(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 November 2018 (29.11.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/217535 A1

(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/US2018/033138

(22) International Filing Date:
17 May 2018 (17.05.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/511,734 26 May 2017 (26.05.2017) US

(71) Applicant: **MICROCHIP TECHNOLOGY INCORPORATED** [US/US]; 2355 West Chandler Blvd, Chandler, Arizona 85224 (US).

(72) Inventor: **CHEN, Huiming**; 3264 Silver Pine Trail, Colorado Springs, Colorado 80920 (US).

(74) Agent: **GUTKE, Steven W.** et al.; 230 S. 500 E., Suite 300, Salt Lake City, Utah 84102 (US).

(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, 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).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

(54) Title: SYSTEM, METHOD, AND APPARATUS FOR OBFUSCATING DEVICE OPERATIONS

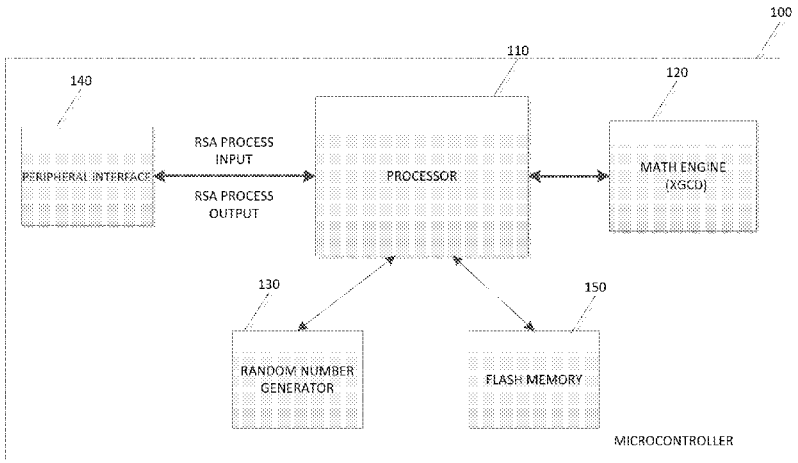

FIG. 1

(57) Abstract: The embodiments of the present disclosure relate generally to systems and methods for obfuscating the operation of a device, in particular, timing and power consumption information.

[Continued on next page]

WO 2018/217535 A1

Published:
— *with international search report (Art. 21(3))*

SYSTEM, METHOD, AND APPARATUS FOR OBFUSCATING DEVICE OPERATIONS

PRIORITY CLAIM

This application claims the benefit under 35 U.S.C. §119(e) of U.S. Provisional Patent Application Serial No. 62/511,734, filed May 26, 2017, the disclosure of which is hereby incorporated herein in its entirety by this reference.

TECHNICAL FIELD

The embodiments of the present disclosure relate generally to systems and methods for obfuscating the operation of a device, in particular, timing and power consumption information.

BACKGROUND

Many calculations are used in cryptography, including to calculate private keys, sub-keys, and public keys. Devices that perform such calculations are employed to facilitate secure and trusted communication among devices.

BRIEF DESCRIPTION OF THE DRAWINGS

The purpose and advantages of the embodiments of the disclosure will be apparent to one of ordinary skill in the art from the summary in conjunction with the accompanying drawings:

FIG. 1 illustrates a secure system that implements various processes in accordance with embodiments of the disclosure.

FIG. 2 illustrates a processor configured to perform various processes in accordance with embodiments of the disclosure.

FIG. 3 illustrates a flowchart of a method of performing a cryptographic process by the system of FIG. 1, according to an embodiment of the disclosure.

FIGS. 4A and 4B illustrate the power consumption difference between two cryptographic processes executed in accordance with embodiments of the disclosure.

MODE(S) FOR CARRYING OUT THE INVENTION

In the following detailed description, reference is made to the accompanying drawings, which form a part hereof, and in which are shown, by way of illustration,

specific examples of embodiments in which the present disclosure may be practiced. These embodiments are described in sufficient detail to enable a person of ordinary skill in the art to practice the present disclosure. However, other embodiments may be utilized, and structural, material, and process changes may be made without departing from the scope of the disclosure. The illustrations presented herein are not meant to be actual views of any particular method, system, device, or structure, but are merely idealized representations that are employed to describe the embodiments of the present disclosure. The drawings presented herein are not necessarily drawn to scale. Similar structures or components in the various drawings may retain the same or similar numbering for the convenience of the reader; however, the similarity in numbering does not mean that the structures or components are necessarily identical in size, composition, configuration, or any other property.

It will be readily understood that the components of the embodiments as generally described herein and illustrated in the drawings could be arranged and designed in a wide variety of different configurations. Thus, the following description of various embodiments is not intended to limit the scope of the present disclosure, but is merely representative of various embodiments. While the various aspects of the embodiments may be presented in drawings, the drawings are not necessarily drawn to scale unless specifically indicated.

Furthermore, specific implementations shown and described are only examples and should not be construed as the only way to implement the present disclosure unless specified otherwise herein. Elements, circuits, and functions may be shown in block diagram form in order not to obscure the present disclosure in unnecessary detail. Conversely, specific implementations shown and described are exemplary only and should not be construed as the only way to implement the present disclosure unless specified otherwise herein. Additionally, block definitions and partitioning of logic between various blocks is exemplary of a specific implementation. It will be readily apparent to one of ordinary skill in the art that the present disclosure may be practiced by numerous other partitioning solutions. For the most part, details concerning timing considerations and the like have been omitted where such details are not necessary to obtain a complete understanding of the present disclosure and are within the abilities of persons of ordinary skill in the relevant art.

Those of ordinary skill in the art would understand that information and signals may be represented using any of a variety of different technologies and techniques. For example, data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout this description may be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof. Some drawings may illustrate signals as a single signal for clarity of presentation and description. It will be understood by a person of ordinary skill in the art that the signal may represent a bus of signals, wherein the bus may have a variety of bit widths and the present disclosure may be implemented on any number of data signals including a single data signal.

The various illustrative logical blocks, modules, and circuits described in connection with the embodiments disclosed herein may be implemented or performed with a general-purpose processor, a special-purpose processor, a Digital Signal Processor (DSP), an Integrated Circuit (IC), an Application Specific Integrated Circuit (ASIC), a Field Programmable Gate Array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general-purpose processor (may also be referred to herein as a host processor or simply a host) may be a microprocessor, but in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing devices, such as a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration. A general-purpose computer including a processor is considered a special-purpose computer while the general-purpose computer is configured to execute computing instructions (*e.g.*, software code) related to embodiments of the present disclosure.

The embodiments may be described in terms of a process that is depicted as a flowchart, a flow diagram, a structure diagram, or a block diagram. Although a flowchart may describe operational acts as a sequential process, many of these acts can be performed in another sequence, in parallel, or substantially concurrently. In addition, the order of the acts may be re-arranged. A process may correspond to a method, a thread, a function, a procedure, a subroutine, a subprogram, etc. Furthermore, the methods disclosed herein may be implemented in hardware, software, or both. If implemented in software, the

functions may be stored or transmitted as one or more instructions or code on computer-readable media. Computer-readable media includes both computer storage media and communication media including any medium that facilitates transfer of a computer program from one place to another.

Any reference to an element herein using a designation such as "first," "second," and so forth does not limit the quantity or order of those elements, unless such limitation is explicitly stated. Rather, these designations may be used herein as a convenient method of distinguishing between two or more elements or instances of an element. Thus, a reference to first and second elements does not mean that only two elements may be employed there or that the first element must precede the second element in some manner. In addition, unless stated otherwise, a set of elements may comprise one or more elements.

Elements described herein may include multiple instances of the same element. These elements may be generically indicated by a numerical designator (e.g., 110) and specifically indicated by the numerical indicator followed by an alphabetic designator (e.g., 110A) or a numeric indicator preceded by a "dash" (e.g., 110-1). For ease of following the description, for the most part element number indicators begin with the number of the drawing on which the elements are introduced or most fully discussed. Thus, for example, element identifiers on a FIG. 1 will be mostly in the numerical format 1xx and elements on a FIG. 4 will be mostly in the numerical format 4xx.

As used herein, the term "substantially" in reference to a given parameter, property, or condition means and includes to a degree that one of ordinary skill in the art would understand that the given parameter, property, or condition is met with a small degree of variance, such as, for example, within acceptable manufacturing tolerances. By way of example, depending on the particular parameter, property, or condition that is substantially met, the parameter, property, or condition may be at least 90% met, at least 95% met, or even at least 99% met.

As used herein, a reference to a "cryptographic process" means the operations, including calculations that form part or all of the protocols relevant to performing encryption and decryption, resolving keys, sub-keys, or performing any other step or calculation that is relevant to cryptology. A cryptographic process may be performed by a device, for example, a cryptographic processor or a general-purpose processor executing some part of a protocol based on firmware or software.

Upon understanding that the calculations are being performed at a device, including modular inverse calculations, it may be revealed through observation of characteristics of a device performing such calculations, by way of non-limiting example, the timing/power consumption of the device. More specifically, it is possible to determine the inputs to the device from the timing/power signature of the device during a calculation if the relationship between the inputs and the timing/power signatures are known. For example, if a device uses a private key to decrypt data, observing the timing/power signatures of the device during decryption may reveal information about the private key or other cryptographic parameters provided to the device and used for those calculations.

The various embodiments described herein relate to techniques for obfuscating externally observable characteristics of a device including, without limitation, techniques that may be applied to any calculation that involves determining a greatest common divisor. Such techniques may, without limitation, obfuscate the timing information and power consumption information of the device performing such calculations. As a particular example, the technique described herein is applied to the Extended Euclidean Greatest Common Divisor Algorithm (XGCD).

As used herein "obfuscating device characteristics," or similar terms, means rendering obscure or unclear any externally observable characteristic of the device including, without limitation, characteristics of the device during operation. Such characteristics may include without limitation: power consumption, timing information, magnetic field information; heat signature information, other information similar in character, and combinations thereof. Obfuscation does not mean that the information is not observable, though that could be the result, and is meant to include making such information less useful or to require more processing to render such information useful.

Modular inverse calculations are used in cryptography, including to calculate private keys, sub-keys, and public keys. The calculation exploits the relationship that:

$$A*A^{-1}=k*m+1$$

Wherein "m" is a modulus, and "k" is an integer.

And thus, $A*A^{-1}\equiv 1$. One or more private keys and sub-keys may be calculated from a handful of base keys using the modular inverse relationships.

XGCD is a technique for determining the inverse of "a mod m" using the Euclidian algorithm (which solves for the greatest common divisor) followed by back substitution to

solve Bezout's Identity. XGCD is used in cryptography and public/private key encryption/decryption methods.

Various embodiments relate to a more secure technique for calculating the modular inverse, in one embodiment, by using a secure binary XGCD algorithm (SB-XGCD). The various embodiments build on the understanding that many of the techniques for deriving private keys from power and timing signatures rely on observations over multiple iterations, e.g., a device performing the calculations multiple times under observation. Accordingly, various embodiments utilize a random element as an obfuscating parameter in each calculation such that the relationship between successive iterations is obfuscated. This renders it orders of magnitude more difficult to determine the input values from the power and timing signature of the device performing the calculations.

An embodiment of a technique for using SB-XGCD is described below (also referred to herein as the "SB-XGCD technique"). The SB-XGCD technique begins with understanding the relationship GCD(x,y) = GCD(x,y+r*x) = 1. The expression recognizes that "y+r*x" should not affect the GCD calculation for x and y if x < y. Thus, at least one of the cryptographic parameters ("x" in the case) may be modified proportionally to the generated random number. This can be substituted into Bezout's Identity to define the relationship described in Eq. 1 that should be satisfied:

$$a*x+b*(y+r*x) = GCD(x,y) = 1 \qquad \text{(Eq. 1)}$$

"r" is a random number.

"a" and "b" are integers.

"x" and "y" are positive integers where x<y, GCD(x,y) = GCD(x,y%x) = 1.

In some embodiments, the random number r may be a 32-bit word with 12-bit leading zeroes. The 12-bit zeroes may be saved in memory to avoid XGCD overflow. Hence, the actual random effect in such an embodiment may be 20 bits (32 bits minus 12 bits). Of course, other word sizes are also contemplated. In addition, the number of bits reserved as leading zeroes are also contemplated to be adjusted depending on the maximum borrows/carries expected to avoid an overflow condition.

A binary XGCD may be performed to determine a and b that satisfy Eq. 1. Some constraints exist when performing this calculation on a computer, one of which is that overflows may occur that result in a and b being negative. A check may be performed to determine if an overflow occurred. Eq. 1 is rearranged into Eq. 2, below:

$$(a+b*r)*x+b*y = 1 \qquad \text{(Eq. 2)}$$

A check may be performed to determine if $b \geq 0$. If $b < 0$ then Eq. 2 with the values for a and b is re-arranged into Eq. 3, below:

$$(a+(b+m*y)*r)*x+(b+n*x)*y = 1 \quad \text{(Eq. 3)}$$

Where "m" and "n" are minimum positive integers so that both b+m*y and b+n*x are positive. Determining m and n is an iterative process performed until n and m results in a positive integer when added to b.

A further check is performed to determine if $(a+(b+m*y)*r) \geq 0$. If $(a+(b+m*y)*r) < 0$ then the left expression in Eq. 3 is re-arranged into Eq. 4, below:

$$(a+(b+m*y)*r+w*y)*x + (b+n*x)*y = 1 \quad \text{(Eq. 4)}$$

Where "w" is a minimum positive integer such that $a+(b+m*y)*r+w*y > 0$. Determining w is also an iterative process performed until w results in a positive integer when added to a.

Once the constraints have been satisfied, Eq. 4 may be re-arranged into the modular inverse equations 5 and 6:

$$x^{-1} \%y = a+(b+m*y)*r+w*y \quad \text{(Eq. 5)}$$

$$y^{-1} \%x = b+n*x \quad \text{(Eq. 6)}$$

The technique described is applicable to any calculation that relies on GCD calculation such as the Euclidean Algorithm.

Applying this technique to a cryptographic environment, for CRT RSA (Rivest, Shamir, Adleman algorithm implementing Chinese remainder theorem), P and Q are private keys, and d_p, d_q, P^{-1} and Q^{-1} are sub-keys. The modular inverse equations to determine those keys might be as follows:

$$d_P = e^{-1} \% (p-1)$$

$$d_q = e^{-1} \% (p-1)$$

$$p_{inv} = p^{-1}\%q$$

$$q_{inv} = q^{-1}\%p$$

For CRT RSA, due, by way of non-limiting example, to memory limitations in a chip, the sub-keys d_P and d_q as well as p_{inv} and q_{inv} may not be pre-calculated and saved in memory. Only keys p and q are stored, and every time the sub-keys are needed they are calculated in real time using the sub-key computation based on p and q. Hence, the timing and power signatures of the device performing that calculation are susceptible to observation and the keys p and q, if they are passed as parameters, are susceptible to being inferred.

FIG. 1 illustrates a secure system 100 that utilizes an embodiment of the SB-XGCD technique described above. In one embodiment, the secure system 100 may be a secure crypto-processor such as a Trusted Platform Module (TPM). The secure system 100 includes a processor 110 operably coupled with a math engine 120, a random number generator 130, a peripheral interface, and memory 150 (e.g., Flash memory). In one embodiment the processor 110 is a RISC (reduced instruction set computer) processor, such as an ARM® processor.

The random number generator 130 may be configured to generate a random number (e.g., a true random number, a pseudo-random number, etc.). The term "random number," as used herein, may be a true random number or a pseudo-random number. By way of non-limiting example, the random number generator 130 may be a non-recursive random number generator on chip, a linear-feedback shift register, or random number generation software. If called, the random number generator 130 provides a random number to the processor 110.

The math engine 120 may be a firmware extension module to the processor 110 or a separate special-purpose microcontroller. The math engine 120 is configured to perform embodiments of the SB-XGCD technique described herein. The math engine 120 accepts as parameters p, q and r as inputs to function calls for the SB-XGCD technique. The math engine 120 returns the results of the performed calculations to the processor 110, which may include the sub-keys or other private keys. In one embodiment, the results may be provided in a shared memory space accessible by both the processor 110 and the math engine 120.

The peripheral interface 140 may enable the secure system 100 to be in communication with any number of devices that utilize cryptographic keys, including the CRT RSA sign/verify 113 illustrated in FIG. 2.

FIG. 2 illustrates a processor 110 according to an embodiment of the disclosure. The processor 110 is configured be used with a variety of cryptographic schemes, including one or more of digital signature schemes such as ECD (elliptic curve digital signature) verify/sign 111, CRT RSA verify/sign 112, encryption/decryption schemes AES CFB (advanced encryption standard cipher feedback) cypher/inverse cypher 113, and CRT RSA encryption/decryption 114. Each such scheme is identified as a module in the processor 110. In various embodiments, the processor 110, in combination with the math engine 120, may determine sub-keys, signatures, encryption/decryption results, and the

like. Padding the data 115 may include adding leading zeroes to the parameter words (e.g., the random number).

The processor 110 may include a shared memory 116 for providing operations and functional data that is accessible by the math engine 120. In one embodiment, the processor 110 provides the math engine 120 with an address in shared memory 116 of the data and operation. The processor 110 may include another shared memory 117 that is accessible by the math engine 120 for providing results of operations to the processor 110. In one embodiment, the math engine 120 provides the processor 110 an address of the result of the requested operation in the shared memory 117.

Embodiments of the secure system 100 may be implemented in secure cryptographic systems that utilize the Euclidian algorithm to generate keys, for example, a key fob token (such as RSA SecurID), automated teller machines, financial transactions that include keys, a hardware lock, software licenses, and the like. In one embodiment, the secure system 100 may be implemented to authenticate devices such as printer cartridges or peripherals for mobile devices, as genuine and not OEMs (original equipment manufacturers).

FIG. 3 illustrates a flowchart of an operation of the secure system 100 of FIG. 1, in accordance with an embodiment of the disclosure. Embodiments may include generating keys used for encryption and/or decryption operations. Some embodiments may also include verifying a signature received by another device that may be helpful in verifying whether or not an obfuscating parameter was utilized by the math engine during key generation. Such a process may begin when the processor 110 receives a request at operation 302. In some embodiments, the request may be an encryption request, a decryption request, and/or a verification request. The processor 110 determines the operations responsive to the request at operation 304, which may include generating a stored private key to determine if a received public key is authentic. As part of the operations to be performed, the processor 110 provides functional data and a requested operation to the math engine 120 at operation 306. The functional data received by the math engine 120 at operation 308 includes a randomly generated number, either individually or as incorporated into the product of the random number and a key. The math engine 120, responsive to the functional data, generates the private key(s) necessary at operation 310, and provides the generated key(s) to the processor 110 at operation 312. The private keys are generated using SB-XGCD as discussed above and for verifying the

signature. Because the operation data includes randomly generated data (e.g., a random number generated by random number generator), each time a private key is generated using SB-XGCD a different random number is used as one of the inputs. In some embodiments, the randomly generated data may be generated by the math engine 120 instead of the processor 110.

The processor 110 receives the generated keys at operation 314. For operations that include signature verification, the processor 110 may analyze and interpret the externally detected signature to determine if it is correct/verified responsive to the generated keys at operation 316. The detected signature may be compared to a stored signature that may have been detected from a prior operation. The processor 110 returns a true or false responsive to its interpretation of the signature at operation 318. The fact that detected signatures are substantially different may be an indication that a random variable has been inserted into the encryption or decryption operations within the math engine 120 as an obfuscating parameter.

One of ordinary skill in the art will understand that the process described in connection with FIG. 3 is merely one implementation of the techniques described herein and could be used for other processes where observing external characteristics of a device may reveal information about device performance including, without limitation, other cryptographic processes.

FIGS. 4A and 4B are power waveforms 400, 450 illustrating that the power waveforms change between successive operations responsive to the randomly generated parameters provided to the math engine 120. For example, the power waveform 400 may be generated by a first operation having a first random variable added to the operation, and the second power waveform 450 may be generated by a second operation having a second random variable added to the operation. As a result, the calculations involved in generating the different power waveforms 400, 450 may be different despite the resulting keys being the same. After obfuscating the inputs, the detected power waveforms 400, 450 may be substantially different – thus, the timing/power information does not directly relate to the cryptographic parameters.

Many of the functional units described in this specification may be illustrated, described or labeled as modules, threads, or other segregations of programming code, in order to more particularly emphasize their implementation independence. Modules may be at least partially implemented in hardware, in one form or another. For example, a module

may be implemented as a hardware circuit comprising custom VLSI circuits or gate arrays, off-the-shelf semiconductors such as logic chips, transistors, or other discrete components. A module may also be implemented in programmable hardware devices such as field programmable gate arrays, programmable array logic, programmable logic devices, or the like. Modules may also be implemented using software or firmware, stored on a physical storage device (e.g., a computer-readable storage medium), in memory, or a combination thereof for execution by various types of processors.

An identified module of executable code may, for instance, comprise one or more physical or logical blocks of computer instructions, which may, for instance, be organized as a thread, object, procedure, or function. Nevertheless, the executable of an identified module need not be physically located together, but may comprise disparate instructions stored in different locations which, when joined logically together, comprise the module and achieve the stated purpose for the module.

Indeed, a module of executable code may be a single instruction, or many instructions, and may even be distributed over several different code segments, among different programs, and across several storage or memory devices. Similarly, operational data may be identified and illustrated herein within modules, and may be embodied in any suitable form and organized within any suitable type of data structure. The operational data may be collected as a single data set, or may be distributed over different locations including over different storage devices, and may exist, at least partially, merely as electronic signals on a system or network. Where a module or portions of a module are implemented in software, the software portions are stored on one or more physical devices, which are referred to herein as computer-readable media.

In some embodiments, the software portions are stored in a non-transitory state such that the software portions, or representations thereof, persist in the same physical location for a period of time. Additionally, in some embodiments, the software portions are stored on one or more non-transitory storage devices, which include hardware elements capable of storing non-transitory states and/or signals representative of the software portions, even though other portions of the non-transitory storage devices may be capable of altering and/or transmitting the signals. Examples of non-transitory storage devices are Flash memory and random-access-memory (RAM). Another example of a non-transitory storage device includes a read-only memory (ROM), which can store signals and/or states representative of the software portions for a period of time. However, the ability to store

the signals and/or states is not diminished by further functionality of transmitting signals that are the same as or representative of the stored signals and/or states. For example, a processor may access the ROM to obtain signals that are representative of the stored signals and/or states in order to execute the corresponding software instructions.

Additional non-limiting embodiments include:

Embodiment 1. A method of communicating between a first device and a second device, the method comprising: generating an obfuscating parameter; providing the obfuscating parameter from the first device to the second device with one or more cryptographic parameters; and receiving a first result responsive to a cryptographic process utilizing the one or more cryptographic parameters and the obfuscating parameter as inputs.

Embodiment 2. The method of Embodiment 1, wherein generating the obfuscating parameter comprises generating a random number.

Embodiment 3. The method of Embodiment 2, further comprising modifying at least one of the cryptographic parameters proportionally to the generated random number.

Embodiment 4. The method of Embodiment 3, further comprising multiplying the at least one cryptographic parameter by the random number.

Embodiment 5. The method of any of Embodiments 1 through 4, further comprising: generating a second obfuscating parameter; providing the second obfuscating parameter from the first device to the second device with the one or more cryptographic parameters; and receiving a second result responsive to a cryptographic process utilizing the one or more cryptographic parameters and the obfuscating parameter as inputs, wherein the first second result is substantially the same as the first result.

Embodiment 6. The method of Embodiment 5, wherein generating the second obfuscating parameter comprises generating a second random number.

Embodiment 7. The method of Embodiment 5, further comprising: detecting a first signature associated with the first cryptographic process; detecting a second signature associated with the second cryptographic process; and determining the first signature and the second signature are substantially different despite the first result and the second result from the cryptographic process being substantially the same.

Embodiment 8. The method of any of Embodiments 1 through 7, wherein the cryptographic process includes encryption.

Embodiment 9. The method of any of Embodiments 1 through 8, wherein the cryptographic process includes decryption.

Embodiment 10. The method of any of Embodiments 1 through 9, wherein the cryptographic process includes resolving keys.

Embodiment 11. The method of any of Embodiments 1 through 11, wherein the cryptographic process includes resolving sub-keys.

Embodiment 12. A system for performing a cryptographic process, the system comprising: a first processor configured to perform a first cryptographic process; and a second processor coupled to the first processor and configured to initiate the first cryptographic process by providing to the first processor one or more cryptographic parameters having at least some randomly generated elements, the randomly generated elements affecting one or more externally observable characteristics of the first processor while executing the first cryptographic process.

Embodiment 13. The system of Embodiment 12, wherein the one or more externally observable characteristics at least one of power consumption, timing information, magnetic field information, heat signature information, or a combination thereof.

Embodiment 14. The system of Embodiment 12 or Embodiment 13, wherein the cryptographic process includes calculating a greatest common divisor of two of the one or more cryptographic parameters.

Embodiment 15. The system of Embodiment 14, wherein the cryptographic process is a modular inverse calculation.

Embodiment 16. The system of Embodiment 15, wherein the modular inverse calculation includes an Extended Euclidean Greatest Common Divisor (XGCD) technique.

Embodiment 17. The system of Embodiment 15, wherein the XGCD technique includes a secure binary XGCD technique.

Embodiment 18. The system of any of Embodiments 12 through 17, further comprising a random number generator.

Embodiment 19. A cryptography device, comprising: a first processor configured to perform a cryptographic process responsive to a first set of cryptographic parameters; and a second processor configured to initiate the cryptographic process at the first processor by providing a second set of cryptographic parameters that are not directly relatable to the first set of cryptographic parameters.

Embodiment 20. The cryptography device of Embodiment 19, further comprising a random number generator.

Embodiment 21. The cryptography device of Embodiment 20, wherein the second processor is configured to combine the first set of cryptographic parameters with a random number from the random number generator as an obfuscating parameter in each calculation to generate the second set of cryptographic parameters.

While the present disclosure has been described herein with respect to certain illustrated embodiments, those of ordinary skill in the art will recognize and appreciate that the present invention is not so limited. Rather, many additions, deletions, and modifications to the illustrated and described embodiments may be made without departing from the scope of the invention as hereinafter claimed along with their legal equivalents. In addition, features from one embodiment may be combined with features of another embodiment while still being encompassed within the scope of the invention as contemplated by the inventor.

CLAIMS

What is claimed is:

1. A method of communicating between a first device and a second device, the method comprising:

generating an obfuscating parameter;

providing the obfuscating parameter from the first device to the second device with one or more cryptographic parameters; and

receiving a first result responsive to a cryptographic process utilizing the one or more cryptographic parameters and the obfuscating parameter as inputs.

2. The method of claim 1, wherein generating the obfuscating parameter comprises generating a random number.

3. The method of claim 2, further comprising modifying at least one of the cryptographic parameters proportionally to the generated random number.

4. The method of claim 3, further comprising multiplying the at least one cryptographic parameter by the random number.

5. The method of claim 1, further comprising:

generating a second obfuscating parameter;

providing the second obfuscating parameter from the first device to the second device with the one or more cryptographic parameters; and

receiving a second result responsive to a cryptographic process utilizing the one or more cryptographic parameters and the obfuscating parameter as inputs, wherein the first second result is substantially the same as the first result.

6. The method of claim 5, wherein generating the second obfuscating parameter comprises generating a second random number.

7. The method of claim 5, further comprising:
detecting a first signature associated with the first cryptographic process;
detecting a second signature associated with the second cryptographic process; and
determining the first signature and the second signature are substantially different despite the first result and the second result from the cryptographic process being substantially the same.

8. The method of claim 1, wherein the cryptographic process includes encryption.

9. The method of claim 1, wherein the cryptographic process includes decryption.

10. The method of claim 1, wherein the cryptographic process includes resolving keys.

11. The method of claim 1, wherein the cryptographic process includes resolving sub-keys.

12. A system for performing a cryptographic process, the system comprising:
a first processor configured to perform a first cryptographic process; and
a second processor coupled to the first processor and configured to initiate the first cryptographic process by providing to the first processor one or more cryptographic parameters having at least some randomly generated elements, the randomly generated elements affecting one or more externally observable characteristics of the first processor while executing the first cryptographic process.

13. The system of claim 12, wherein the one or more externally observable characteristics at least one of power consumption, timing information, magnetic field information, heat signature information, or a combination thereof.

14. The system of claim 12, wherein the cryptographic process includes calculating a greatest common divisor of two of the one or more cryptographic parameters.

15. The system of claim 14, wherein the cryptographic process is a modular inverse calculation.

16. The system of claim 15, wherein the modular inverse calculation includes an Extended Euclidean Greatest Common Divisor (XGCD) technique.

17. The system of claim 15, wherein the XGCD technique includes a secure binary XGCD technique.

18. The system of claim 12, further comprising a random number generator.

19. A cryptography device, comprising:

a first processor configured to perform a cryptographic process responsive to a first set of cryptographic parameters; and

a second processor configured to initiate the cryptographic process at the first processor by providing a second set of cryptographic parameters that are not directly relatable to the first set of cryptographic parameters.

20. The cryptography device of claim 19, further comprising a random number generator.

21. The cryptography device of claim 20, wherein the second processor is configured to combine the first set of cryptographic parameters with a random number from the random number generator as an obfuscating parameter in each calculation to generate the second set of cryptographic parameters.

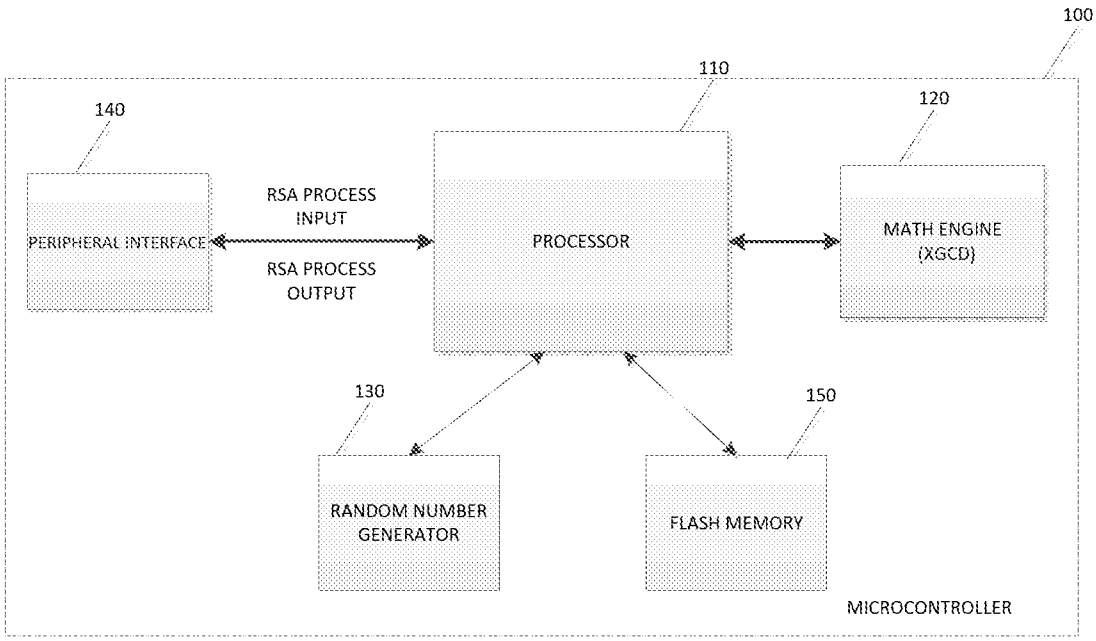
100
110
120
140
RSA PROCESS INPUT
RSA PROCESS OUTPUT
PERIPHERAL INTERFACE
PROCESSOR
MATH ENGINE (XGCD)
130
150
RANDOM NUMBER GENERATOR
FLASH MEMORY
MICROCONTROLLER

FIG. 1

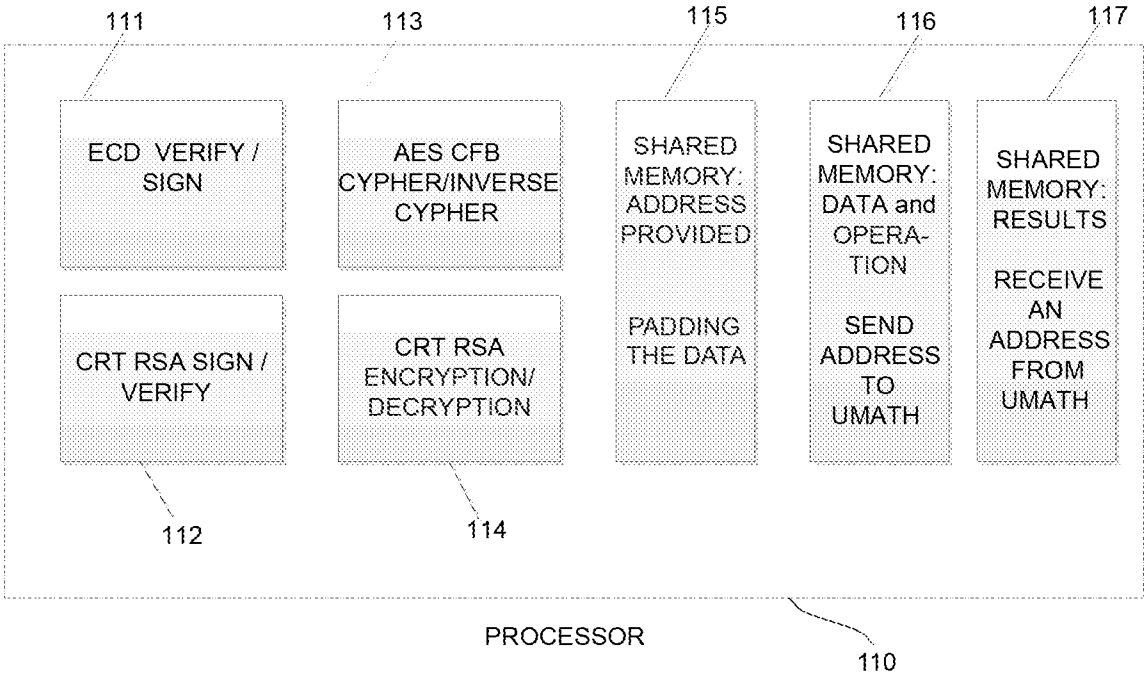
111
113
115
116
117
ECD VERIFY / SIGN
AES CFB CYPHER/INVERSE CYPHER
SHARED MEMORY: ADDRESS PROVIDED
PADDING THE DATA
SHARED MEMORY: DATA and OPERA-TION
SEND ADDRESS TO UMATH
SHARED MEMORY: RESULTS
RECEIVE AN ADDRESS FROM UMATH
CRT RSA SIGN / VERIFY
CRT RSA ENCRYPTION/ DECRYPTION
112
114
PROCESSOR
110

FIG. 2

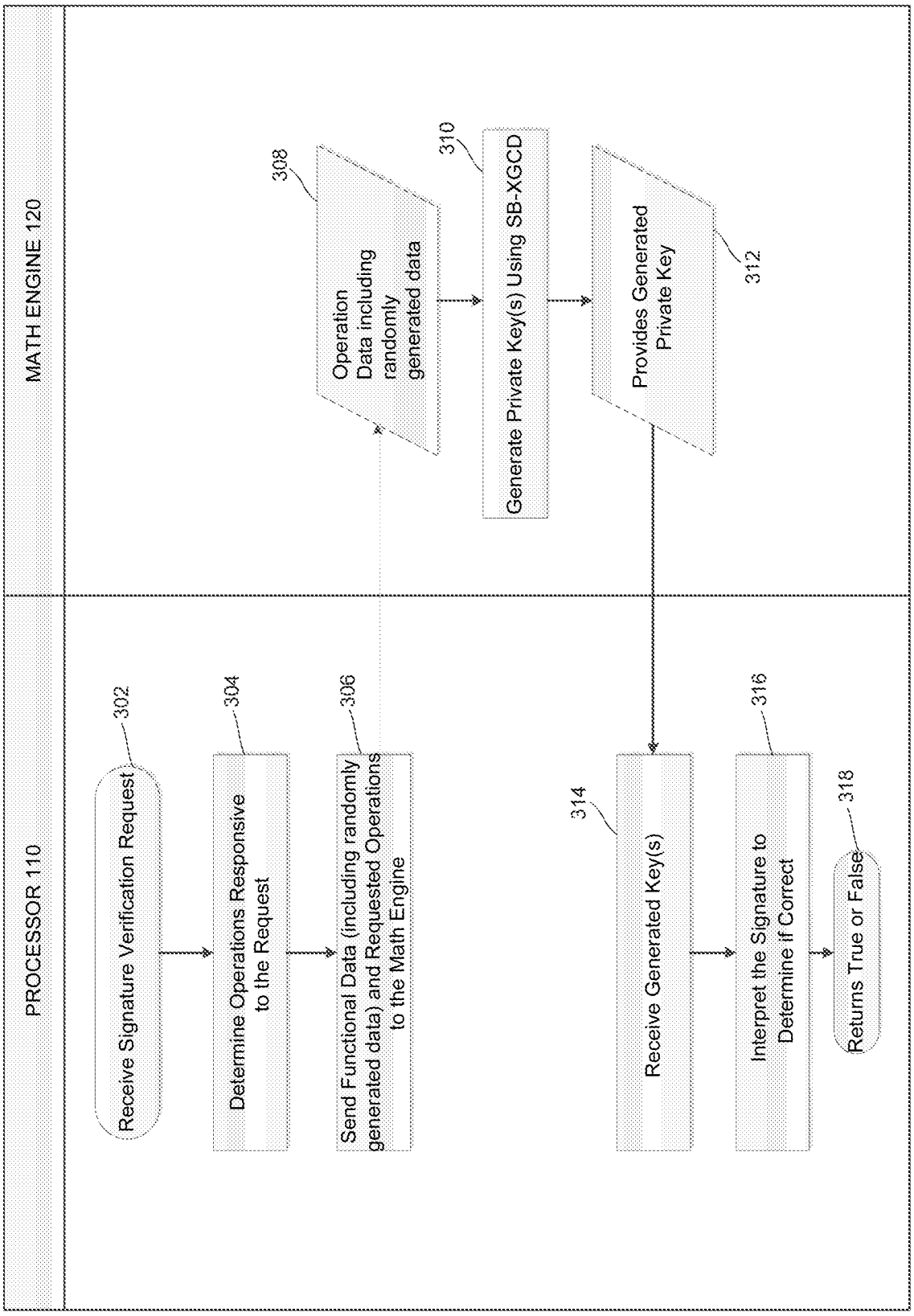
PROCESSOR 110
MATH ENGINE 120
Receive Signature Verification Request
302
Determine Operations Responsive to the Request
304
Send Functional Data (including randomly generated data) and Requested Operations to the Math Engine
306
Operation Data including randomly generated data
308
Generate Private Key(s) Using SB-XGCD
310
Provides Generated Private Key
312
Receive Generated Key(s)
314
Interpret the Signature to Determine if Correct
316
Returns True or False
318

FIG. 3

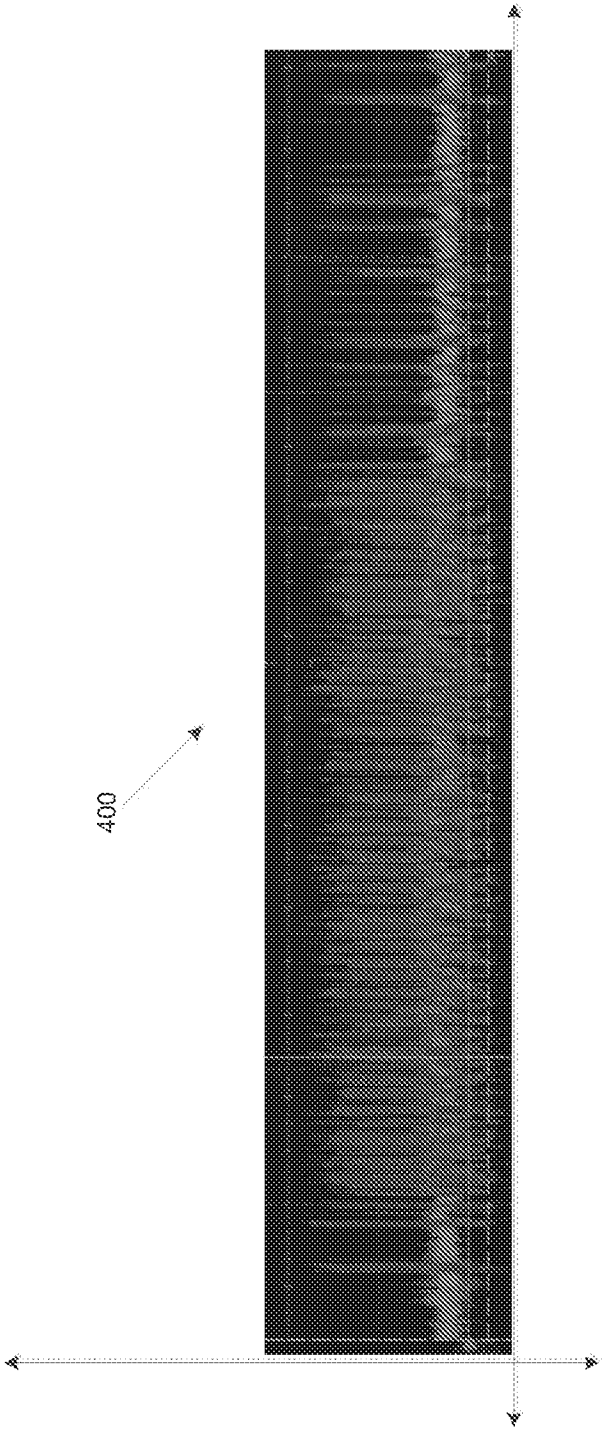

FIG. 4A

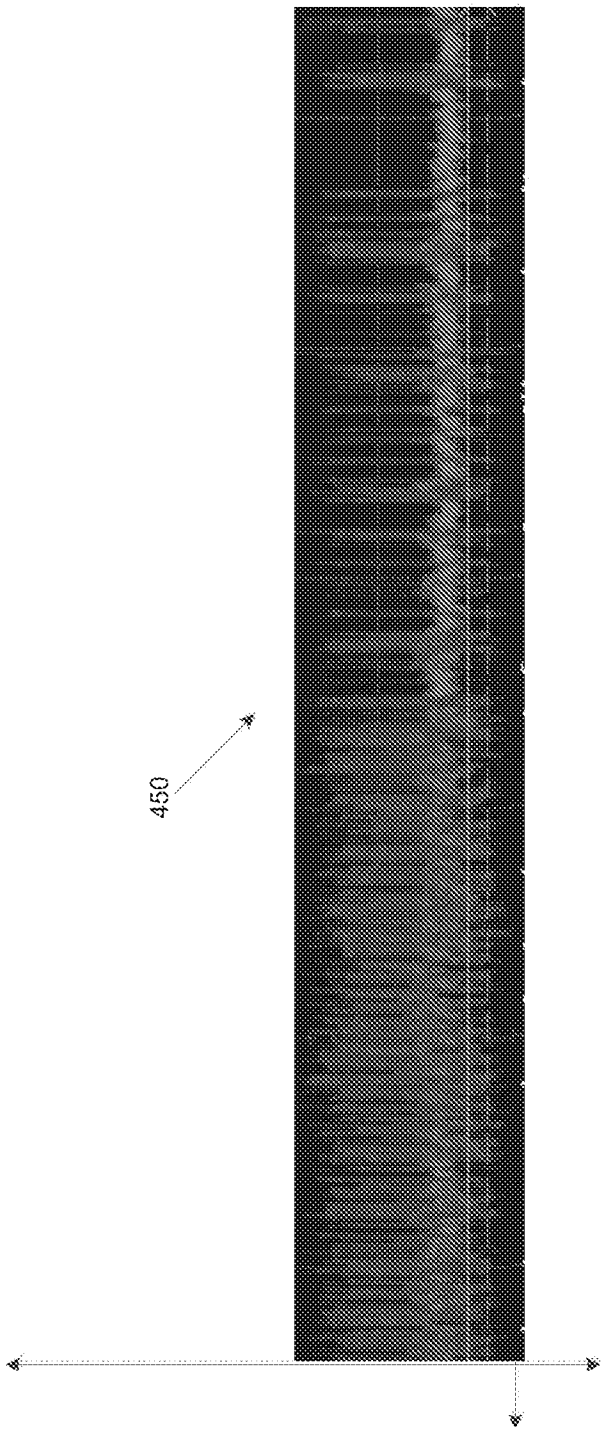

FIG. 4B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2018/033138

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-11

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2018/033138

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/00
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)
H04L

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/002531 A1 (MICHAELSEN DAVID L [US]) 6 January 2005 (2005-01-06) abstract paragraphs [0010] - [0019] paragraphs [0113] - [0132] -----	1-11
X	US 2017/091485 A1 (YUEN TSZ HON [SG] ET AL) 30 March 2017 (2017-03-30) abstract paragraphs [0008] - [0031] -----	1-11
X	WO 2016/092097 A1 (KONINKL PHILIPS NV [NL]) 16 June 2016 (2016-06-16) abstract page 2, line 1 - page 3, line 4 -----	1-11

☐ 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	Date of mailing of the international search report
28 June 2018	29/08/2018

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Di Felice, M

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2018/033138

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005002531 A1	06-01-2005	NONE	
US 2017091485 A1	30-03-2017	CN 107078899 A	18-08-2017
		EP 3134994 A1	01-03-2017
		SG 10201502401X A	28-10-2016
		US 2017091485 A1	30-03-2017
		WO 2016153430 A1	29-09-2016
WO 2016092097 A1	16-06-2016	BR 112017012092 A2	16-01-2018
		CN 107004072 A	01-08-2017
		EP 3231125 A1	18-10-2017
		JP 6368051 B2	01-08-2018
		JP 2018503862 A	08-02-2018
		US 2017324546 A1	09-11-2017
		WO 2016092097 A1	16-06-2016

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-11

   Method of generating an obfuscating parameter, providing it to another device along with one or more cryptographic parameters, and receiving the result of a cryptographic process utilizing said parameters; thereby solving the technical problem of securing communications between two devices.

   ---

2. claims: 12-18

   System comprising multiple processors, wherein one processor initiates a cryptographic process on another processor by providing one or more cryptographic parameters including random elements to the other processor, wherein the random elements affect one or more externally observable characteristics of said other processor; thereby solving the technical problem of securely having a co-processor perform a cryptographic operation.

   ---

3. claims: 19-21

   Cryptographic device comprising a first processor executing a cryptographic operation on a first set of cryptographic parameters, and a second processor initiating the cryptographic process by providing it with a second set of cryptographic parameters that are not directly relatable to the first set; thereby solving the technical problem of securely performing distinct cryptographic operations on multiple independent processors.
