



(51) International Patent Classification:

G06F 21/75 (2013.01) G01R 19/00 (2006.01)

G01R 31/08 (2006.01) G01R 29/26 (2006.01)

H04L 9/00 (2006.01) G01R 19/165 (2006.01)

(21) International Application Number:

PCT/EP2019/060059

(22) International Filing Date:

18 April 2019 (18.04.2019)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

18386008.9 20 April 2018 (20.04.2018) EP

18386016.2 13 June 2018 (13.06.2018) EP

19386023.6 11 April 2019 (11.04.2019) EP

(71) Applicant: ARM LIMITED [GB/GB]; 110 Fulbourn Road, Cambridge CB1 9NJ (GB).

(72) Inventors: VINCENT, Hugo John Martin; 110 Fulbourn Road, Cambridge CB1 9NJ (GB). DAS, Shidhartha; 110 Fulbourn Road, Cambridge CB1 9NJ (GB). MERIAC, Milosch; 110 Fulbourn Road, Cambridge CB1 9NJ (GB). TENENTES, Vasileios; 110 Fulbourn Road, Cambridge CB1 9NJ (GB).

(74) Agent: TLIP LTD; 14 King Street, Leeds Yorkshire LS1 2HL (GB).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME,

(54) Title: DYNAMIC RESPONSE OF POWER DELIVERY NETWORK FOR ATTESTATION AND IDENTIFICATION

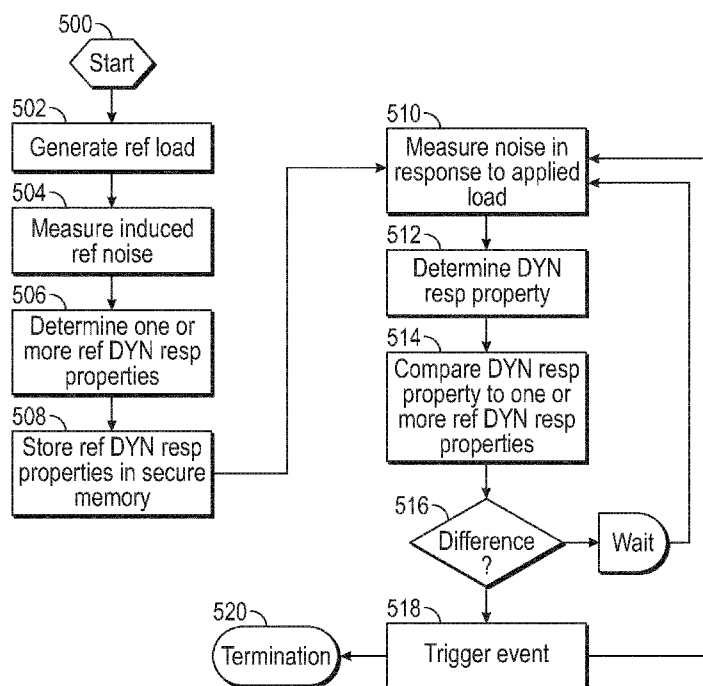


FIG. 5

(57) Abstract: A method and authenticator for authenticating a device in a system using the electrical properties of the device is disclosed. Embodiments of the disclosure enable authentication by receiving a plurality of input seed values from a requestor. For each input seed value, load stimuli a regenerated to produce an electrical load sequence on a power delivery network powering at least part of the system. Noise induced in the power delivery network is measured in response to the electrical load sequence using one or more sensors located on the power delivery network. Based on the measured noise, a dynamic response property (magnitude and phase response as a function of frequency) of the power delivery network corresponding to a respective input seed value can be determined and returned to the requestor.



MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,
SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

DYNAMIC RESPONSE OF POWER DELIVERY NETWORK FOR ATTESTATION AND IDENTIFICATION

[001] The present disclosure relates generally to hardware security, and more particularly,
5 to remote detection and mitigation of attempted non-invasive, semi-invasive, or invasive
tampering to a power delivery network.

[002] Various attacks on hardware pose an ever-increasing risk to security. One such attack
is differential power analysis, where oscilloscope probes are attached to power supply rails on
a printed circuit board (PCB) containing the victim system-on-chip (SoC). In this attack,
10 power supply decoupling capacitors are commonly removed to increase the signal to noise
ratio and/or frequency content of the power side channel leakage. Another such attack is
referred to as a fault injection attack, where a signal generator probe is attached to the power
rail (or AC coupled via any other package pin(s)) as a precursor to injecting faults.

[003] Further attacks might involve adding additional circuitry on PCB level/mainboard
15 level to circumvent security features or for backdooring devices – examples of such devices
have been mod-chips on contemporary gaming consoles, backdooring devices for server
mainboards or sniffer-devices added to Point-of Sales terminals (PoS) to intercept and relay
credit card information to remote attackers. Most of these circuits draw power from existing
power sources inside the device – and changing the dynamic response of the existing power
20 circuitry as a result. It's important to highlight that this influence can be visible even across
voltage regulator boundaries – albeit at a usually worse signal-response ratio. This means for
example that a processor might observe unexpected loads on an upstream voltage rail across a
voltage regulator (LDO) boundary – at the cost of power supply ripple rejection (PSSR) –
that can be commonly in the range of 40-70dB. This extends the reach of the present
25 disclosure beyond the immediately accessible power network and might allow peeking into
related power network (connected by linear regulators, DC/DC converters and similar
means).

[004] It would therefore be desirable to provide a novel apparatus and methodology for
remote attestation of the SoC to detect, if and when probes or malicious circuitry have been
30 attached or other affordances made, even before a fault is injected, a backdoor opened, an
internal information leaked or a side channel analysis conducted.

[005] The present disclosure is illustrated by way of example and not limited in the accompanying figures in which like reference numerals indicate similar elements and in which:

[006] **FIG. 1** is a high-level schematic diagram of an example shared power-delivery network (PDN);

[007] **FIG. 2** is a graph of the PDN input impedance (as seen from the die), as a function of frequency for the simplified PDN of **FIG. 1**;

[008] **FIG. 3** is a graph of current-step excitations that exercise the three prominent system resonance frequencies in the PDN;

[009] **FIG. 4** is a high-level block diagram of an example embodiment in accordance with the present disclosure;

[0010] **FIG. 5** is a flow diagram of a method for detecting a change in electrical properties in a system powered by a PDN in accordance with an embodiment of the present disclosure;

[0011] **FIG. 6** is a high-level schematic of an apparatus for implementing embodiments of the present disclosure;

[0012] **FIG. 7** is a flow diagram of a remote attestation method in accordance with an embodiment of the present disclosure;

[0013] **FIG. 8** is block diagram of a decimation step in accordance with an embodiment of the present disclosure;

[0014] **FIG. 9** is a timing diagram of a test load, sampling window, and sampled values of dynamic system load, respectively, in accordance with the attestation method of an embodiment of the present disclosure;

[0015] **FIG. 10** is a flow diagram for authenticating a device in a system using electrical properties in the system in accordance with a method of an embodiment of the present disclosure; and

[0016] **FIG. 11** is a high-level block diagram of an authenticator in accordance with an embodiment of the present disclosure.

[0017] Specific embodiments of the disclosure will now be described in detail regarding the accompanying figures. For simplicity and clarity of illustration, where considered

appropriate, reference numerals may be repeated among the figures to indicate corresponding or analogous elements. In addition, numerous specific details are set forth in order to provide a thorough understanding of the examples described herein. However, it will be understood

by those of ordinary skill in the art that the examples described herein may be practiced without these specific details. In other instances, well-known methods, procedures and components have not been described in detail so as not to obscure the examples described herein. Also, the description is not to be considered as limiting the scope of the examples described herein.

[0018] It will be appreciated that the examples and corresponding diagrams used herein are for illustrative purposes only. Different configurations and terminology can be used without departing from the principles expressed herein. For instance, components and modules can be added, deleted, modified, or arranged with differing connections without departing from these principles.

[0019] In the following detailed description of embodiments of the disclosure, numerous specific details are set forth in order to provide a more thorough understanding of the disclosure. However, it will be apparent to those skilled in the art that the disclosure may be practiced without these specific details. In other instances, well-known features have not been described in detail to avoid unnecessarily complicating the description.

[0020] It is to be understood that the terminology used herein is for the purposes of describing various embodiments in accordance with the present disclosure, and is not intended to be limiting. The terms “a” or “an,” as used herein, are defined as one or more than one. The term “plurality,” as used herein, is defined as two or more than two. The term “another,” as used herein, is defined as at least a second or more. The terms “including” and/or “having,” as used herein, are defined as comprising (i.e., open language). The term “coupled,” as used herein, is defined as connected, although not necessarily directly, and not necessarily mechanically. The term “providing” is defined herein in its broadest sense, e.g., bringing/coming into physical existence, making available, and/or supplying to someone or something, in whole or in multiple parts at once or over a period.

[0021] As used herein, the terms “about” or “approximately” apply to all numeric values, irrespective of whether these are explicitly indicated. Such terms generally refer to a range of numbers that one of skill in the art would consider equivalent to the recited values (i.e., having the same function or result). These terms may include numbers that are rounded to the nearest significant figure. In this document, any references to the term “longitudinal” should be understood to mean in a direction corresponding to an elongated direction of a personal computing device from one terminating end to an opposing terminating end.

[0022] In accordance with an embodiment of the present disclosure, there is provided a method for authenticating a device in a system using electrical properties in the system. The method includes: receiving, from a requestor, a plurality of input seed values; generating, for each input seed value, load stimuli to generate an electrical load sequence on a power delivery network powering at least part of the system, each electrical load sequence relating to at least one magnitude and phase component in a specific frequency band corresponding to a dynamic response of the system; measuring, using one or more sensors located on the power delivery network, noise induced in the power delivery network in response to the electrical load sequence; determining, based on the measured noise, a dynamic response property of the power delivery network corresponding to a respective input seed value; generating, from the dynamic response property of the power delivery network a plurality of authentication response values, each authentication response value relating to at least one magnitude and phase component in a specific frequency band corresponding to the measured dynamic response property; returning the authentication response values to the requestor; and at the requestor, comparing the authentication response values to known authentication response values to authenticate the device.

[0023] In accordance with another embodiment, there is provided an authenticator for authenticating a device in a system using electrical properties in the system. The authenticator includes: a processor operable to: receive, from a requestor, a plurality of input seed values; generate, for each input seed value, load stimuli for generating an electrical load sequence on a power delivery network powering at least part of the system, each electrical load sequence relating to at least one magnitude and phase component in a specific frequency band corresponding to a dynamic response of the system; receive data representing noise induced in the power delivery network in response to the electrical load sequence measured using one or more sensors located on the power delivery network; determine, based on the measured noise, a dynamic response property of the power delivery network corresponding to a respective input seed value; generate, from the dynamic response property of the power delivery network a plurality of authentication response values, each authentication response value relating to at least one magnitude and phase component in a specific frequency band corresponding to the measured dynamic response property; and return the dynamic response property of the power delivery network to the requestor, the requestor operable to compare

the authentication response values to known authentication response values to authenticate the device.

[0024] Referring to **FIG. 1**, there is depicted a high-level schematic diagram of an example power-delivery network (PDN) 100 composed of a die-package-printed circuit board (PCB) system. Such a die-package-printed circuit board is disclosed in S.Das, P.Whatmough, and D.Bull, “Modeling and characterization of the system-level power delivery network for a dual-core arm cortex-a57 cluster in 28nm cmos,” in 2015 IEEE/ACM International Symp. on Low Power Electronics and Design (ISLPED), July 2015, the content of which is incorporated by reference herein in its entirety. The die-package-PCB system is generally depicted and includes a die (chip) 102, package 104 and PCB 106. A plurality of die switching transistors on the die are lumped together and modeled as a current source, I_{die} . Explicit on-die decoupling capacitors and non-switching transistors act as local charge reservoirs that are modeled by a capacitor, C_{die} . The power-line traces on the package and board are represented using R-L networks. Discrete decoupling capacitors (referred to as decaps) on the package (C_{PKG}) and the bulk capacitors on the PCB (C_{BULK}) are modeled by capacitors in series with their effective series resistance (ESR) and inductance (ESL). Eqn. (1) represents an analytic solution for the voltage droop seen at the die supply rails for such a simplified model of the PDN:

$$\text{Eqn. 1: } \Delta V_{die}(t) \cong 2I_{max} R + I_{max} \sqrt{\frac{2L_{pkg}}{C_{die}}} \cdot e^{-\frac{R}{2L_{pkg}} t} \sin(\omega_r t - \theta)$$

The voltage droop can be decomposed into a DC IR- drop term and an AC $L di/dt$ term. The resistive component of the droop is addressed by increasing the metallization resources in the PDN 100. The inductive component is a trade-off between the package and the die and far exceeds the resistive droop magnitude in modern computing systems.

[0025] Referring now to **FIG. 2**, there is depicted a graph 200 of the PDN input impedance (as seen from the die) as a function of frequency for the simplified PDN 100 illustrated in **FIG. 1**. The impedance spectrum shows three distinct impedance peaks attributable to each capacitor resonating with its counterpart inductor. The highest impedance peak, referred to as the “first-order resonance,” also occurs at the highest frequency (~100MHz) and is due to the resonance between the die capacitance and the package inductance. The second-and third-order resonances are due to downstream capacitor networks, and occur at relatively lower frequencies (~1MHz and ~10KHz for the 2nd and 3rd-order resonances, respectively).

[0026] With reference to **FIG. 3**, there is shown a graph 300 of current-step excitations that exercise the three prominent system resonance frequencies in the PDN 100 due to micro-architectural events such as pipeline interlocks. The maximum magnitude of the voltage droop is caused due to the first-order resonance, which as such dominates the total timing margin.

[0027] Referring now to **FIG. 4**, there is depicted a high-level block diagram of an example embodiment 400 in accordance with the present disclosure. One 402₁ or more (402₂ ... 402_N) on-chip power supply rail noise monitoring sensors are coupled to PDN 100. The power delivery network might include networks across power supply boundaries, LDOs, DC/DC converters. In an example embodiment, an electrical property change on one side of an optically isolated DC/DC converter might be detected using the disclosed methods on the other side of it by creating the mentioned sample loads. The sensor(s) may be of the type disclosed in U.S. Patent Application Publication No. 2015/0137864, entitled "Circuit Delay Monitoring Apparatus and Method," assigned to the Assignee of the present application, the content of which is incorporated herein in its entirety. This sensor, which goes by the product name "VSurge" utilizes a digital sampling oscilloscope that measures the sensor's own power supply rail, and includes triggering circuitry to generate an event when the rail droops below a programmable threshold. A signal generator for generating on-chip loads as a signal generator for power supply noise is represented by block 404. Advantageously, dynamic-responses might be coordinated to occur at multiple points on the board or chip – either coordinated or uncoordinated. Such excitation may occur at multiple points, optionally time-diverse, to generate more complex patterns in accordance with embodiments of the present disclosure. These multiple points are conceptually and generally represented by reference numerals 401₁, 401₂, ... 401_N. As will be appreciated, the term "dynamic response" is generally construed as the response of a system to a dynamic (i.e. time varying) event. Thus, a dynamic response is intended to include an impulse response (time-domain response to an impulse function input; or its frequency-domain equivalent), a step response (same, but to a step function input), peak resonant frequency, top-N resonant peaks, frequency response, and the like. As will be appreciated, such measurements can be transformed using conventional signal processing techniques, e.g. a Fourier transform.

[0028] As shown in **FIG. 4**, the on-chip power supply noise sensor 402₁ and loads quantify the impedance and frequency response of the power delivery network (off chip and on chip

regulators, decoupling capacitances, parasitics, etc.), and this measurement is utilized to detect changes in the response due to additions or removals of elements in the network (such as a removal of a decoupling capacitor, or additional inductance due to patching a probe wire onto the PCB trace). A processor generally represented by block 406 is employed to

5 implement the functionality of the disclosure as described in further detail below. The processor 406 is operably coupled to the one or more or more sensors ($402_1, 402_2 \dots 402_N$) and secure memory 408. The architecture disclosed herein can be implemented as a hardware and software co-design or as a fully embedded on-chip hardware block. Additional software can be provided to drive the sensors ($402_1, 402_2 \dots 402_N$) for a set of security applications in
10 accordance with embodiment of the disclosure. Compared to the logic nets and gates of system on chips (SoCs), which are referred to herein as points of interest, the sensors themselves have inconsequential small performance, power and area (PPA) impact and therefore, the software can run on a low power processor or a dedicated hardware block can be used that implements these services.

15 **[0029]** In general, a method in accordance with an embodiment of the disclosure generally consists of three phases: characterization, protection and reaction. During characterization, the response of the points of interest is characterized. During this phase, stress-tests stimuli are applied (e.g. instruction sequences result in a large change in current consumption, such as a mis-predicted branch for a CPU core intellectual property (IP) block), and the sensor(s)
20 ($402_1, 402_2 \dots 402_N$) are used to measure how the PDN 100 responds to this impulse. The (complex) frequency response of the power delivery network provides a measurement indication of the power network impedance (S-parameters). In addition to stress-tests stimuli, complex stimuli can be used to generate arbitrary signals or waveforms, such as AC coupled onto the SoC power supply rail(s) that can speed up the characterization phase. Another
25 option is to use design-specific custom stimuli, and measuring the responses from the points of interest, which allows for a faster responses characterization. Optionally, custom hardware, can be integrated together with the sensor, and could be used to generate stimuli for a faster points of interest characterization. The characteristics of the points of interest are stored as golden reference characteristics in the secure memory 408. In addition to the characteristics,
30 attacks can also be emulated and the deviation of the responses of the points of interest can be stored for diagnostic purposes. The characterization phase can also be executed online to store historical responses. This is represented generally by a server 414 coupled to a

communications network 416. At a high-level, the server 414 includes at least one processor 410 and memory 412 for storing the historical responses. In this manner, two functionalities are enabled. First, the type of attack to be protected against can be emulated, and the responses of the points of interest collected. This enables the collection of the attack-response characterization. Second, the points of interest in the system can be continuously placed under response-monitoring, and the responses can be compared with stored reference responses that belong to systems that are under attack in order to diagnose the type of the attack. It will be appreciated also that quantities of operating conditions such as the temperature, humidity, moisture through condensation, ageing etc., which can be provided by other sensors and predictive models, can be used to cluster the responses from points of interest to enhance their accuracy. Furthermore, the characteristics of a power distribution network are affected by the location of the points of interest that are observed. Therefore, multiple responses can be stored as golden references from multiple locations, and this can be used for enhancing further the diagnosis ability of the type of threat/attack that is detected.

[0030] During the protection phase, the system applies, continuously and/or periodically, the characterization phase to collect responses (dynamic response properties) from the sensors ($402_1, 402_2 \dots 402_N$) that monitor the points of interest based on which the system response is formed. Deviation between the system response from the golden reference system response, is used to detect possible threats and/or attacks that are imminent and/or are taking place on the protected hardware. Diagnosis of the threat can then take place to identify the type of threat (disordering, etc.) and its location. The first can be implemented by using the stored dynamic-responses from emulated threats, or from threats that have already been diagnosed by other protection-systems, and the latter using the location of points of interest. Another option for diagnosis of the threat's location, is the deviation of the PDN impedance compared to the golden reference. First-, second- and third-order resonance deviation, as described above and illustrated in **FIG. 3**, provides an indication that the attack took place at the die, the package or the PCB respectively. The protection phase can occur continuously, measuring the points-of-interest characteristics in real-time. The comparison with the golden references can be implemented either in software executing on the low power processor (the same that was used for characterization) and/or dedicated hardware operable for this purpose (collectively represented by block 406). The protection phase can be executed once during boot, and/or continuously or periodically at run-time.

[0031] In accordance with the present disclosure, embodiments thereof prevent an attacker from predicting scheduled pulses and measurements and easily evading detection. In this regard, it will be appreciated that by aggregating many data-windows at random or pseudorandom time offsets, it is possible to cancel out non-predictable background system behavior (systematic or non-systematic). Such randomness thus decouples any sampling from regularities in power consumption of the system. The system power consumption typically has a much stronger signal than the much weaker response to the programmable applied load. By aggregating 100-thousands of time-series windows (each with, for example, a 10k sample time series), it is possible to cancel out system operation noise, and to emphasize the dynamic-response signal(s) for further analysis.

[0032] In a first example (Simple Power Analysis Case), the measurements are scheduled at a time where the power consumption pattern is fully understood. This can be either during known power load profiles of certain instructions, using either the load pattern of the instruction, or by adding additional loads using load circuits. In many cases such measurement can be performed in idle processor states of the CPU (optionally suspending unpredictable chip functions during the measurements). A single measurement time series window or a few measurement windows aggregated can already result in useful response patterns at low noise in this case. In a second example (Differential Power Analysis Case), the power measurements/load generations are ideally scheduled at random intervals, but in fixed time relation between pulse-start and sampling-start. This allows summing up all the individual samples of multiple windows for the same time Δ_t /array index respective from the start of sampling. This results in aggregation that averages out random influences with respect to this sample, and emphasizes the signal of interest – the weak dynamic-response hidden within the strong system operation noise. Over 100-thousands of iterations of aggregation of time series sample windows, that signal becomes much stronger than the noise associated with system operation and it can be used to ascertain changes in system response. By doing more aggregations or by increasing the load strength for the test load on the power delivery network, the time and iterations required for capturing the signal of interest, the impulse response, can be controlled. Depending on the current trust level of the system, the test load strength or the time between running a new time series sample-sequence can be modified. This allows the system to decrease the time needed to accurately measure the system response at expense of power consumption and visibility to potential attackers.

[0033] Referring to **FIG. 5**, there is illustrated a flow diagram of a method for detecting a change in electrical properties in a system powered at least in part, by a power delivery network (PDN 100). The method starts at block 500 and proceeds to block 502, where a reference load is generated on the power delivery network in the collection phase. The

5 reference load is generated, for example, by the signal generator 404 as described above. As described above, the test load strength or time between running a new time-series sample sequence can be modified. At block 504, a reference noise induced in the PDN 100 is measured, using one or more sensors ($402_1, 402_2 \dots 402_N$) located on the PDN 100, in response to the reference load. At block 506, one or more dynamic-response properties are
10 determined based on the measured reference noise by the processor 406. At block 508, the processor stores the one or more reference dynamic-response properties in secure memory 408. Such reference dynamic-response property(ies) (the golden reference(s)) are used to determine the presence of attacks. In the protection phase, at block 510, using the sensors located on the PDN 100, noise induced in the power delivery network is measured in
15 response to an applied load. Based on this measured noise, at block 512 a dynamic response property of the PDN 100 is determined in response to the applied load. At block 514, the processor 406 compares the dynamic-response property of the PDN 100 to the stored one or more reference dynamic-response properties of the PDN 100. At block 516, if there is a difference between the dynamic-response property and one or more reference dynamic-
20 response properties stored in the secure memory 408, then at block 518 system triggers a response to the event. The protection phase may proceed continuously, in which case the process loops from blocks 516 and 518 back to block 510. Otherwise, after an event triggered at block 518, the process terminates at block 520.

[0034] Referring now to **FIG. 6**, there is depicted a high-level schematic of an apparatus 600
25 for implementing embodiments of the present disclosure. The characteristics of the points of interest used can be the power rail voltage time-domain, current rate of change di/dt , the number of sensor triggers count and the frequency domain of their respective impedance. A load circuit is characterized generally by the reference numeral 602. A trigger type of sensor instructs an on-chip oscilloscope 604 whether or not to wait for a trigger condition, and how
30 to handle the arrival of such trigger. A trigger engine 606 of the oscilloscope consists of blocks that are configured to provide flexibility on triggering the sensor, similar to an external oscilloscope. Auto-triggers, event counters and time stamp blocks also allow points

of interest to be monitored, timed and counted. These quantities are sensitive to the workload executed and the electrical characteristics of the power delivery network, and are described in detail in P. N. Whatmough, S. Das, Z. Hadjilambrou, and D. M. Bull, "Power integrity analysis of a 28 nm dual-core arm cortex-a57 cluster using an all-digital power delivery monitor,"

5 IEEE Journal of Solid-State Circuits, vol. 52, no. 6, June 2017, and the publication "Modeling and characterization of the system-level power delivery network for a dual-core arm cortex-a57 cluster in 28nm cmos," described above. For the responses, statistically significant data from long stimuli sequences are used, therefore threats from attacks that cause systematic deviation of the responses can be separated by insignificant events that
10 cause random deviation of the responses compared to the golden references. For example, attaching an oscilloscope probe to a package pin could produce a systematic change in network response due to the addition of parasitics (inductances/capacitances) or stubs to the network, or by changing the loading on the line and causing response changes due to significant nonlinearities in components (such as ceramic capacitors) in the network. The
15 configuration illustrated in **FIG. 6** can be modified to implement the Differential Power Analysis Case described above by, instead of replacing samples in the SRAM buffer, the Decimation output is added to each point (index). By having a wider register for each point (i.e., 32 bits or more), many samples can be aggregated for processing. The resulting SRAM buffer would have eliminated the system power noise as long as the triggers for the sample
20 start are scheduled randomly.

[0035] The reaction phase in accordance with the disclosure is triggered when a threat has been detected. The reactions can be different depending on the configuration of the system and the type of threat: e.g. locking down the system, reducing its "trust score" (locally and/or to a cloud management server), avoiding performing any sensitive operations (such as
25 cryptographic operations) until the response returned to expected values, or in other ways as appropriate to the end application of the SoC. The reaction phase can be implemented by software, but for more secure applications is preferably implemented as a hardware design.

[0036] In accordance with an embodiment of the disclosure as illustrated in **FIGS. 7 - 9**, there is provided a methodology for deriving secure unique identification or attestation
30 information from dynamic response of the power delivery network of an SoC to power demand stimuli as described above. This embodiment utilizes a power rail noise monitoring sensor and the approach described above, wherein the dynamic response (impulse response,

complex impedance, S-parameters etc) of the power delivery network of an SoC and PCB-level system is characterised/estimated. It will be appreciated by those skilled in the art, that ADC sensors as used in microcontrollers where the power supply voltage can be routed to the ADC and compared against an internal bandgap, allow absolute sampling of the supply voltage. Load can be generated either with switchable load resistors on the SoC or the existing switchable load resistors as used on GPIO pins that can be driven against power or signal rails. Alternatively, output GPIO pins can be directly driven against GND, Signal or Supply rails (power limited by the driving circuit) to generate momentarily high load.

Embodiments of the disclosure ensure that the voltage rails sensors are only accessible to a privileged security level, which, among others, prevents side channel attacks from within. A programmable on-chip load, and phase-aligning that load with the start of a short sampling window of one or more sensors on power rails enables the system to capture 10's of thousands or millions of windows. These windows are all over the place and randomly distributed (unpredictable to potential attackers). This ensures that system level power deviations cancel each other out over time when averaging these windows. At the same time, embodiments of the disclosure emphasize the effects of minute differences resulting from the step response to the programmable load that is a constant distance to the sampling window.

[0037] From the above, a frequency response of the system that is affected by minute differences in the system PCB can be obtained. Such a fingerprint can be obtained during production while the system is regarded to be secure. Optionally, a discrete Fourier transform (DFT) may be performed on the one aggregated window (high resolution) to identify the frequency/phase response.

[0038] The known-good fingerprint is then stored into a secure memory controlled by the trusted code (Trustlet, v8M uVisor compartment etc.)

[0039] The secure fingerprint is continuously compared against the system state.

[0040] The windows can be either aggregated in blocks or continuously in a sliding window of windows. This creates a lowpass function that establishes a baseline removing noise generated by system activity.

[0041] The stored reference can be continuously updated during lifetime of the PCB to compensate aging of components like capacitors.

[0042] The system is operable to detect step functions in changes to frequency and phase response by comparing the current response to the stored reference.

[0043] As the reference is stored in secure memory, detection of modification of the main PCB may be obtained even after the circuit was turned off for a brief or long period of time.

[0044] From a protocol level a secure attestation key or an identity key - ideally chip specific and optimally tied to the chip manufacturer through a certificate chain, is provided.

- 5 Optionally the verification of frequency response patterns can be implemented via a cloud service. The system only needs to forward the signed frequency response (time series or frequency distribution).

[0045] In accordance with an embodiment of the disclosure, the interested party sends a NONCE to the attesting party. The trusted code performs the measurement or takes a
10 reasonably fresh measurement and compares that to the stored reference. If the differences between both are within an acceptable threshold, the system proves integrity to the interested party by replying with "Yes, I can attest that my system is not compromised - here's my reply including your NONCE, signed by a chip identity/attestation key". The NONCE ensures that an attacker can't replay these attestations, proving freshness.

15 [0046] The generated attestation load that is averaged over many windows can be either a simple square wave or a complex load wave pattern at multiple spatially/temporally different points of the chip or the board. The pattern can be constant, per remote party or per board (inferred from their public identity, optionally encrypting the response with the requestors public key). This complicates attacks against the scheme as the load patterns are not
20 transferrable across devices and require more complex countermeasures from the attacker.

[0047] Load orchestration can be implemented across chip boundaries by synchronizing multiple chips for generating loads on power rails not directly accessible to the measuring chip and/or measure local cause of remote load effects. The orchestration synchronizes sampling with load allowing to remove the normal system load from the measurements.

25 Multiple reference characteristics can be stored for reflecting different behaviours for different load cases (chip/board components enabled, or power gated), different power supply cases, different discharge levels of batteries, changing battery impedance during discharge, different temperature levels or humidity levels. The system is operable to choose the appropriate for comparison at that point.

30 [0048] Known deviations might be parametrised over the model to interpolate changed distribution of the frequency response depending on battery impedance etc. This avoids storing multiple versions of the response.

[0049] In one embodiment, to avoid the requirement for a high-speed ADC, the load resistor window may alternatively be moved relative to a low speed ADC at high resolution. Through additional oversampling, the time resolution can be increased.

[0050] Embodiments of the disclosure can be employed to verify integrity of IO pins (both digital and analog) by performing ADC readings in parallel to IO operations. In this regard, a light load may be applied on the measured pins by using integrated pull-up/pull-down resistors (100kOhm or higher impedance).

[0051] With reference now to the flow diagram of **FIG. 7**, the block diagram of **FIG. 8**, and the timing diagram of **FIG. 9**, there is depicted a method of remote attestation in hardware or software in accordance with embodiments of the disclosure. The method starts at block 700, with a request for attestation and receipt of a remote NONCE, and proceeds to block 702 where the system acquires one Sample Window (FN_GET_WINDOW).

[0052] In block 704, the system generates True Random Number Generator (TRNG), Pseudorandom Number Generator (PRNG) or non-periodic value t_{rnd} .

[0053] In block 706, the system configures the timer to wait for t_{rnd} cycles – resulting in the $t_{rndWait}$ time.

[0054] In block 708, after expiration of the configured time period $t_{rndWait}$ the method proceeds to block 710 and starts the capture process of the power rail voltage – current sensor (“VSurge” component 800, **FIG. 8**) using the signal name VSURGE_SAMPLE_START.

VSURGE_SAMPLE_START resets the index counter INDEX_COUNTER (**FIG. 8**) to zero, determining the currently active array index in the buffer VSURGE_SAMPLE_BUFFER. VSurge samples VSURGE_SAMPLE, a value with 12 bit resolution.

[0055] In block 712, each sample output of Vsurge (VSURGE_SAMPLE) is combined with the buffer by adding it to the current buffer value at the index INDEX_COUNTER:

SAMPLE_BUFFER[INDEX_COUNTER] += VSURGE_SAMPLE.

In block 714 INDEX_COUNTER is incremented, the next VSURGE_SAMPLE is acquired, and the previous step (block 712) is repeated for all SAMPLE_BUFFER entries (1024 buffer entries in this case, each 32 bit size).

[0056] In block 716, at a fixed time relative to VSURGE_SAMPLE_START, the test load pattern is generated. The pattern can be as simple as, for example, “Increase System Load by 1mA for 50% of the time of the sample window”. The duration of the load determines the frequency response. In a more complex scenario the test load pattern can be arbitrary

complex (digital or analog waveform). It's important that the load pattern is identical for all aggregated windows and always at the same time-relative position to

VSURGE_SAMPLE_START. This is illustrated in the timing diagrams 900 of **FIG. 9**.

[0057] An aggregation of multiple windows (FN_GET_WINDOW_AGGREGATED) is

5 performed. By running FN_GET_WINDOW multiple times, VSURGE_SAMPLE values are aggregated time-relative to the sample load. Thanks to the non-periodic property of scheduling FN_GET_WINDOW using VSURGE_SAMPLE_START, the system load becomes non-periodic/random related to the sample window start. This enables the sample to asymptotically approach a single shared value for each entry of the SAMPLE_BUFFER.

10 As the impulse response of the system is expected to be similar across multiple sample windows, the effect of the impulse response becomes significant in the data over 10's of thousands of aggregated windows. An example calculation for 12 bit VSURGE_SAMPLES – aggregated in 32 bit buffer registers allows $2^{32-12}=2^{20}=1048576$ windows to be aggregated before the aggregation buffer overflows. As this example calculation demonstrates, ~1M
15 windows can be aggregated. At this oversampling factor it can be expected that the system activity to average out thanks to the random/non-periodic scheduling of the VSURGE_SAMPLE_START signal, and emphasizing the frequency response for the test load, thereby lifting it out of the noise of the system load. The system load in most cases is expected to be at 100x or more of the magnitude of the test load signal (i.e., up to 100mA
20 system load, varying between 0.001mA and averaging around 10mA – and a test load of 1mA).

[0058] In block 718, the DC-Offset of the aggregated data is either removed in postprocessing and/or during aggregation to make better use of the buffer resolution.

25 Removing the DC offset removes the effect of different averages of system load when comparing two waveforms collected under different load conditions.

[0059] The system then generates a golden reference waveform (i.e., trusted reference waveform) (FN_GET_WINDOW_AGGREGATED_REF). In block 720, the waveform FN_GET_WINDOW_AGGREGATED is captured in a trusted environment, preferably as the last step of a trusted manufacturing process.

30 **[0060]** In block 722, the waveform FN_GET_WINDOW_AGGREGATED is stored in a trusted storage (optionally signed to prevent tampering, and tied to the root of trust framework of the device).

[0061] The system then verifies the reference waveform.

(FN_GET_WINDOW_AGGREGATED_ATTEST). In block 724, the waveform FN_GET_WINDOW_AGGREGATED is captured in the deployed system. Preferably all hardware and software responsible for the collection and performing the verification steps runs in a trusted environment like TrustZone, ARM Secure Island (available from the assignee of the present application) or a dedicated security processor. The peripherals like timers and VSurge should only be made accessible by the trusted domain to ensure untrusted code can't tamper with the acquisition data or logic.

[0062] In block 726, the waveform is then compared with the waveform captured

FN_GET_WINDOW_AGGREGATED_REF (this comparison ideally happens in the trusted domain). Multiple golden references might be stored for different environmental conditions (temperature ranges, humidity levels, battery voltage levels, battery impedance depending on discharge levels etc.). The comparison is done to the golden reference matching made under environmental conditions that most closely match the current environmental conditions.

Golden references for two adjacent environmental conditions can be optionally interpolated if needed to generate an even closer "virtual golden references". The golden reference and the measured waveform can be either directly compared (error square analysis etc.) – or analyzed for frequency bands and signal magnitudes using DFT or similar means. The stored reference would then be a set of frequency bands and related expected magnitudes of the signal in these bands depending on the length/frequency composition of the test load pattern. The analysis methods are described above. The result of the analysis is either a match/no-match output based on an internal threshold, or a confidence value relating the level of trust into the system being close to the golden reference.

[0063] In block 728, the result is then signed cryptographically (Public Key Signatures or HMAC using a shared secret) – optionally adding a trusted/secure time stamp, a sequence counter or a proof-of-freshness like a NONCE provided by the requesting party. All of the above processing is ideally protected by the trusted environment to prevent tampering with the logic or data, or signature secrets before or after the signatures are applied. The signing secrets are ideally protected against exfiltration.

[0064] Next, there is performed remote attestation of the reference waveform (FN_GET_WINDOW_AGGREGATED_REMOTE_ATTEST). In block 730, a remote cloud server system triggers locally the FN_GET_WINDOW_AGGREGATED_ATTEST

mechanism, for example, by providing a server-generated random NONCE, that must be co-signed with the trust value calculated in the

FN_GET_WINDOW_AGGREGATED_ATTEST step.

[0065] In block 732, the signed attestation including the NONCE and the trust value result is transferred to the non-secure side in case secure/non-secure separation exists.

[0066] In block 734, a fully untrusted network stack then returns the attestation packet to the cloud server.

[0067] In block 736, the server verifies whether the attestation packet is consistent with the expected device identity (either based on the shared HMAC secret or a valid certificate chain for the device attestation certificate that has been used for signing the trust value. If, at block 734 the trust value is determined to be high enough, or the binary indication confirms a match of the internal golden reference with the freshly captured and aggregated waveform, the server can then safely provision further secrets or confidential data(s) or code to the device.

This method therefore enables reasoning of the extended board level integrity (tamper, attached parasite circuits, loggers etc.) from within an application processor die or microcontroller. This verification can be remotely attested cryptographically using the above steps – including proof of freshness.

[0068] Referring now to **FIG. 10**, there is illustrated a flow diagram of a method for authenticating a device in a system using electrical properties in the system.

[0069] In block 1000 the method starts with a request to authenticate the device.

[0070] In block 1002, a plurality of input seed values are received from a requestor. The seed values enable the initialization sequence for each load stimuli. In this connection, there is provided a causal relationship between an input load seed values and the load stimulus such that both the authenticator/requestor and authenticatee jointly know the mapping of seeds to load stimuli. In one embodiment, a defined function may be utilized, taking one or more seeds as input and returning one or more stimuli as output. In other embodiments, it may be parameterizable based on a shared secret (e.g. as an additional input to the defined function). In yet other embodiments, the nature of the stimuli can be configured in the form of a variable current load enabled by explicit load circuitry. Alternatively, the stimulus can also be provided by execution of sequence of instructions.

[0071] In block 1004; for each input seed value, load stimuli are generated to produce an electrical load sequence on a power delivery network (see above) powering at least part of the

system. Each electrical load sequence relates to at least one magnitude and phase component in a specific frequency band corresponding to a dynamic response of the system

[0072] In block 1006, noise induced in the power delivery network in response to the electrical load sequence is measured, using one or more sensors located on the power delivery network.

[0073] In block 1008, based on the measured noise, a dynamic response property of the power delivery network corresponding to a respective input seed value is determined.

[0074] In block 1010, the dynamic response property of the power delivery network is returned to the requestor.

[0075] The input seed value can be modified by a secret known only to the device to ensure that an attacker cannot predict the load sequence from the input seed value. Further, the input seed value can be modified by a secret shared between the requestor and the device. The shared secret compensates for aging of components of the device by modifying a threshold applied by the requestor in the authentication. Advantageously and as discussed above, the dynamic response property is stored in a secure memory as a set of reference parameters. The device may be authenticated using a shared HMAC secret or a valid certificate chain.

[0076] Referring now to **FIG. 11**, there is depicted a high-level block diagram of an example authenticator 1100 in accordance with an embodiment of the present disclosure. The authenticator 1100 may be embodied in hardware, software or a combination thereof. In an example embodiment, authenticator 1100 includes a processor 1102 operable to receive, from a requestor 1104 (i.e., an electronic device configured to communicate with the authenticator over a hardwired, wireless and/or networked connection), a plurality of input seed values 1106 and generate, for each input seed value 1106, load stimuli 1108 for generating an electrical load sequence 1110 on a power delivery network 1112 powering at least part of a system 1114. Each electrical load sequence relates to at least one magnitude and phase component in a specific frequency band corresponding to a dynamic response of the system 1114. The processor 1102 is further operable to receive data representing noise 1116 induced in the power delivery network 1112 in response to the electrical load sequence 1110 measured using one or more sensors 1118 located on the power delivery network 1112. The processor 102 determines, based on the measured noise, a dynamic response property 1120 of the power delivery network 1112 corresponding to a respective input seed value, and returns

the dynamic response property 1120 of the power delivery network 1112 to the requestor 1104.

[0077] The terms “program,” “software application,” and the like, as used herein, are defined as a sequence of instructions designed for execution on a computer system. A “program,”

5 “computer program,” or “software application” may include a subroutine, a function, a procedure, an object method, an object implementation, an executable application, an applet, a servlet, a source code, an object code, a shared library/dynamic load library and/or other sequence of instructions designed for execution on a computer system.

[0078] The present disclosure may be embodied within a system, a method, a computer
10 program product or any combination thereof. The computer program product may include a computer readable storage medium or media having computer readable program instructions thereon for causing a processor to carry out aspects of the present disclosure. The computer readable storage medium can be a tangible device that can retain and store instructions for use by an instruction execution device. The computer readable storage medium may be, for
15 example, but is not limited to, an electronic storage device, a magnetic storage device, an optical storage device, an electromagnetic storage device, a semiconductor storage device, or any suitable combination of the foregoing.

[0079] Reference in the specification to “one embodiment” or “an embodiment” means that a particular feature, structure, or characteristic described in connection with the embodiment is
20 included in at least one embodiment of the system. The appearances of the phrase “in one embodiment” in various places in the specification are not necessarily all referring to the same embodiment.

[0080] Embodiments of the present disclosure are described herein with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems), and computer
25 program products according to embodiments of the present disclosure. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer readable program instructions.

[0081] Some portions of the detailed descriptions, like the processes may be presented in
30 terms of algorithms and symbolic representations of operations on data bits within a computer memory. An algorithm may be generally conceived to be steps leading to a desired result. The steps are those requiring physical transformations or manipulations of physical

quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

[0082] It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussion, it is appreciated that throughout the description, discussions utilizing terms such as “processing” or “computing” or “calculating” or “determining” or “displaying” or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

[0083] The operations described herein can be performed by an apparatus. This apparatus may be specially constructed for the required purposes, or it may comprise a general-purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program may be stored in a computer readable storage medium, such as, but is not limited to, any type of disk, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, or any type of media suitable for storing electronic instructions. A computer readable storage medium, as used herein, is not to be construed as being transitory signals per se, such as radio waves or other freely propagating electromagnetic waves, electromagnetic waves propagating through a waveguide or other transmission media (e.g., light pulses passing through a fiber-optic cable), or electrical signals transmitted through a wire.

[0084] Computer readable program instructions described herein can be downloaded to respective computing/processing devices from a computer readable storage medium or to an external computer or external storage device via a network, for example, the Internet, a local area network, a wide area network and/or a wireless network. The network may comprise copper transmission cables, optical transmission fibers, wireless transmission, routers, firewalls, switches, gateway computers and/or edge servers. A network adapter card or

network interface in each computing/processing device receives computer readable program instructions from the network and forwards the computer readable program instructions for storage in a computer readable storage medium within the respective computing/processing device.

5 **[0085]** Computer readable program instructions for carrying out operations of the present disclosure may be assembler instructions, instruction-set-architecture (ISA) instructions, machine instructions, machine dependent instructions, microcode, firmware instructions, state-setting data, or either source code or object code written in any combination of one or more programming languages, including an object oriented programming language such as
10 Smalltalk, C++ or the like, and conventional procedural programming languages, such as the "C" programming language or similar programming languages. The computer readable program instructions may execute entirely on one computer, partly on the computer, as a stand-alone software package, partly on the first computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may
15 be connected to the first computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider). In some embodiments, electronic circuitry including, for example, programmable logic circuitry, field-programmable gate arrays (FPGA), or programmable logic arrays (PLA) may
20 execute the computer readable program instructions by utilizing state information of the computer readable program instructions to personalize the electronic circuitry to perform embodiments of the present disclosure.

[0086] Accordingly, embodiments and features of the present disclosure are set out in the following numbered items:

25 **[0087]** 1. A method for authenticating a device in a system using electrical properties in the system, the method including: receiving, from a requestor, a plurality of input seed values; generating, for each input seed value, load stimuli to generate an electrical load sequence on a power delivery network powering at least part of the system, each electrical load sequence relating to at least one magnitude and phase component in a specific frequency
30 band corresponding to a dynamic response of the system; measuring, using one or more sensors located on the power delivery network, noise induced in the power delivery network in response to the electrical load sequence; determining, based on the measured noise, a

dynamic response property of the power delivery network corresponding to a respective input seed value; generating, from the dynamic response property of the power delivery network a plurality of authentication response values, each authentication response value relating to at least one magnitude and phase component in a specific frequency band corresponding to the measured dynamic response property; returning the authentication response values to the requestor; and at the requestor, comparing the authentication response values to known authentication response values to authenticate the device.

[0088] 2. The method of item 1, where the system is stimulated by the electrical load sequence and the response measured at pseudo-random time intervals.

[0089] 3. The method of items 1 or 2, where the input seed value is modified by a secret known only to the device.

[0090] 4. The method of any of items 1 to 3, where the input seed value is modified by a secret shared between the requestor and the device.

[0091] 5. The method of item 4, where the shared secret compensates for aging of components of the device by modifying one or more thresholds applied by the requestor.

[0092] 6. The method of any of items 1 to 5, where the dynamic response property is stored in a secure memory as a set of reference parameters.

[0093] 7. The method of any of items 1 to 6, further including authenticating the device by combining the dynamic response authentication with a cryptographic authentication using certificates, pre-shared keys, or public/private key pairs.

[0094] 8. An authenticator for authenticating a device in a system using electrical properties in the system, the authenticator including: a processor operable to: receive, from a requestor, a plurality of input seed values; generate, for each input seed value, load stimuli for generating an electrical load sequence on a power delivery network powering at least part of the system, each electrical load sequence relating to at least one magnitude and phase component in a specific frequency band corresponding to a dynamic response of the system; receive data representing noise induced in the power delivery network in response to the electrical load sequence measured using one or more sensors located on the power delivery network; determine, based on the measured noise, a dynamic response property of the power delivery network corresponding to a respective input seed value; generate, from the dynamic response property of the power delivery network a plurality of authentication response values, each authentication response value relating to at least one magnitude and

phase component in a specific frequency band corresponding to the measured dynamic response property; and return the dynamic response property of the power delivery network to the requestor, the requestor operable to compare the authentication response values to known authentication response values to authenticate the device.

5 **[0095]** 9. The authenticator of item 8, where the system is stimulated by the electrical load sequence and the response measured at pseudo-random time intervals.

[0096] 10. The authenticator of items 8 or 9, where the input seed value is modified by a secret known only to the device.

[0097] 11. The authenticator of any of items 8 to 10, where the input seed value is
10 modified by a secret shared between the requestor and the device.

[0098] 12. The authenticator of item 11, where the shared secret compensates for aging of components of the device by modifying one or more thresholds applied by the requestor.

[0099] 13. The authenticator of any of items 8 to 12, further including a secure memory,
15 where the dynamic response property is stored in the secure memory as a set of reference parameters.

[00100] 14. The authenticator of any of items 8 to 13, further comprising authenticating the device by combining the dynamic response authentication with a cryptographic authentication using certificates, pre-shared keys, or public/private key pairs.

[00101] In accordance with the foregoing, a novel apparatus and method for
20 authenticating a device in a system using electrical properties in the system is disclosed.

Having thus described the present disclosure in detail and by reference to embodiments thereof, it will be apparent that modifications and variations are possible without departing from the scope of the present disclosure defined in the appended claims as follows:

CLAIMS

1. A method for authenticating a device in a system using electrical properties in the system, the method comprising:
 - receiving, from a requestor, a plurality of input seed values;
 - generating, for each input seed value, load stimuli to generate an electrical load sequence on a power delivery network powering at least part of the system, each electrical load sequence relating to at least one magnitude and phase component in a specific frequency band corresponding to a dynamic response of the system;
 - measuring, using one or more sensors located on the power delivery network, noise induced in the power delivery network in response to the electrical load sequence;
 - determining, based on the measured noise, a dynamic response property of the power delivery network corresponding to a respective input seed value;
 - generating, from the dynamic response property of the power delivery network a plurality of authentication response values, each authentication response value relating to at least one magnitude and phase component in a specific frequency band corresponding to the measured dynamic response property;
 - returning the authentication response values to the requestor; and
 - at the requestor, comparing the authentication response values to expected authentication response values to authenticate the device.
2. The method of claim 1, where the system is stimulated by the electrical load sequence and the response measured at pseudo-random time intervals.
3. The method of claims 1 or 2, where the input seed value is modified by a secret known only to the device.
4. The method of any of claims 1 to 3, where the input seed value is modified by a secret shared between the requestor and the device.
5. The method of claim 4, where the shared secret compensates for aging of components of the device by modifying one or more thresholds applied by the requestor.

6. The method of any of claims 1 to 5, where the dynamic response property is stored in a secure memory as a set of reference parameters.
7. The method of any of claims 1 to 6, further comprising authenticating the device by combining the dynamic response authentication with a cryptographic authentication using certificates, pre-shared keys, or public/private key pairs.
8. An authenticator for authenticating a device in a system using electrical properties in the system, the authenticator comprising:
 - a processor operable to:
 - receive, from a requestor, a plurality of input seed values;
 - generate, for each input seed value, load stimuli for generating an electrical load sequence on a power delivery network powering at least part of the system, each electrical load sequence relating to at least one magnitude and phase component in a specific frequency band corresponding to a dynamic response of the system;
 - receive data representing noise induced in the power delivery network in response to the electrical load sequence measured using one or more sensors located on the power delivery network;
 - determine, based on the measured noise, a dynamic response property of the power delivery network corresponding to a respective input seed value;
 - generate, from the dynamic response property of the power delivery network a plurality of authentication response values, each authentication response value relating to at least one magnitude and phase component in a specific frequency band corresponding to the measured dynamic response property; and
 - return the dynamic response property of the power delivery network to the requestor, the requestor operable to compare the authentication response values to known authentication response values to authenticate the device.
9. The authenticator of claim 8, where the system is stimulated by the electrical load sequence and the response measured at pseudo-random time intervals.

10. The authenticator of claims 8 or 9, where the input seed value is modified by a secret known only to the device.
11. The authenticator of any of claims 8 to 10, where the input seed value is modified by a secret shared between the requestor and the device.
12. The authenticator of claim 11, where the shared secret compensates for aging of components of the device by modifying one or more thresholds applied by the requestor.
13. The authenticator of any of claims 8 to 12, further comprising a secure memory, where the dynamic response property is stored in the secure memory as a set of reference parameters.
14. The authenticator of any of claims 8 to 13, further comprising authenticating the device by combining the dynamic response authentication with a cryptographic authentication using certificates, pre-shared keys, or public/private key pairs.

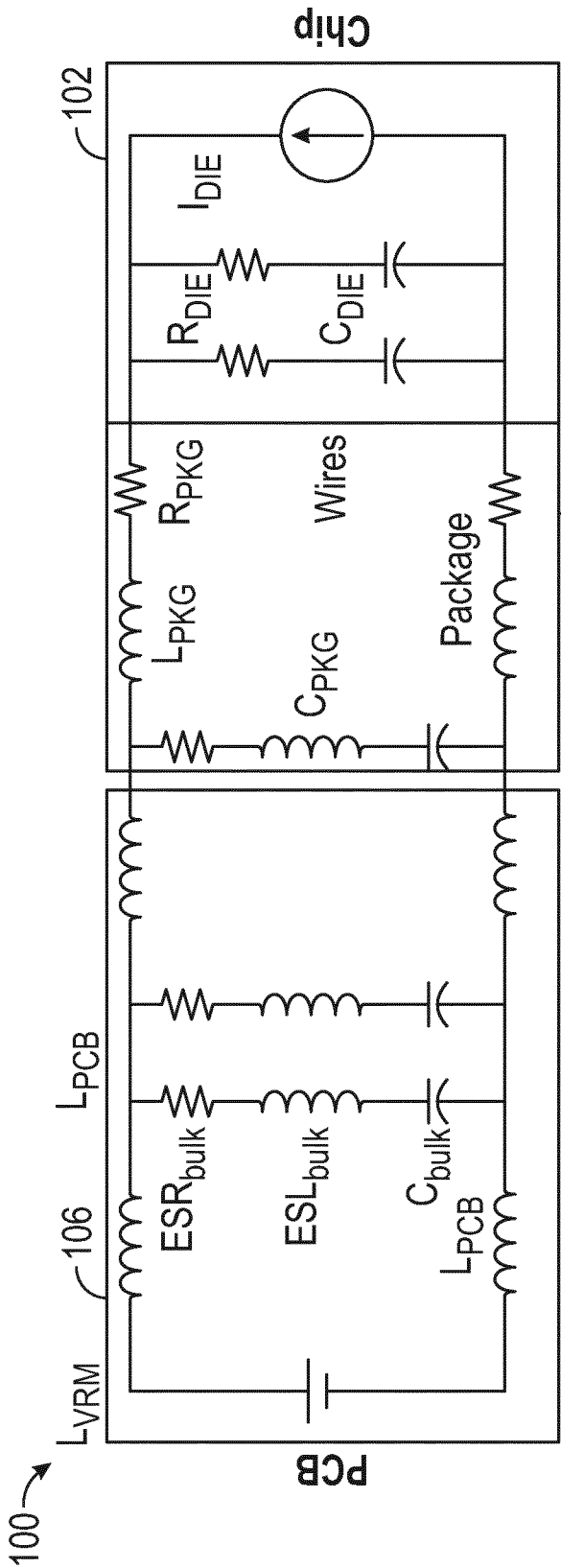


FIG. 1

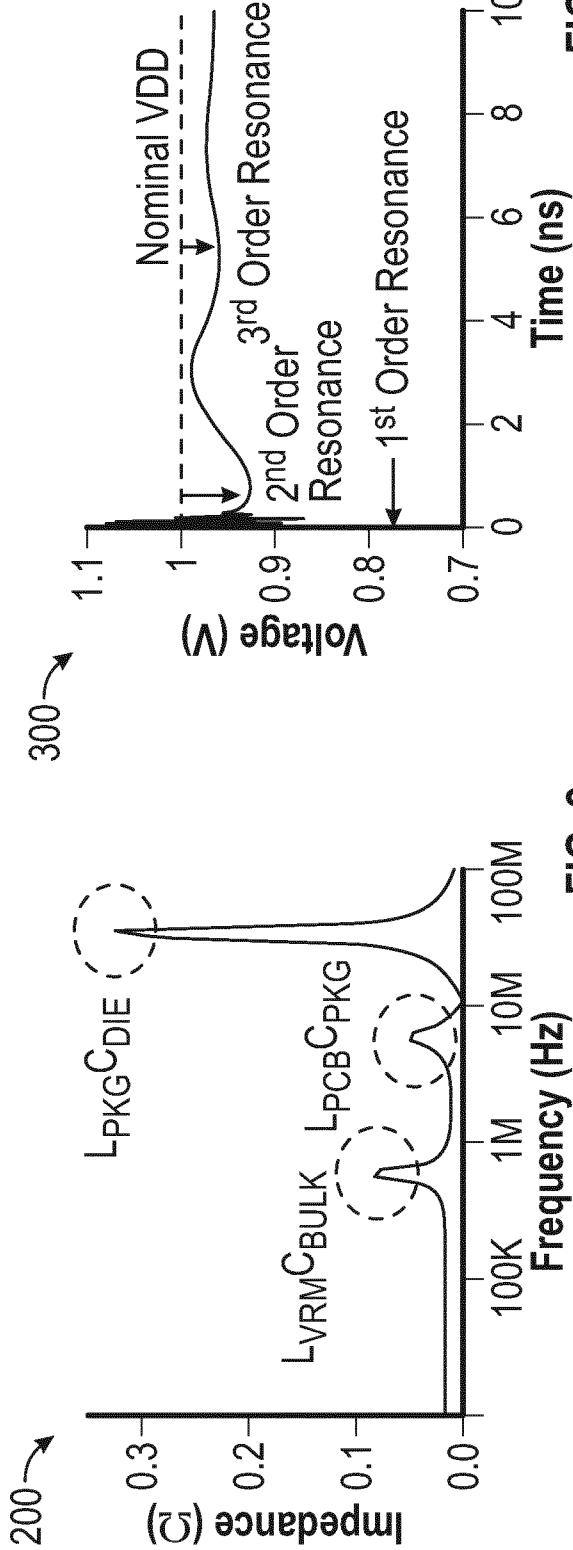


FIG. 2

FIG. 3

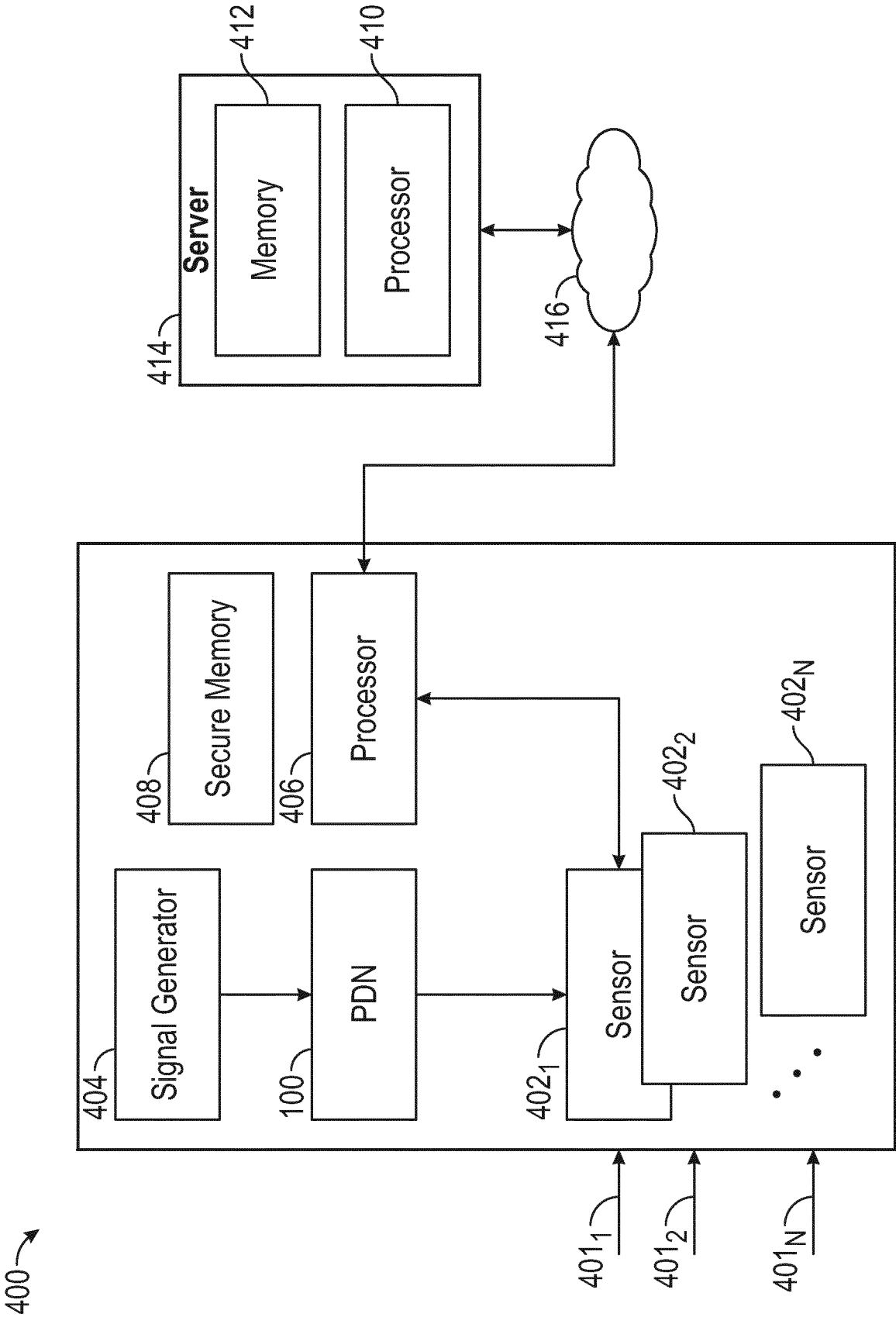


FIG. 4

3/8

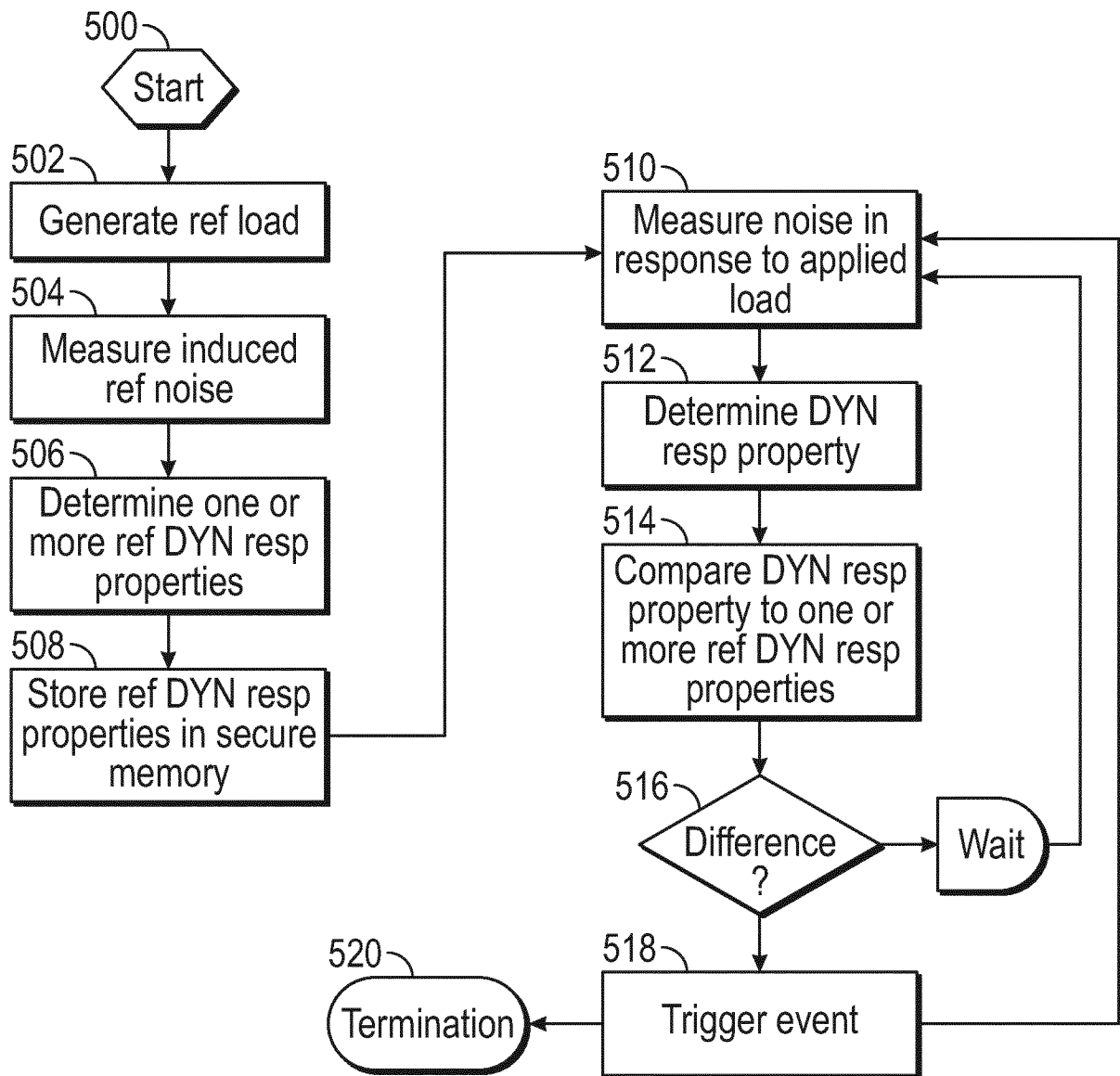


FIG. 5

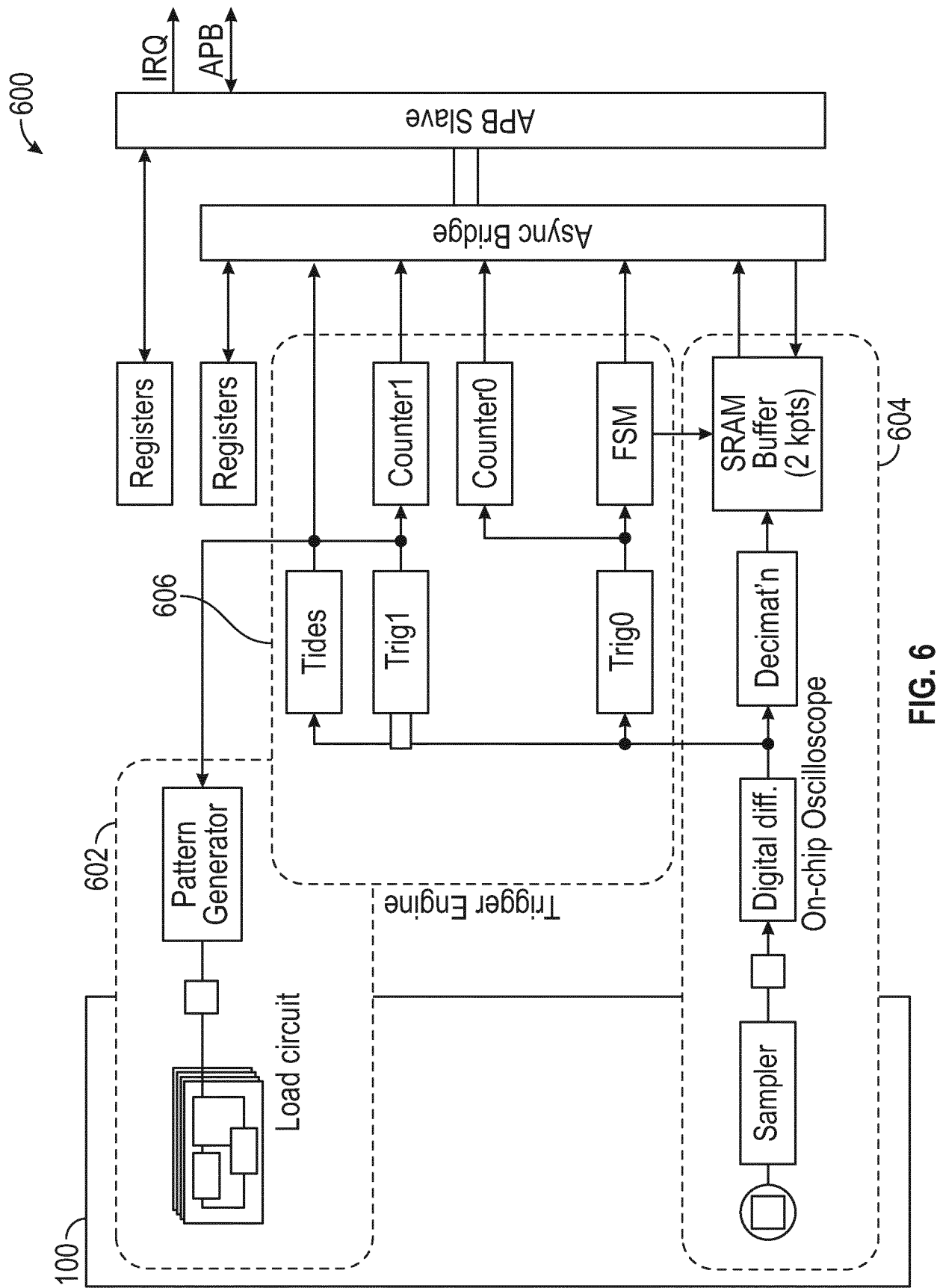


FIG. 6

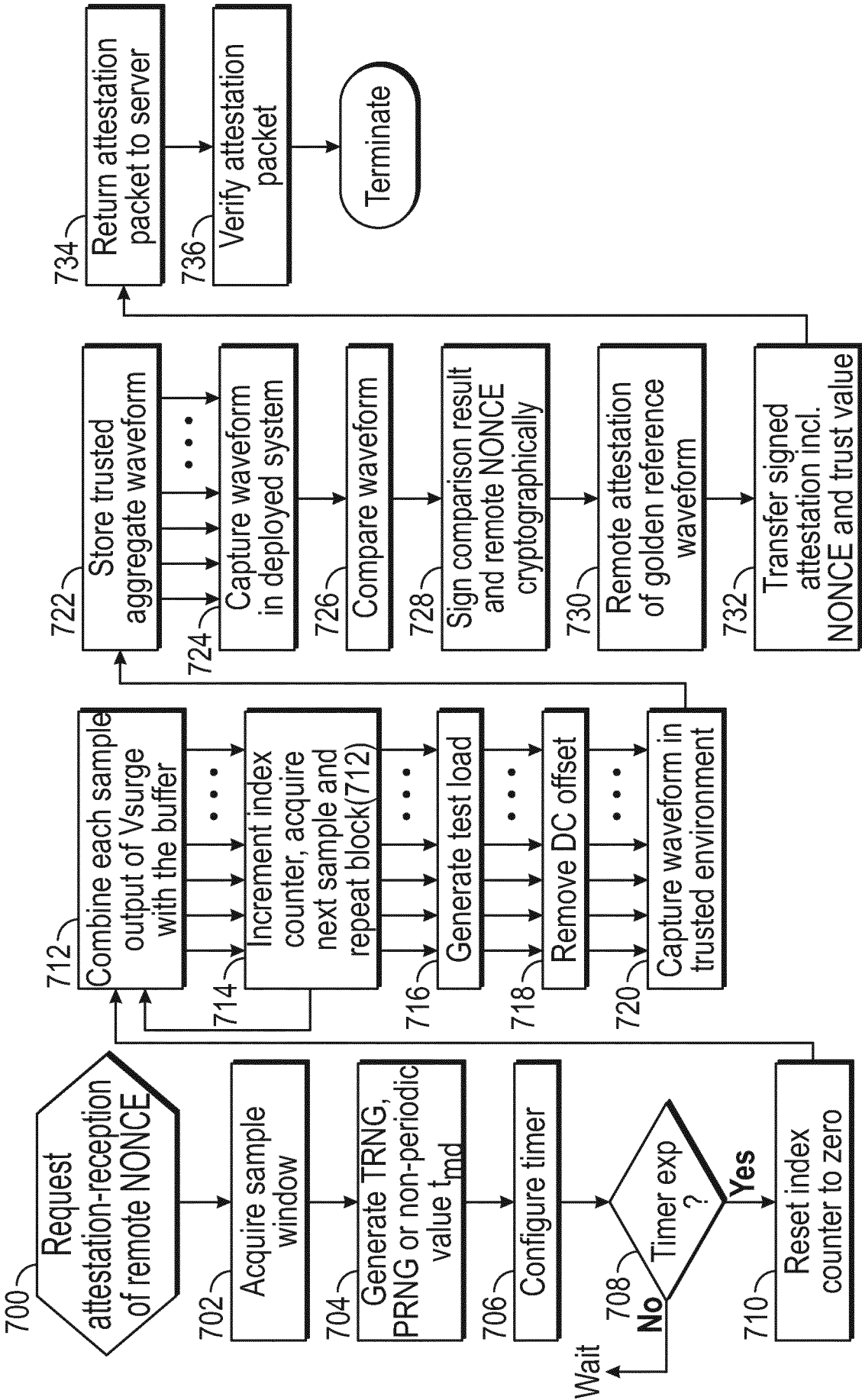


FIG. 7

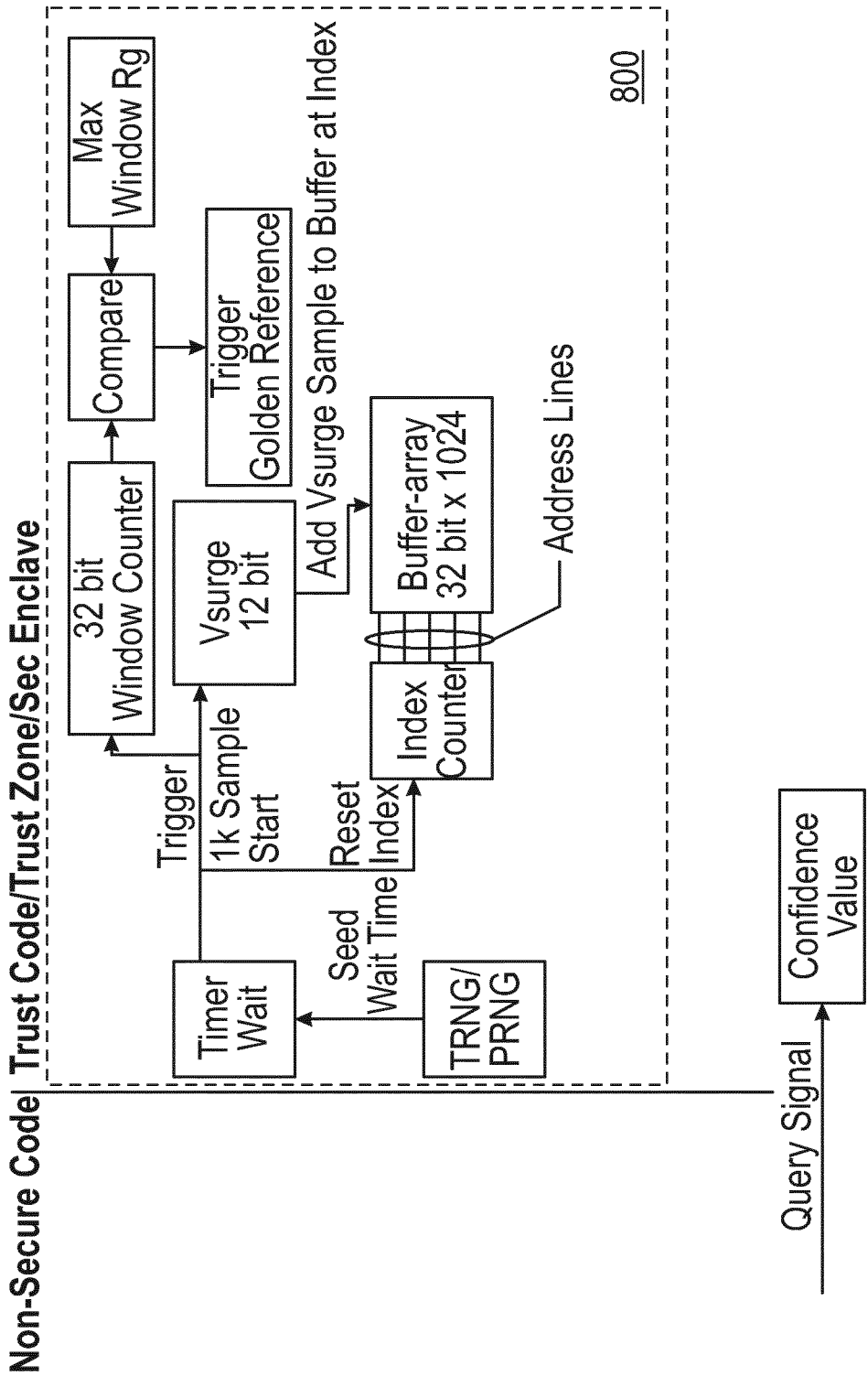


FIG. 8

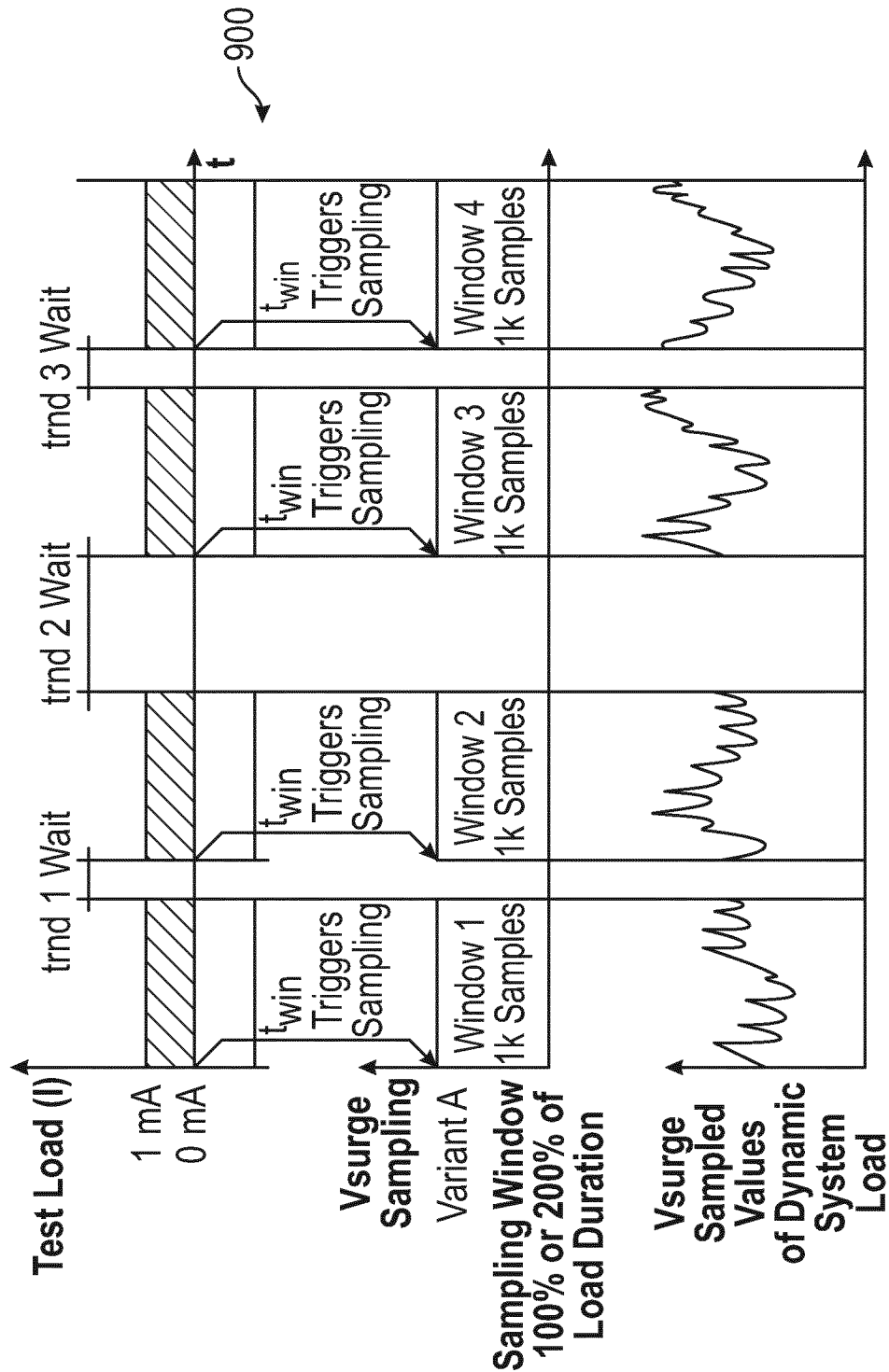


FIG. 9

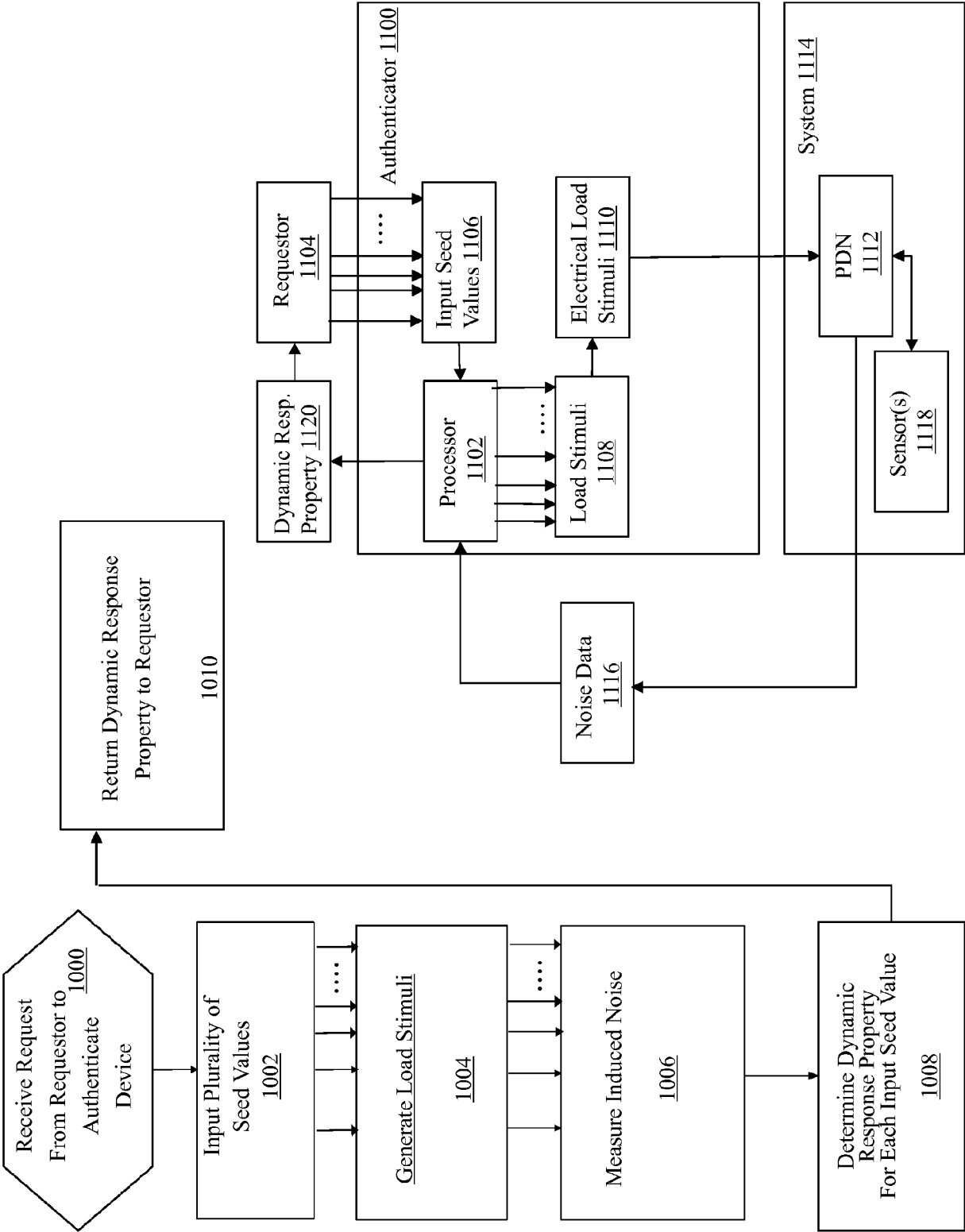


FIG. 11

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2019/060059

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/75 G01R31/08 H04L9/00 G01R19/00 G01R29/26
G01R19/165

ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G01R H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 2 571 131 A1 (RESEARCH IN MOTION LTD [CA]) 20 March 2013 (2013-03-20) abstract; claims 1-16; figures 1-15 paragraph [0006] - paragraph [0029] paragraph [0054] - paragraph [0208] -----	1-14
A	US 2017/030954 A1 (WHATMOUGH PAUL NICHOLAS [GB] ET AL) 2 February 2017 (2017-02-02) abstract; claims 1-19; figures 1-14B paragraph [0006] - paragraph [0009] paragraph [0026] - paragraph [0089] -----	1-14
A	US 2015/195082 A1 (HAN MINGHUI [US] ET AL) 9 July 2015 (2015-07-09) abstract; claims 1-20; figures 1-9 paragraph [0015] - paragraph [0062] ----- -/-	1-14



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

12 July 2019

Date of mailing of the international search report

22/07/2019

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Nadal, Rafael

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2019/060059

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2007/164754 A1 (SMITH GEORGE E III [US] ET AL) 19 July 2007 (2007-07-19) abstract; claims 1-8; figures 1,2 paragraph [0005] - paragraph [0006] paragraph [0010] - paragraph [0018] -----	1-14
A	WHATMOUGH PAUL N ET AL: "Power Integrity Analysis of a 28 nm Dual-Core ARM Cortex-A57 Cluster Using an All-Digital Power Delivery Monitor", IEEE JOURNAL OF SOLID-STATE CIRCUITS, IEEE SERVICE CENTER, PISCATAWAY, NJ, USA, vol. 52, no. 6, 1 June 2017 (2017-06-01), pages 1643-1654, XP011649766, ISSN: 0018-9200, DOI: 10.1109/JSSC.2017.2669025 [retrieved on 2017-05-24] cited in the application the whole document -----	1-14

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2019/060059

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2571131	A1	20-03-2013	CA 2788377 A1 16-03-2013
		EP 2571131 A1	20-03-2013

US 2017030954	A1	02-02-2017	GB 2540812 A 01-02-2017
		KR 20170015169 A	08-02-2017
		TW 201724698 A	01-07-2017
		US 2017030954 A1	02-02-2017

US 2015195082	A1	09-07-2015	NONE

US 2007164754	A1	19-07-2007	NONE
