(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 570 484 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
30.09.2020 Bulletin 2020/40

(21) Application number: **19185064.3**

(22) Date of filing: **28.08.2015**

(51) Int Cl.:
H04L 9/06 *(2006.01)* ***H04L 9/08*** *(2006.01)*
H04L 29/06 *(2006.01)* ***H04W 12/02*** *(2009.01)*
H04W 12/08 *(2009.01)* ***H04W 12/10*** *(2009.01)*

(54) **LOCATION AND PROXIMITY BEACON TECHNOLOGY TO ENHANCE PRIVACY AND SECURITY**

LOKALISIERUNGS- UND PROXIMITÄTSBAKENTECHNOLOGIE ZUR VERBESSERUNG DER PRIVATSPHÄRE UND SICHERHEIT

TECHNOLOGIE DE LOCALISATION ET DE BALISE DE PROXIMITÉ POUR AMÉLIORER LA CONFIDENTIALITÉ ET LA SÉCURITÉ

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **25.09.2014 US 201414495936**

(43) Date of publication of application:
20.11.2019 Bulletin 2019/47

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:
15845198.9 / 3 198 905

(73) Proprietor: **Intel Corporation**
Santa Clara, CA 95054 (US)

(72) Inventors:
- **Deleeuw, William C.**
  Beaverton, OR Oregon 97006 (US)
- **Needham, Bradford**
  North Plains, OR Oregon 97133 (US)

(74) Representative: **Maiwald Patent- und Rechtsanwaltsgesellschaft mbH**
Elisenhof
Elisenstraße 3
80335 München (DE)

(56) References cited:
EP-A1- 2 469 480
US-A1- 2014 245 020
US-B1- 7 095 850

EP 3 570 484 B1

Printed by Jouve, 75001 PARIS (FR)

Description

TECHNICAL FIELD

[0001] Embodiments generally relate to beaconing systems. More particularly, embodiments relate to location and proximity beacon technology that enhances privacy and security.

BACKGROUND

[0002] Indoor beaconing systems may use Bluetooth (e.g., Institute of Electrical and Electronics Engineers/IEEE 802.15.1-2005, Wireless Personal Area Networks) technology to wirelessly transmit a unique identifier or personal name/identifier that is detectable by compatible devices in the nearby area. Thus, if the transmitter of the beaconing system is fixed, nearby devices may determine and/or prove their position based on the detected transmission. Such a solution may be vulnerable, however, to other devices "spoofing" the wireless transmission and potentially enabling the receiving devices to misrepresent their true location. Moreover, the use of such a solution may be inappropriate in other situations when the beacon transmitter is mobile (e.g., worn by a person) due to privacy concerns (e.g., individuals may be reluctant to broadcast their position in certain settings).

[0003] US 20141245020 A1 describes systems and methods for authentication systems for digital records having a hash tree structure that computes an uppermost, root hash value that may be digitally signed. A random or pseudo-random number is hashed together with hash values of the digital records and acts as a blinding mask, making the authentication system secure even for relative low-entropy digital records. A candidate digital record is considered verified if, upon recomputation through the hash tree structure given sibling hash values in the recomputation path and the pseudo-random number, the same root hash value is computed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] The various advantages of the embodiments will become apparent to one skilled in the art by reading the following specification and appended claims, and by referencing the following drawings, in which:

FIG. 1 is a block diagram of an example of a pseudo random number (PRN) tree according to an embodiment;
FIG. 2 is a flowchart of an example of a method of operating a beaconing system according to an embodiment;
FIG. 3 is a block diagram of an example of a beacon device according to an embodiment;
FIG. 4 is a block diagram of an example of an observation device according to an embodiment;
FIG. 5 is a block diagram of an example of a processor according to an embodiment; and
FIG. 6 is a block diagram of an example of a computing system according to an embodiment.

DESCRIPTION OF EMBODIMENTS

[0005] Turning now to FIG. 1, a pseudo random number (PRN) tree 10 is shown in which the PRN tree 10 has time-dependent branches that may be used to grant time-bounded access to a beacon signal. As will be discussed in greater detail, configuring the PRN tree 10 to enable time-bounded access to the beacon signal may provide substantial advantages with regard to security as well as privacy. Moreover, the beacon signal may appear to be random to non-trusted observers. In the illustrated example, an entropy level root seed value 12 ("R0") is generated by a true random number generator (TRNG), wherein the root seed value 12 may be statistically unique and associated with a particular beacon device (e.g., beacon 0). Thus, other root seed values (not shown) may be generated for other beacon devices. The root seed value 12 may be stored to a location (e.g., a secure location) on the beacon device, wherein the secure location may include, for example, memory and/or registers that are unexposed to and/or inaccessible by components not having entropy level access privileges to the beacon device in question. Alternatively, a PRN generator (PRNG) may use a secret value (e.g., known only to the manufacturer of the beacon device) to generate the root seed value 12.

[0006] The beacon device may use a beacon level pseudo random number generator (PRNG 0) and the root seed value 12 to generate a sequence of year-dependent branches 16 (16a-16n) containing PRNs that define a yearly timing schedule for the signal emitted by the beacon device. For example, a first year-dependent branch 16a ("P00") may represent the PRN for a first year (e.g., 2014) during which the beacon device emits a signal. Similarly, an n^{th} year-dependent branch 16n ("P0y") may represent the PRN for an n^{th} year (e.g., 2034) during which the beacon device emits a signal. In one example, an Advance Encryption Standard (AES) Counter (CTR) mode is used to generate PRNs.

[0007] Each year-dependent branch 16 of the tree 10 may in turn be used in conjunction with one or more yearly level PRNGs (e.g., PRNG 00 to PRNG 0y) to generate a sequence of day-dependent branches 18 (18a-18n) containing PRNs that define a daily timing schedule for the signal emitted by the beacon device. For example, a first day-dependent branch 18a ("P000") may represent the PRN for a first day (e.g., January 1) of the first year during which the beacon device emits a signal. Similarly, a second day-dependent branch 18b ("P001") may represent the PRN for a second day (e.g., January 2) of the first year during which the beacon device emits a signal. Additionally, an n^{th} day-dependent branch 18n ("P00d") may represent the PRN for an n^{th} day (e.g., December

31) of the first year during which the beacon device emits a signal.

[0008] Each day-dependent branch 18 of the tree may also be used in conjunction with one or more daily level PRNGs (e.g., PRNG 0010 to PRNG 001h) to generate a sequence of hour-dependent branches 20 (20a-20n) containing PRNs that define an hourly timing schedule for the signal emitted by the beacon device. For example, a first hour-dependent branch 20a ("P0010") may represent the PRN for a first hour (e.g., 12:00AM to 1:00AM) of the second day of the first year during which the beacon device emits a signal, whereas an n^{th} hour-dependent branch 20n ("P001h") may represent the PRN for an n^{th} hour (e.g., 11:00PM to 12:00AM) of the second day of the first year during which the beacon device emits a signal. The illustrated tree 10 may be further expanded for minutes, seconds, fractions of seconds, and so forth. The time periods provided herein are to facilitate discussion only and may vary depending upon the circumstances.

[0009] The resulting output 22 (e.g., leaves) of the time-dependent branches may be wirelessly transmitted as a beacon signal (e.g., one branch value each second) for observation by nearby devices. In one example, the output 22 is applied to a signature stage 24 that determines signature values for the branches of the PRN tree 10 based on a private key 26. In such a case, a secure beacon signal 28 may contain the signatures. Such an approach may prevent spoofing of the secure beacon signal 28 and further enhance privacy.

[0010] Turning now to FIG. 2, a method 30 of operating a beaconing system is shown. The method 30 may be implemented as a module or related component in a set of logic instructions stored in a machine- or computer-readable storage medium such as random access memory (RAM), read only memory (ROM), programmable ROM (PROM), firmware, flash memory, etc., in configurable logic such as, for example, programmable logic arrays (PLAs), field programmable gate arrays (FPGAs), complex programmable logic devices (CPLDs), in fixed-functionality hardware logic using circuit technology such as, for example, application specific integrated circuit (ASIC), complementary metal oxide semiconductor (CMOS) or transistor-transistor logic (TTL) technology, or any combination thereof. For example, computer program code to carry out operations shown in method 30 may be written in any combination of one or more programming languages, including an object oriented programming language such as Java, Smalltalk, C++, ACPI source language (ASL) or the like and conventional procedural programming languages, such as the "C" programming language or similar programming languages.

[0011] Illustrated beacon block 32 provides for obtaining a seed value such as, for example, the root seed value 12 (FIG. 1), from a secure location on a beacon device. As already noted, the secure location may include, for example, memory and/or registers that are unexposed to and/or inaccessible by components not having entropy level access privileges to the beacon device in question. The seed value may be used at beacon block 34 to initiate generation of a PRN tree such as, for example, the PRN tree 10 (FIG. 1), having time-dependent branches. One or more of the time-dependent branches of the PRN tree may be associated with a particular year, a particular day, a particular hour, a particular minute, a particular second, a particular fraction of a second, and so forth.

[0012] In one example, an optional beacon block 36 determines one or more signature values for one or more branches of the PRN tree based on a private key, which may also be obtained from a secure location on the beacon device. Block 36 might involve, for example, deriving (e.g., by hashing) the private key from the seed value so that the beacon device may be provisioned only with the seed value at the time of manufacture and/or update of the beacon device. Illustrated beacon block 38 sends (e.g., broadcasts) a beacon signal based on the PRN tree and a timing schedule that corresponds to the time-dependent branches. If the beacon block 36 is implemented, beacon block 38 may include broadcasting the signature values. Otherwise, beacon block 38 may include broadcasting the leaves (e.g., output of the lowest level branches) of the PRN tree.

[0013] Additionally, an observation block 40 may provide for receiving, via an out-of-band link, a PRN associated with a particular period of time (as well as an indication of the particular period of time). Block 40 may also include receiving a public key and/or digital certificate associated with the beacon device. The out-of-band link may include any communications link (e.g., email, text message, instant message, voice message) other than the link used by the beacon device to send the beacon signal. The particular time period may be, for example, a range of minutes, hours, days, months, years, etc., subscribed to or otherwise obtained on the part of a user of the observation device. For example, if the beacon device is fixed (e.g., located at a stationary vending machine, store, mall, and so forth) and the observation device is mobile (e.g., notebook computer, tablet computer, convertible tablet, mobile Internet device/MID, smart phone, wearable computer, media player, and so forth), the particular time period might correspond to a range of days during which a sales promotion is held at the fixed location. If, on the other hand, the beacon device is mobile (e.g., carried and/or worn by an individual) and the observation device is fixed (e.g., located at a stationary vending machine, store, mall, and so forth) or both devices are mobile, the particular time period may correspond to a range of hours during which the individual carrying the beacon device has consented to permitting the observation device to monitor the beacon signal.

[0014] Illustrated observation block 42 uses the PRN to generate a subset of the PRN tree that corresponds to the particular time period. For example, if the observation device has been authorized to monitor the beacon signal from 5:00PM to 7:00PM on February 23, 2015,

then the observation device may only be given the PRN for the year (2015), day (February 23) and hours (5:00PM and 6:00PM) of that branch of the PRN tree. As a result, the observation device may only be able to recreate the PRNs for the minutes, seconds, etc., to which the observation device has been subscribed.

[0015] A beacon signal may be detected at observation block 44, wherein a public key associated with the beacon device may optionally be used at observation block 46 to verify a digital signature as the beacon signal. The public key may be obtained from, for example, a digital certificate provided by an appropriate certifying authority. Illustrated observation block 48 provides for conducting a proximity determination of whether the detected beacon signal corresponds to one or more time-dependent branches of the subset of the PRN tree. Of particular note is that observation block 48 may be conducted entirely by the observation device and without accessing a remote server. Such an approach may substantially obviate privacy concerns associated with the sharing of beacon signal information.

[0016] Observation block 50 may report the results of the proximity determination (e.g., in order to determine indoor location, provide location attestation, conduct personal tracking, etc.). For example, block 50 may include reporting that a mobile source of the beacon signal traveled within proximity of the observation device during the particular time period if the proximity determination indicates that the beacon signal corresponds to one or more time-dependent branches of the subset of the PRN tree. If, on the other hand, the proximity determination does not indicate that the beacon signal corresponds to one or more time-dependent branches of the subset of the PRN tree, block 50 may involve reporting that the mobile source of the beacon did not travel within proximity of the observation device during the particular time period. Moreover, if the observation device is a mobile device, observation block 50 may involve reporting whether the mobile observation device traveled within proximity of the source of the beacon signal during the particular time period. The illustrated method may therefore provide enhanced security and privacy in a wide variety of settings such as, for example, advertising, promotions, criminal tracking, and so forth.

[0017] The ordering of the illustrated blocks may also vary. For example, the observation device might detect and record all nearby beacon signals, and then later receive one or more PRNs and corresponding public keys from individuals interested in proving that they were nearby at particular time periods. Upon receiving the PRNs and corresponding public keys, the observation blocks 46, 48 and 50 may be conducted for the appropriate time periods.

[0018] Turning now to FIG. 3, a beacon device 52 (52a-52e) is shown. The beacon device 52 may generally implement one or more of the beacon blocks of the method 30 (FIG. 2), already discussed. More particularly, the illustrated beacon device 52 includes a secure location 52a (e.g., memory, register(s), etc., that are unexposed to and/or inaccessible by components not having entropy level access privileges) having a seed value 54 (e.g., true random number). The beacon device 52 may also include a seed retriever 52b coupled to the secure location 52a, wherein the seed retriever 52b is configured to obtain the seed value 54 from the secure location. Additionally, a tree generator 52c coupled to the seed retriever 52b may use the seed value 54 to generate at least a portion of a PRN tree (e.g., depending on memory space and/or power limitations) having time-dependent branches. Although the tree generator 52c might only generate a portion of the PRN tree at a given moment in time due to space and/or power limitations, the illustrated tree generator 52c does not have the same time bounded limitations placed on observing devices with regard to tree generation. In one example, the PRN tree is similar to the PRN tree 10 (FIG. 1), already discussed, and the tree generator 52c includes the PRNGs that generate the branches of the tree. Thus, one or more of the time-dependent branches of the PRN tree may be associated with a particular year, day, hour, second, fraction of a second, and so forth.

[0019] The illustrated beacon device 52 also includes a transmitter 52d (e.g., wireless and/or wired transmitter) coupled to the tree generator 52c, wherein the transmitter 52d is configured to send a beacon signal based on the PRN tree and a timing schedule that corresponds to the time-dependent branches. In one example, the transmitter 52d sends one or more branches of the PRN tree. In another example, the beacon device 52 also includes a security component 52e to determine one or more signature values for one or more branches of the PRN tree based on a private key 56, wherein the transmitter sends the one or more signature values. In such a case, the secure location 52a may further include the private key 56. Additionally, a key generator 58 may derive (e.g., via hashing) the private key 56 from the seed value 54.

[0020] FIG. 4 shows an observation device 60 (60a-60g). The observation device 60 may generally implement one or more of the observation blocks of the method 30 (FIG. 2) for one or more different beacon signals. More particularly, the observation device 60 may include an authorization controller 60a that receives, via an out-of-band link 60b, a PRN associated with a particular time period. The authorization controller 60a may also receive an indication of the particular time period along with the PRN. A partial tree generator 60c (e.g., including one or more PRNGs) may be coupled to the authorization controller 60a, wherein the partial tree generator 60c is configured to use the PRN to generate a subset of a PRN tree that corresponds to the particular time period. Additionally, the observation device 60 may include a receiver 60e (e.g., wireless Bluetooth receiver) to detect a beacon signal and a proximity verifier 60d to conduct a proximity determination of whether the detected beacon signal corresponds to one or more time-dependent branches of the subset of the PRN tree. As already noted, one or

more of the time-dependent branches may be associated with a particular year, day, hour, second, fraction of a second, and so forth.

[0021] In one example, the observation device 60 also includes a signature verifier 60f to use a public key associated with a beacon device to verify a digital signature as the beacon signal. Additionally, the proximity verifier 60d may use a report interface 60g (e.g., display, speaker, printer, mass storage, network controller, etc.), to report that a mobile source of the beacon signal traveled within proximity of the observation device 60 during the particular time period if the proximity determination indicates that the beacon signal corresponds to one or more time-dependent branches of the subset of the PRN tree. In another example, if the observation device 60 is a mobile observation device, the proximity verifier 60d may use the report interface 60g to report whether the mobile observation device traveled within proximity of a source of the beacon signal during the particular time period.

[0022] Additionally, portions of the beacon device 52 (FIG. 3) and/or the observation device 60 may be distributed across multiple platforms. For example, one could use a phone, for example, to generate PRNG trees and signatures, or to verify them, wherein a separate device might transmit and/or receive beacon signals and pass them on to another device for computation.

[0023] FIG. 5 illustrates a processor core 200 according to one embodiment. The processor core 200 may be the core for any type of processor, such as a microprocessor, an embedded processor, a digital signal processor (DSP), a network processor, or other device to execute code. Although only one processor core 200 is illustrated in FIG. 5, a processing element may alternatively include more than one of the processor core 200 illustrated in FIG. 5. The processor core 200 may be a single-threaded core or, for at least one embodiment, the processor core 200 may be multithreaded in that it may include more than one hardware thread context (or "logical processor") per core.

[0024] FIG. 5 also illustrates a memory 270 coupled to the processor core 200. The memory 270 may be any of a wide variety of memories (including various layers of memory hierarchy) as are known or otherwise available to those of skill in the art. The memory 270 may include one or more code 213 instruction(s) to be executed by the processor core 200, wherein the code 213 may implement the beacon blocks or the observation blocks of the method 30 (FIG. 2), already discussed. In one example, the memory 270 is non-flash memory. The processor core 200 follows a program sequence of instructions indicated by the code 213. Each instruction may enter a front end portion 210 and be processed by one or more decoders 220. The decoder 220 may generate as its output a micro operation such as a fixed width micro operation in a predefined format, or may generate other instructions, microinstructions, or control signals which reflect the original code instruction. The illustrated front end portion 210 also includes register renaming logic 225 and scheduling logic 230, which generally allocate resources and queue the operation corresponding to the convert instruction for execution.

[0025] The processor core 200 is shown including execution logic 250 having a set of execution units 255-1 through 255-N. Some embodiments may include a number of execution units dedicated to specific functions or sets of functions. Other embodiments may include only one execution unit or one execution unit that can perform a particular function. The illustrated execution logic 250 performs the operations specified by code instructions.

[0026] After completion of execution of the operations specified by the code instructions, back end logic 260 retires the instructions of the code 213. In one embodiment, the processor core 200 allows out of order execution but requires in order retirement of instructions. Retirement logic 265 may take a variety of forms as known to those of skill in the art (e.g., re-order buffers or the like). In this manner, the processor core 200 is transformed during execution of the code 213, at least in terms of the output generated by the decoder, the hardware registers and tables utilized by the register renaming logic 225, and any registers (not shown) modified by the execution logic 250.

[0027] Although not illustrated in FIG. 5, a processing element may include other elements on chip with the processor core 200. For example, a processing element may include memory control logic along with the processor core 200. The processing element may include I/O control logic and/or may include I/O control logic integrated with memory control logic. The processing element may also include one or more caches.

[0028] Referring now to FIG. 6, shown is a block diagram of a computing system 1000 embodiment in accordance with an embodiment. Shown in FIG. 6 is a multiprocessor system 1000 that includes a first processing element 1070 and a second processing element 1080. While two processing elements 1070 and 1080 are shown, it is to be understood that an embodiment of the system 1000 may also include only one such processing element.

[0029] The system 1000 is illustrated as a point-to-point interconnect system, wherein the first processing element 1070 and the second processing element 1080 are coupled via a point-to-point interconnect 1050. It should be understood that any or all of the interconnects illustrated in FIG. 6 may be implemented as a multi-drop bus rather than point-to-point interconnect.

[0030] As shown in FIG. 6, each of processing elements 1070 and 1080 may be multicore processors, including first and second processor cores (i.e., processor cores 1074a and 1074b and processor cores 1084a and 1084b). Such cores 1074a, 1074b, 1084a, 1084b may be configured to execute instruction code in a manner similar to that discussed above in connection with FIG. 5.

[0031] Each processing element 1070, 1080 may include at least one shared cache 1896a, 1896b. The shared cache 1896a, 1896b may store data (e.g., instruc-

tions) that are utilized by one or more components of the processor, such as the cores 1074a, 1074b and 1084a, 1084b, respectively. For example, the shared cache 1896a, 1896b may locally cache data stored in a memory 1032, 1034 for faster access by components of the processor. In one or more embodiments, the shared cache 1896a, 1896b may include one or more mid-level caches, such as level 2 (L2), level 3 (L3), level 4 (L4), or other levels of cache, a last level cache (LLC), and/or combinations thereof.

[0032] While shown with only two processing elements 1070, 1080, it is to be understood that the scope of the embodiments are not so limited. In other embodiments, one or more additional processing elements may be present in a given processor. Alternatively, one or more of processing elements 1070, 1080 may be an element other than a processor, such as an accelerator or a field programmable gate array. For example, additional processing element(s) may include additional processors(s) that are the same as a first processor 1070, additional processor(s) that are heterogeneous or asymmetric to processor a first processor 1070, accelerators (such as, e.g., graphics accelerators or digital signal processing (DSP) units), field programmable gate arrays, or any other processing element. There can be a variety of differences between the processing elements 1070, 1080 in terms of a spectrum of metrics of merit including architectural, micro architectural, thermal, power consumption characteristics, and the like. These differences may effectively manifest themselves as asymmetry and heterogeneity amongst the processing elements 1070, 1080. For at least one embodiment, the various processing elements 1070, 1080 may reside in the same die package.

[0033] The first processing element 1070 may further include memory controller logic (MC) 1072 and point-to-point (P-P) interfaces 1076 and 1078. Similarly, the second processing element 1080 may include a MC 1082 and P-P interfaces 1086 and 1088. As shown in FIG. 6, MC's 1072 and 1082 couple the processors to respective memories, namely a memory 1032 and a memory 1034, which may be portions of main memory locally attached to the respective processors. While the MC 1072 and 1082 is illustrated as integrated into the processing elements 1070, 1080, for alternative embodiments the MC logic may be discrete logic outside the processing elements 1070, 1080 rather than integrated therein.

[0034] The first processing element 1070 and the second processing element 1080 may be coupled to an I/O subsystem 1090 via P-P interconnects 1076 1086, respectively. As shown in FIG. 6, the I/O subsystem 1090 includes P-P interfaces 1094 and 1098. Furthermore, I/O subsystem 1090 includes an interface 1092 to couple I/O subsystem 1090 with a high performance graphics engine 1038. In one embodiment, bus 1049 may be used to couple the graphics engine 1038 to the I/O subsystem 1090. Alternately, a point-to-point interconnect may couple these components.

[0035] In turn, I/O subsystem 1090 may be coupled to a first bus 1016 via an interface 1096. In one embodiment, the first bus 1016 may be a Peripheral Component Interconnect (PCI) bus, or a bus such as a PCI Express bus or another third generation I/O interconnect bus, although the scope of the embodiments are not so limited.

[0036] As shown in FIG. 6, various I/O devices 1014 (e.g., cameras, sensors) may be coupled to the first bus 1016, along with a bus bridge 1018 which may couple the first bus 1016 to a second bus 1020. In one embodiment, the second bus 1020 may be a low pin count (LPC) bus. Various devices may be coupled to the second bus 1020 including, for example, a keyboard/mouse 1012, communication device(s) 1026, and a data storage unit 1019 such as a disk drive or other mass storage device which may include code 1030, in one embodiment. The illustrated code 1030 may implement the beacon blocks or the observation blocks of the method 30 (FIG. 2), already discussed, and may be similar to the code 213 (FIG. 5), already discussed. Further, an audio I/O 1024 may be coupled to second bus 1020 and a battery 1010 may supply power to the computing system 1000.

[0037] Note that other embodiments are contemplated. For example, instead of the point-to-point architecture of FIG. 6, a system may implement a multi-drop bus or another such communication topology. Also, the elements of FIG. 6 may alternatively be partitioned using more or fewer integrated chips than shown in FIG. 6.

[0038] Thus, techniques described herein may provide a seemingly random and changing beacon signal for each individual beacon device, where the sequence of seemingly random values may be validated as belonging to a given group associated with a location and/or person. Because the beacon signal is dynamic, unpredictable and time-bounded, it may provide probabilistic evidence of a person being in a given place without advertising that fact to a service. In other words, the beacon device may emit a changing stream of seemingly random numbers that may be associated with a single value by someone authorized to do so. Moreover, the stream may not require a server to associate the values contained therein with the single value. To preserve privacy, access to beacon identity may be limited to a specific time frame and also does not require a server to convert the stream into an identity. Additionally, digitally signing the stream may enable verification of the identity of a beacon device without permitting the verifier to masquerade as that beacon device.

[0039] Indeed, techniques may provide after-the-fact proof that an anonymous person was at a specific place at a specific time. For example, a location specific infrastructure may benefit from being able to observe people carrying beacon devices nearby, without knowing their identity, yet being able to prove later that they were present. In one such example, a vending machine might offer incentives to those close enough to the machine to observe advertising displayed on the machine. Another example may be a system located in a coffee shop that

rewards customers for frequent visits. Such a system might offer an occasional free drink to people who spend a considerable amount of time nearby. Of particular note is that using asymmetric cryptography as described herein may ensure that such systems are not "gamed" into giving away incentives in excess of incentives actually earned. By using signed time-bounded PRN trees, protection against such unauthorized activity may be obtained.

[0040] Embodiments are applicable for use with all types of semiconductor integrated circuit ("IC") chips. Examples of these IC chips include but are not limited to processors, controllers, chipset components, programmable logic arrays (PLAs), memory chips, network chips, systems on chip (SoCs), SSD/NAND controller ASICs, and the like. In addition, in some of the drawings, signal conductor lines are represented with lines. Some may be different, to indicate more constituent signal paths, have a number label, to indicate a number of constituent signal paths, and/or have arrows at one or more ends, to indicate primary information flow direction. This, however, should not be construed in a limiting manner. Rather, such added detail may be used in connection with one or more exemplary embodiments to facilitate easier understanding of a circuit. Any represented signal lines, whether or not having additional information, may actually comprise one or more signals that may travel in multiple directions and may be implemented with any suitable type of signal scheme, e.g., digital or analog lines implemented with differential pairs, optical fiber lines, and/or single-ended lines.

[0041] Example sizes/models/values/ranges may have been given, although embodiments are not limited to the same. As manufacturing techniques (e.g., photolithography) mature over time, it is expected that devices of smaller size could be manufactured. In addition, well known power/ground connections to IC chips and other components may or may not be shown within the figures, for simplicity of illustration and discussion, and so as not to obscure certain aspects of the embodiments. Further, arrangements may be shown in block diagram form in order to avoid obscuring embodiments, and also in view of the fact that specifics with respect to implementation of such block diagram arrangements are highly dependent upon the computing system within which the embodiment is to be implemented, i.e., such specifics should be well within purview of one skilled in the art. Where specific details (e.g., circuits) are set forth in order to describe example embodiments, it should be apparent to one skilled in the art that embodiments can be practiced without, or with variation of, these specific details. The description is thus to be regarded as illustrative instead of limiting.

[0042] The term "coupled" may be used herein to refer to any type of relationship, direct or indirect, between the components in question, and may apply to electrical, mechanical, fluid, optical, electromagnetic, electromechanical or other connections. In addition, the terms "first", "second", etc. may be used herein only to facilitate discussion, and carry no particular temporal or chronological significance unless otherwise indicated.

[0043] As used in this application and in the claims, a list of items joined by the term "one or more of' may mean any combination of the listed terms. For example, the phrases "one or more of A, B or C" may mean A; B; C; A and B; A and C; B and C; or A, B and C.

[0044] Those skilled in the art will appreciate from the foregoing description that the broad techniques of the embodiments can be implemented in a variety of forms. Therefore, while the embodiments have been described in connection with particular examples thereof, the true scope of the embodiments should not be so limited since other modifications will become apparent to the skilled practitioner upon a study of the drawings, specification, and following claims.

[0045] The invention is defined by the appended claims.

Claims

1. An observation device (60) comprising:

an authorization controller (60a) to receive, via an out-of-band link, a pseudo random number associated with a particular time period;
a partial tree generator (60c) coupled to the authorization controller, the partial tree generator to use the pseudo random number to generate a subset of a pseudo random number tree that corresponds to the particular time period; and
a proximity verifier (60d) coupled to the partial tree generator, the proximity verifier to conduct a proximity determination of whether a detected beacon signal corresponds to one or more time-dependent branches of the subset of the pseudo random number tree;

wherein either (i) the proximity verifier is to report that a mobile source of the beacon signal traveled within proximity of the observation device during the particular time period if the proximity determination indicates that the beacon signal corresponds to one or more time-dependent branches of the subset of the pseudo random number tree; or (ii)
the observation device is a mobile observation device, and wherein the proximity verifier is to report that the mobile observation device traveled within proximity of a source of the beacon signal during the particular time period if the proximity determination indicates that the beacon signal corresponds to one or more time-dependent branches of the subset of the pseudo random number tree.

2. The observation device of claim 1, wherein one or more of the time-dependent branches is to be asso-

ciated with one of a particular year, a particular day, a particular hour, a particular minute, a particular second or a particular fraction of a second.

3. The observation device of claim 1, further including a signature verifier to use a public key associated with a beacon device to verify a digital signature as the beacon signal.

4. At least one computer readable storage medium comprising a set of instructions which, when executed by an observation device, cause the observation device to:

receive, via an out-of-band link, a pseudo random number associated with a particular time period;
use the pseudo random number to generate a subset of a pseudo random number tree that corresponds to the particular time period; and
conduct a proximity determination of whether a detected beacon signal corresponds to one or more time-dependent branches of the subset of the pseudo random number tree;

wherein either (i) the instructions, when executed, cause the observation device to report that a mobile source of the beacon signal traveled within proximity of the observation device during the particular time period if the proximity determination indicates that the beacon signal corresponds to one or more time-dependent branches of the subset of the pseudo random number tree; or
(ii) the observation device is to be a mobile observation device, and wherein the instructions, when executed, cause the observation device to report that the mobile observation device traveled within proximity of a source of the beacon signal during the particular time period if the proximity determination indicates that the beacon signal corresponds to one or more time-dependent branches of the subset of the pseudo random number tree.

5. The at least one computer readable storage medium of claim 4, wherein one or more of the time-dependent branches is to be associated with one of a particular year, a particular day, a particular hour, a particular minute, a particular second or a particular fraction of a second.

6. The at least one computer readable storage medium of claim 4, wherein the instructions, when executed, cause the observation device to use a public key associated with a beacon device to verify a digital signature as the beacon signal.

Patentansprüche

1. Beobachtungsvorrichtung (60), umfassend:

eine Autorisierungssteuerung (60a) zum Empfangen, über eine Verknüpfung außerhalb des Bands, einer mit einer besonderen Zeitperiode assoziierten Pseudozufallszahl;
einen Teilbaumgenerator (60c), gekoppelt an die Autorisierungssteuerung, wobei der Teilbaumgenerator die Pseudozufallszahl verwenden soll, eine Teilmenge eines Pseudozufallszahlenbaums zu erzeugen, der mit der besonderen Zeitperiode korrespondiert; und
einen Näheverifizierer (60d), gekoppelt an den Teilbaumgenerator, wobei der Näheverifizierer eine Nähebestimmung dahingehend durchführen soll, ob ein detektiertes Bakensignal mit einem oder mehreren zeitabhängigen Zweigen der Teilmenge des Pseudozufallszahlenbaums korrespondiert;
wobei entweder (i) der Näheverifizierer berichten soll, dass sich eine mobile Quelle des Bakensignals in die Nähe der Beobachtungsvorrichtung während der besonderen Zeitperiode bewegt hat, wenn die Nähebestimmung angibt, dass das Bakensignal mit einem oder mehreren zeitabhängigen Zweigen der Teilmenge des Pseudozufallszahlenbaums korrespondiert; oder (ii)
die Beobachtungsvorrichtung eine mobile Beobachtungsvorrichtung ist, und wobei der Näheverifizierer berichten soll, dass die mobile Beobachtungsvorrichtung sich in die Nähe einer Quelle des Bakensignals während der besonderen Zeitperiode bewegt hat, wenn die Nähebestimmung angibt, dass das Bakensignal mit einem oder mehreren zeitabhängigen Zweigen der Teilmenge des Pseudozufallszahlenbaums korrespondiert.

2. Beobachtungsvorrichtung nach Anspruch 1, wobei einer oder mehrere der zeitabhängigen Zweige mit einem eines besonderen Jahres, eines besonderen Tags, einer besonderen Stunde, einer besonderen Minute, einer besonderen Sekunde oder einer besonderen Fraktion einer Sekunde assoziiert werden soll.

3. Beobachtungsvorrichtung nach Anspruch 1, ferner enthaltend, dass ein Signaturverifizierer einen mit einer Bakenvorrichtung assoziierten öffentlichen Schlüssel verwenden soll, um eine digitale Signatur als das Bakensignal zu verifizieren.

4. Mindestens ein computerlesbares Speichermedium, umfassend eine Menge von Anweisungen, die, wenn sie durch eine Beobachtungsvorrichtung aus-

geführt werden, bewirken, dass die Beobachtungsvorrichtung Folgendes durchführt:

Empfangen, über eine Verknüpfung außerhalb des Bands, einer mit einer besonderen Zeitperiode assoziierten Pseudozufallszahl;
Verwenden der Pseudozufallszahl, eine Teilmenge eines Pseudozufallszahlenbaums zu erzeugen, der mit der besonderen Zeitperiode korrespondiert; und
Durchführen einer Nähebestimmung dahingehen, ob ein detektiertes Bakensignal mit einem oder mehreren zeitabhängigen Zweigen der Teilmenge des Pseudozufallszahlenbaums korrespondiert;
wobei entweder (i) die Anweisungen, wenn sie ausgeführt werden, bewirken, dass die Beobachtungsvorrichtung berichtet, dass sich eine mobile Quelle des Bakensignals in die Nähe der Beobachtungsvorrichtung während der besonderen Zeitperiode bewegt hat, wenn die Nähebestimmung angibt, dass das Bakensignal mit einem oder mehreren zeitabhängigen Zweigen der Teilmenge des Pseudozufallszahlenbaums korrespondiert; oder
(ii) die Beobachtungsvorrichtung eine mobile Beobachtungsvorrichtung sein soll, und wobei die Anweisungen, wenn sie ausgeführt werden, bewirken, dass die Beobachtungsvorrichtung berichtet, dass die mobile Beobachtungsvorrichtung sich in die Nähe einer Quelle des Bakensignals während der besonderen Zeitperiode bewegt hat, wenn die Nähebestimmung angibt, dass das Bakensignal mit einem oder mehreren zeitabhängigen Zweigen der Teilmenge des Pseudozufallszahlenbaums korrespondiert.

5. Mindestens ein computerlesbares Speichermedien nach Anspruch 4, wobei einer oder mehrere der zeitabhängigen Zweige mit einem eines besonderen Jahres, eines besonderen Tags, einer besonderen Stunde, einer besonderen Minute, einer besonderen Sekunde oder einer besonderen Fraktion einer Sekunde assoziiert werden soll.

6. Mindestens ein computerlesbares Speichermedien nach Anspruch 4, wobei die Anweisungen, wenn sie ausgeführt werden, bewirken, dass die Beobachtungsvorrichtung einen mit einer Bakenvorrichtung assoziierten öffentlichen Schlüssel verwendet, um eine digitale Signatur als das Bakensignal zu verifizieren.

Revendications

1. Dispositif (60) d'observation comportant :

un contrôleur (60a) d'autorisation servant à recevoir, via une liaison hors bande, un nombre pseudo-aléatoire associé à une période particulière ;
un générateur (60c) d'arbre partiel couplé au contrôleur d'autorisation, le générateur d'arbre partiel servant à utiliser le nombre pseudo-aléatoire pour générer un sous-ensemble d'un arbre de nombres pseudo-aléatoires qui correspond à la période particulière ; et
un vérificateur (60d) de proximité couplé au générateur d'arbre partiel, le vérificateur de proximité servant à effectuer une détermination de proximité selon laquelle un signal de balise détecté correspond ou non à une ou plusieurs branches dépendantes du temps du sous-ensemble de l'arbre de nombres pseudo-aléatoires ;
caractérisé soit en ce que (i) le vérificateur de proximité sert à rendre compte du fait qu'une source mobile du signal de balise a circulé à proximité du dispositif d'observation pendant la période particulière si la détermination de proximité indique que le signal de balise correspond à une ou plusieurs branches dépendantes du temps du sous-ensemble de l'arbre de nombres pseudo-aléatoires ;
soit en ce que (ii) le dispositif d'observation est un dispositif mobile d'observation, et en ce que le vérificateur de proximité sert à rendre compte du fait que le dispositif mobile d'observation a circulé à proximité d'une source du signal de balise pendant la période particulière si la détermination de proximité indique que le signal de balise correspond à une ou plusieurs branches dépendantes du temps du sous-ensemble de l'arbre de nombres pseudo-aléatoires.

2. Dispositif d'observation selon la revendication 1, une ou plusieurs des branches dépendantes du temps devant être associées à une période parmi une année particulière, un jour particulier, une heure particulière, une minute particulière, une seconde particulière et une fraction de seconde particulière.

3. Dispositif d'observation selon la revendication 1, comprenant en outre un vérificateur de signature servant à utiliser une clé publique associée à un dispositif de balise pour vérifier une signature numérique en tant que signal de balise.

4. Au moins un support de stockage lisible par ordinateur comportant un ensemble d'instructions qui, lorsqu'elles sont exécutées par un dispositif d'observation, amènent le dispositif d'observation à :

recevoir, via une liaison hors bande, un nombre pseudo-aléatoire associé à une période

particulière ;
utiliser le nombre pseudo-aléatoire pour générer un sous-ensemble d'un arbre de nombres pseudo-aléatoires qui correspond à la période particulière ; et
effectuer une détermination de proximité selon laquelle un signal de balise détecté correspond ou non à une ou plusieurs branches dépendantes du temps du sous-ensemble de l'arbre de nombres pseudo-aléatoires ;
caractérisé soit en ce que (i) les instructions, lorsqu'elles sont exécutées, amènent le dispositif d'observation à rendre compte du fait qu'une source mobile du signal de balise a circulé à proximité du dispositif d'observation pendant la période particulière si la détermination de proximité indique que le signal de balise correspond à une ou plusieurs branches dépendantes du temps du sous-ensemble de l'arbre de nombres pseudo-aléatoires ;
soit en ce que (ii) le dispositif d'observation est destiné à être un dispositif mobile d'observation, et en ce que les instructions, lorsqu'elles sont exécutées, amènent le dispositif d'observation à rendre compte du fait que le dispositif mobile d'observation a circulé à proximité d'une source du signal de balise pendant la période particulière si la détermination de proximité indique que le signal de balise correspond à une ou plusieurs branches dépendantes du temps du sous-ensemble de l'arbre de nombres pseudo-aléatoires.

5. Le ou les supports de stockage lisibles par ordinateur selon la revendication 4, une ou plusieurs des branches dépendantes du temps devant être associées à une période parmi une année particulière, un jour particulier, une heure particulière, une minute particulière, une seconde particulière et une fraction de seconde particulière.

6. Le ou les supports de stockage lisibles par ordinateur selon la revendication 4, les instructions, lorsqu'elles sont exécutées, amenant le dispositif d'observation à utiliser une clé publique associée à un dispositif de balise pour vérifier une signature numérique en tant que signal de balise.

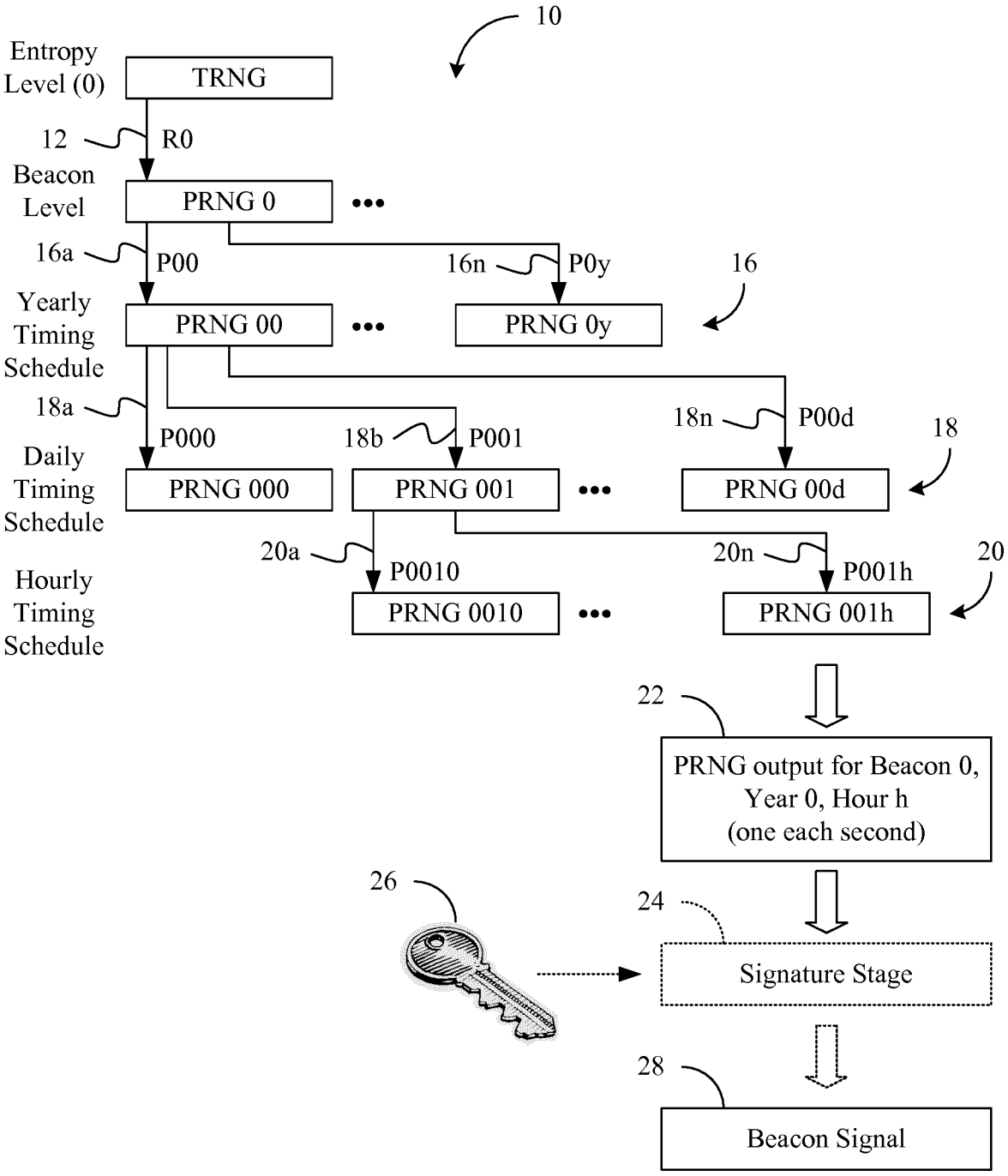

10
Entropy Level (0)
TRNG
12
R0
Beacon Level
PRNG 0
16a
P00
16n
P0y
16
Yearly Timing Schedule
PRNG 00
PRNG 0y
18a
P000
18b
P001
18n
P00d
18
Daily Timing Schedule
PRNG 000
PRNG 001
PRNG 00d
20a
P0010
20n
P001h
20
Hourly Timing Schedule
PRNG 0010
PRNG 001h
22
PRNG output for Beacon 0, Year 0, Hour h (one each second)
26
24
Signature Stage
28
Beacon Signal

FIG. 1

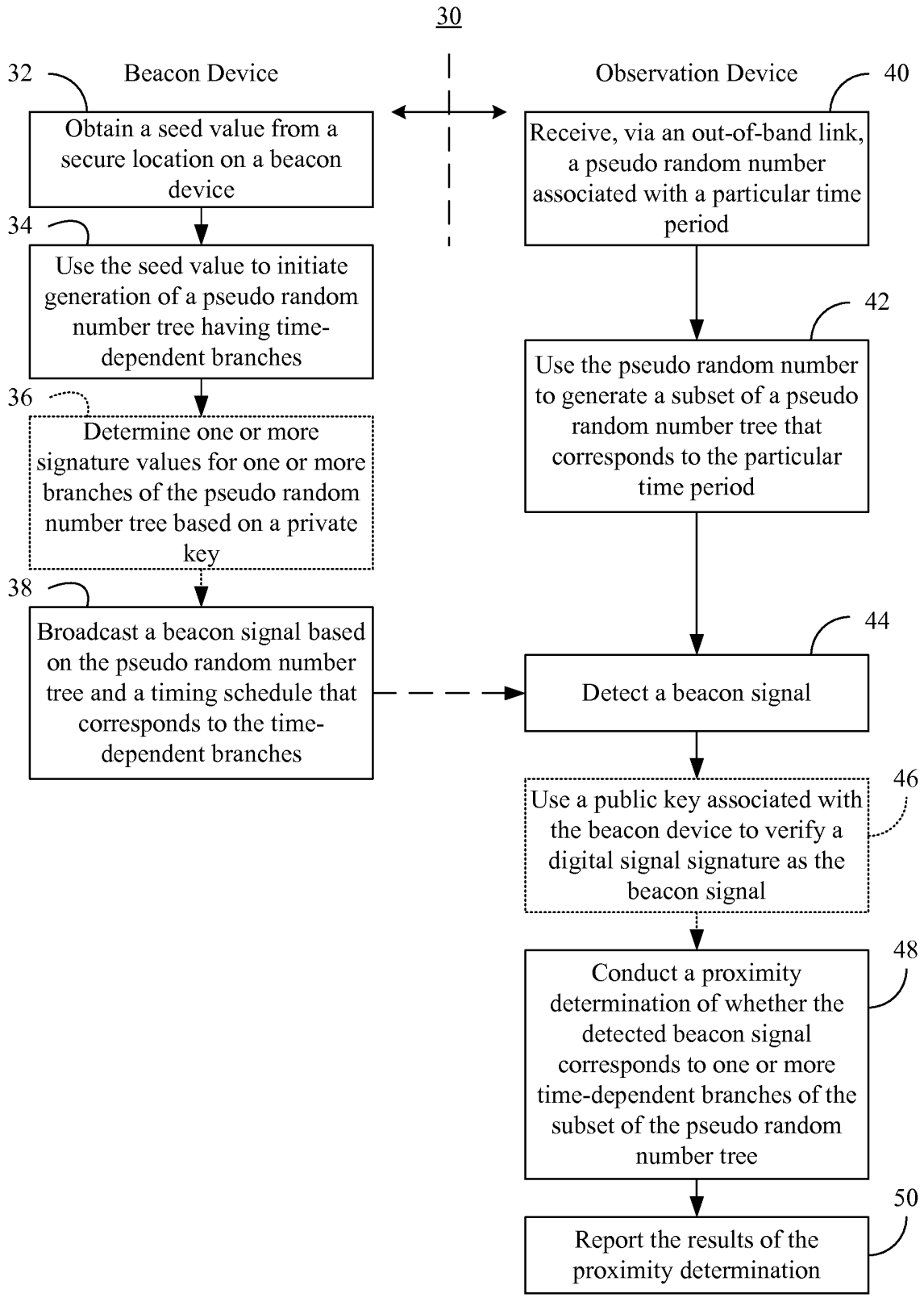

30
32
Beacon Device
Obtain a seed value from a secure location on a beacon device
34
Use the seed value to initiate generation of a pseudo random number tree having time-dependent branches
36
Determine one or more signature values for one or more branches of the pseudo random number tree based on a private key
38
Broadcast a beacon signal based on the pseudo random number tree and a timing schedule that corresponds to the time-dependent branches
Observation Device
40
Receive, via an out-of-band link, a pseudo random number associated with a particular time period
42
Use the pseudo random number to generate a subset of a pseudo random number tree that corresponds to the particular time period
44
Detect a beacon signal
46
Use a public key associated with the beacon device to verify a digital signal signature as the beacon signal
48
Conduct a proximity determination of whether the detected beacon signal corresponds to one or more time-dependent branches of the subset of the pseudo random number tree
50
Report the results of the proximity determination

FIG. 2

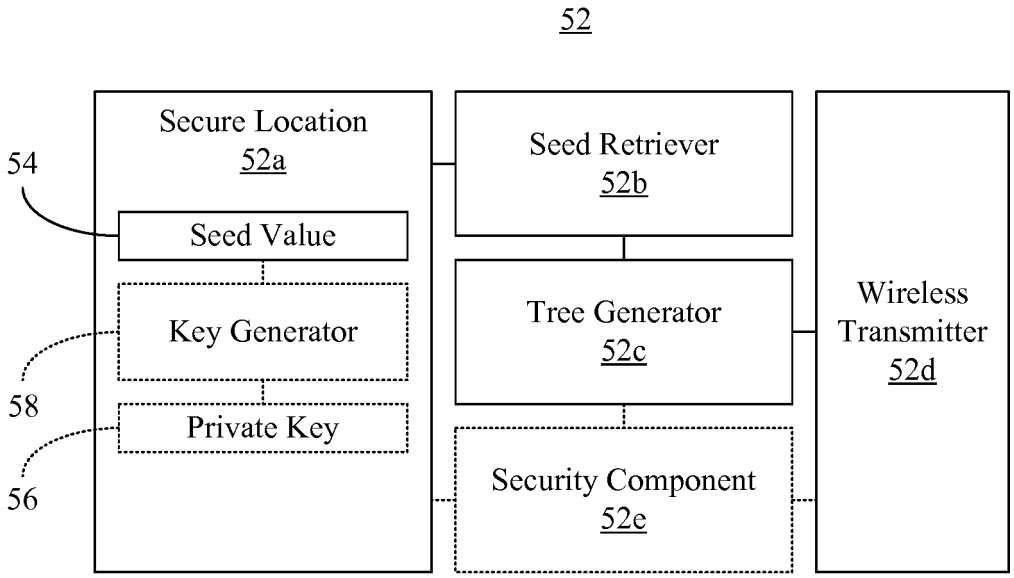

52
Secure Location
52a
54
Seed Value
Key Generator
58
Private Key
56
Seed Retriever
52b
Tree Generator
52c
Security Component
52e
Wireless
Transmitter
52d

FIG. 3

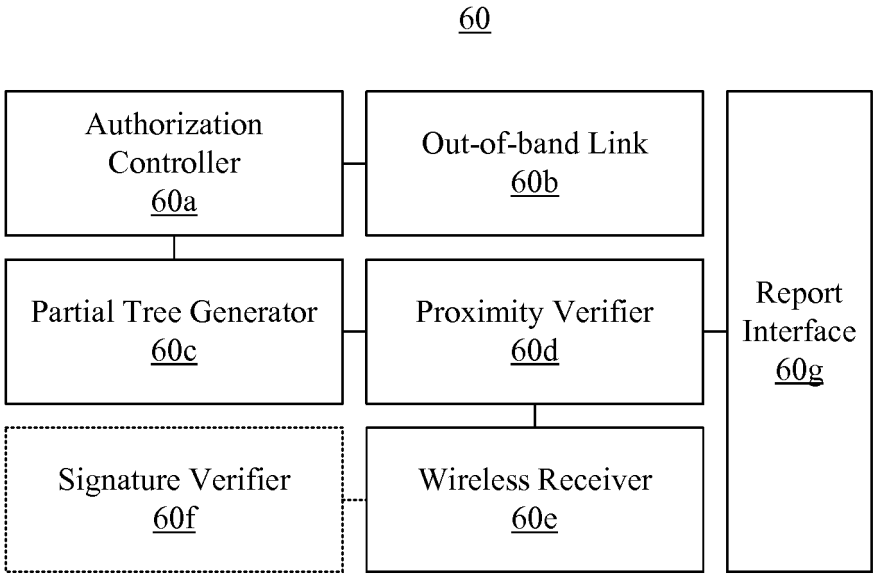

60
Authorization
Controller
60a
Out-of-band Link
60b
Partial Tree Generator
60c
Proximity Verifier
60d
Report
Interface
60g
Signature Verifier
60f
Wireless Receiver
60e

FIG. 4

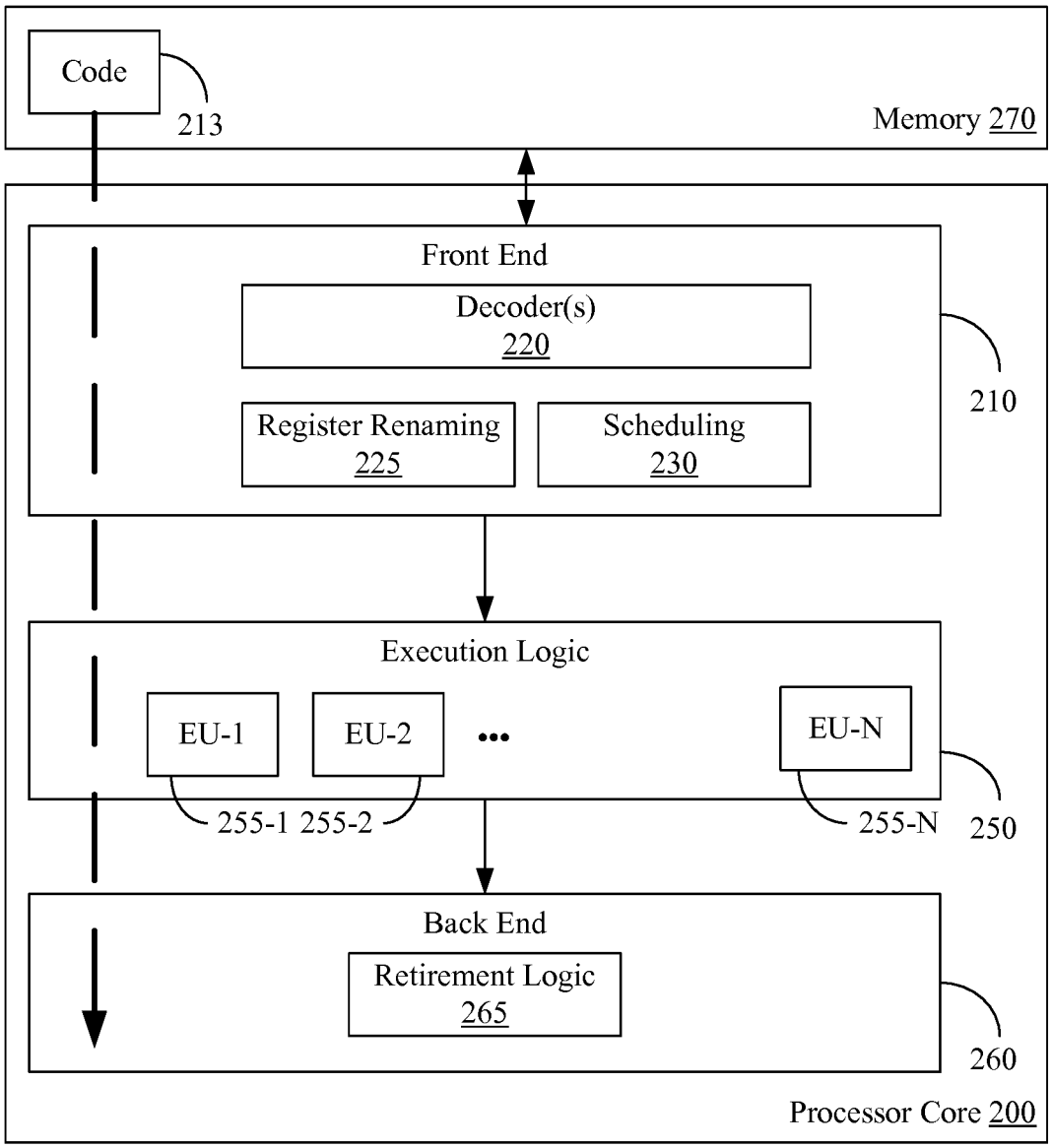
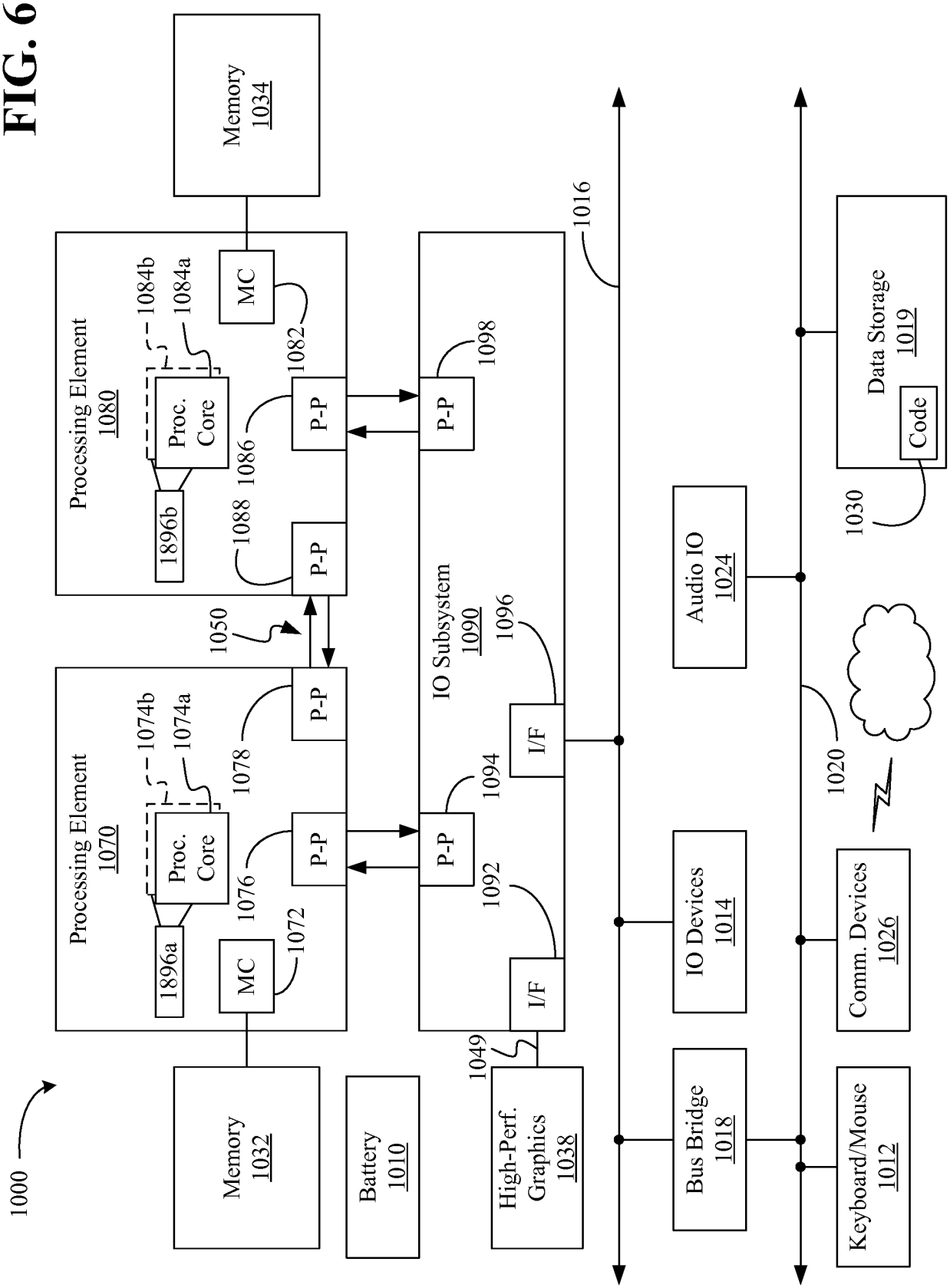

Code
213
Memory 270
Front End
Decoder(s)
220
Register Renaming
225
Scheduling
230
210
Execution Logic
EU-1
EU-2
...
EU-N
255-1
255-2
255-N
250
Back End
Retirement Logic
265
260
Processor Core 200

FIG. 5

FIG. 6


1000
Memory 1034
Processing Element 1080
MC
1082
1084b
1084a
Proc. Core
1896b
1086
P-P
1088
P-P
1050
Processing Element 1070
1074b
1074a
Proc. Core
1896a
MC
1072
1076
P-P
1078
P-P
Memory 1032
Battery 1010
IO Subsystem 1090
P-P
1098
P-P
1094
I/F
1096
1092
I/F
1049
High-Perf. Graphics 1038
1016
Audio IO 1024
IO Devices 1014
Bus Bridge 1018
Keyboard/Mouse 1012
Comm. Devices 1026
1020
Data Storage 1019
Code
1030

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 20141245020 A1 **[0003]**