signals are dealt with precisely synchronizing each waveform, faster and higher precision results are possible.

As a variant over the examples shown and described, the invention also offers the capacity to pipeline multiple signals in multiple pipelines as well as capacity to pipeline the same signal in different pipelines. The example shown and described shows only one manner of pipeline organization, and all possible pipeline configurations are possible and contained within the invention.

The invention has also been described with various examples. It is to be appreciated that

the foregoing examples are not exhaustive, that they may be applied singly or collectively within the invention, and in all combinations, and that many other variants, which can be applied within the invention, which are included in the invention, will be known to those skilled in the art.

The invention is further clarified by the following Claims.

Claims.

1. An apparatus for investigating the content of a device under test, the apparatus comprising:

means to apply selectable test signals to the device under test;

means to receive result signals from the device under test, generated by the device under test in response to application of the selected test signals;

one or more analogue sensors, operable to sense analogue qualities of the device under test with the test signals applied thereto, where each of the one or more analogue sensors is operable to provide a respective analogue output signal for each selected test signal;

analogue signal analyzing means, operable to analyze the one or more analogue output signals; and

test signal modification means, operable to change the selected test signal in response to the analogue signal analysis.

2. An apparatus, according to Claim 1, wherein:

the means to apply test signals is operable to successively select and apply different test signals to the device under test, each selected test signal being applied for a sampling period;

wherein

the analog signal analyzing means is operable to compare the one or more analogue signals obtained when a first test signal is applied in a first sampling period with the corresponding one or more analogue signals obtained when a previous test signal was applied.

3. The apparatus, according to Claim 2, wherein the analog signal analyzing means is operable to provide, as output, the difference between the one or more analogue signals obtained when a first test signal is applied and the corresponding one or more analogue signals obtained when the previous test signal in the sequence of test signals was applied.

4. The apparatus according to Claim 2 or Claim 3 wherein the previous test signal is the next previous test signal.

5. The apparatus, according to any of the preceding claims, wherein the one or more analogue sensors are operable to give possible indication of at least one of: the state of the device under test; and changes in type of activity.

6. The apparatus, according to any of the claims 2 to 5, wherein the analogue output signals, from the one or more analogue sensors, are provided as input to an analogue signal pipeline, output of the analogue signal pipeline being provided as input to the analogue signal analyzing means.

7. The apparatus, according to any of the preceding claims, wherein the one or more analogue sensors are operable to sense at least one of: mechanical vibration; timing variation; heat dissipation; temperature; electrical noise, electromagnetic emission, power consumption; and optical or photon emission.

8. The apparatus, according to any of the preceding Claims, comprising means to synchronize the means to apply selectable test signals to the device under test with one or more signals derived from the device under test.

9. A method for investigating the content of a device under test, the method comprising the steps of:

a step of applying selectable test signals to the device under test;

a step of receiving result signals from the device under test, generated by the device under test in response to application of the selected test signals;

a step of applying one or more analogue sensors to sense analogue qualities of the device under test with the test signals applied thereto, each of the one or more analogue sensors is providing a respective analogue output signal for each selected test signal;

a step of analyzing the one or more analogue output signals; and

a step of changing the selected test signal in response to the analogue signal analysis.

10. A method, according to Claim 9, wherein:

the step of applying test signals includes successively selecting and applying different test signals to the device under test, and applying each selected test signal for a sampling period;

and

the step of step of analyzing the one or more analogue output signals includes comparing the one or more analogue signals obtained when a first test signal is applied in a first sampling period with the corresponding one or more analogue signals obtained when a previous test signal was applied.

11. The method, according to Claim 10, wherein the step of analyzing the one or more analogue output signals includes providing, as output, the difference between the one or more analogue signals obtained when a first test signal is applied and the corresponding one or more analogue signals obtained when the previous test signal in the sequence of test signals was applied.

12. The method, according to Claim 10 or Claim 11, wherein the previous test signal is the next previous test signal.

13. The method, according to any of claims 8 to 11, wherein the one or more analogue sensors are employed to give possible indication of at least one of: the state of the device under test; and changes in type of activity.

14. The method, according to any of the claims 10 to 13, including providing the analogue output signals, from the one or more analogue sensors, as input to an analogue signal pipeline, and providing the output of the analogue signal pipeline as input for the step of analyzing the one or more analogue output signals.

15. The method, according to any of claims 9 to 14, wherein the one or more analogue sensors sense at least one of: mechanical vibration; timing variation; heat dissipation; temperature; electrical noise, electromagnetic emission, power consumption; and optical or photon emission.

16. The method, according to any of Claims 9 to 15, including the step of employing one or more signals derived from the device under test to synchronize test signals applied to the device under test.

17. An apparatus, according to any of Claims 1 to 8, wherein some or all of the sensing and processing elements are integrated and embedded in one or more co-operative semiconductor integrated circuits.

INTEGRATED CIRCUIT INVESTIGATION METHOD AND APPARATUS

Abstract

An apparatus 10 investigates the content of a device under test 26 (DUT) by applying successive sets of digital test signals 48, each for a sampling period, to the device under test 26 and receiving digital result signals 50 resulting from the applied test signals. Analogue sensors 46 are disposed proximate to the device under test 26 to measure, and to provide analogue output 30, indicative of qualities of the device under test 26 as the digital test signals 48 are applied for each sampling period. The analogue output signals 30 are analyzed in a waveform analyzer 36 between successive sampling periods to determine the difference between them. The difference is employed in deciding what next digital test signal 48 to apply. The analogue sensors 46 provide possible indication of the state of the device under test; and any changes in type of activity in the device under test 26. The analogue sensors 46 provide output 30 indicative of one, some or all of: mechanical vibration; timing variation; heat dissipation; temperature; electrical noise, electromagnetic emission, power consumption; and optical or photon emission: within the device under test 26. The apparatus can synchronize applied test signals with one or more signals derived from the device under test 26 to achieve enhanced sensitivity. Some or all of the sensing and controlling elements of the apparatus can be integrated and embedded within one or more co-operative semiconductor integrated circuits.

Figure 1