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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 June 2014 (26.06.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/098998 A1

(51) International Patent Classification:
G06F 21/60 (2013.01)

(21) International Application Number:
PCT/US2013/047279

(22) International Filing Date:
24 June 2013 (24.06.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/719,939 19 December 2012 (19.12.2012) US

(71) Applicant *(for all designated States except US)*: **INTEL CORPORATION** [US/US]; 2200 Mission College Blvd., Santa Clara, California 95054 (US).

(72) Inventors; and

(71) Applicants *(for US only)*: **JOHNSON, Simon** [GB/US]; 14964 SW Opal Drive, Beaverton, Oregon 97007 (US). **DAS, Abhishek** [IN/US]; 950 SW 21st, Apt. 811, Portland, Oregon 97205 (US). **ROZAS, Carlos** [US/US]; 1534 NW Morgan Lane, Portland, Oregon 97229 (US). **SAVAGAONKAR, Uday** [IN/US]; 5507 NW 133rd Ave, Portland, Oregon 97229 (US). **BLANKENSHIP, Robert** [US/US]; 3115 N. 20th Street, Tacoma, Washington 98406 (US). **PADWEKAR, Kiran** [US/US]; 19566 Brockton Lane, Saratoga, California 95070 (US).

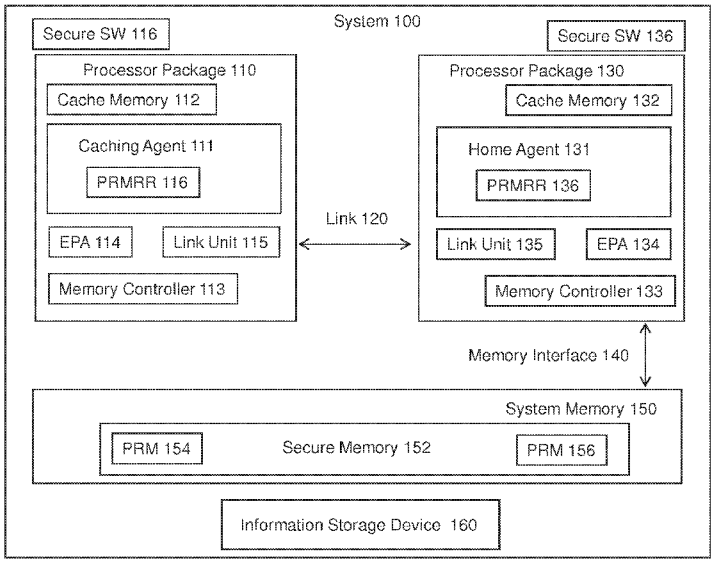
(74) Agent: **LANE, Thomas R.**; c/o CPA Global, P.O. Box 52050, Minneapolis, Minnesota 55402 (US).

(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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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.

[Continued on next page]

(54) Title: SECURING DATA TRANSMISSIONS BETWEEN PROCESSOR PACKAGES

FIGURE 1



(57) Abstract: Embodiments of an invention for securing transmissions between processor packages are disclosed. In one embodiment, an apparatus includes an encryption unit to encrypt first content to be transmitted from the apparatus to a processor package directly through a point-to-point link.

WO 2014/098998 A1

(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, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

SECURING DATA TRANSMISSIONS BETWEEN PROCESSOR PACKAGES

BACKGROUND

1. Field

The present disclosure pertains to the field of information processing, and more particularly, to the field of security in information processing systems.

2. Description of Related Art

Malicious attacks are a serious threat to the security of information processing systems. Many techniques have been developed to defend against these attacks, but more are needed as information processing system development continues.

Brief Description of the Figures

The present invention is illustrated by way of example and not limitation in the accompanying figures.

Figure 1 illustrates a system in which data transmissions between processor packages may be secured according to an embodiment of the present invention.

Figure 2 illustrates a processor according to an embodiment of the present invention.

Figure 3 illustrates an encryption proxy agent according to an embodiment of the present invention.

Figure 4 illustrates a method for securing data transmissions between processor packages according to an embodiment of the present invention.

Detailed Description

Embodiments of an invention for securing data transmissions between processor packages are described. In this description, numerous specific details, such as component and system configurations, may be set forth in order to provide a more thorough understanding of the present invention. It will be appreciated, however, by one skilled in the art, that the invention may be practiced without such specific details. Additionally, some well-known structures, circuits, and other features have not been shown in detail, to avoid unnecessarily obscuring the present invention.

In the following description, references to "one embodiment," "an embodiment," "example

embodiment," "various embodiments," etc., indicate that the embodiment(s) of the invention so described may include particular features, structures, or characteristics, but more than one embodiment may and not every embodiment necessarily does include the particular features, structures, or characteristics. Further, some embodiments may have some, all, or none of the features described for other embodiments.

As used in the claims, unless otherwise specified the use of the ordinal adjectives "first," "second," "third," etc. to describe an element merely indicate that a particular instance of an element or different instances of like elements are being referred to, and is not intended to imply that the elements so described must be in a particular sequence, either temporally, spatially, in ranking, or in any other manner.

Figure 1 illustrates system 100, an information processing system in which an embodiment of the present invention may be present and/or operate. System 100 may represent any type of information processing system, such as a server, a desktop computer, a portable computer, a set-top box, a hand-held device, or an embedded control system. System 100 includes processor package 110, inter-package link 120, processor package 130, memory interface 140, system memory 150, and information storage device 160. Processor package 110 and processor package 130 are coupled to each other through inter-package link 120. Processor package 130 and system memory 150 are coupled to each other through memory interface 140. Systems embodying the present invention may include any number of each of these components and any other components or other elements, such as information storage devices, peripherals, and input/output devices. Any or all of the other components or other elements in any system embodiment, such as information storage device 160, may be connected, coupled, or otherwise in communication with each other through any number of buses, point-to-point, or other wired or wireless interfaces or connections.

Processor package 110 may include one or more processors packaged within a single package, each of which may include multiple threads and/or multiple execution cores, in any combination. Each processor may be any type of processor, including a general purpose microprocessor, such as a processor in the Intel® Core® Processor Family, Intel® Atom® Processor Family, or other processor family from Intel® Corporation, or another processor from another company, or a special purpose processor or microcontroller.

Processor package 110 includes caching agent 111, cache memory 112, memory controller 113, encryption proxy agent 114, and link unit 115. Caching agent 111 may represent any processor as set forth above, which in this embodiment serves as a caching agent for purposes of this description. Cache memory 112 may represent any one or more levels of cache memory in a memory hierarchy of system 100, implemented in static random access memory or any other

memory technology. Cache memory 112 may include any combination of cache memories dedicated to or shared among any one or more execution cores or processors within processor package 110 according to any known approaches to caching in information processing systems.

Encryption proxy agent 114 may include any logic, circuitry, or other hardware to execute one or more encryption algorithms and the corresponding decryption algorithms. Link unit 115 may include any circuitry or other hardware with which processor package 110 may communicate another processor package in system 100 through a point-to-point link.

Inter-package link 120 may represent a point-to-point interface, which may be a point-to-point link in an interconnect fabric according to any system interconnect architecture, such as that of Intel® Quick Path Interconnect or an embodiment of a High Performance Interconnect described in the co-pending U.S. Patent application entitled Method, Apparatus, System for a High Performance Interconnect architecture, filed October 22, 2012, Serial No. 61/717,091, which is incorporated herein by reference. Data, control information, or other information may be transmitted or otherwise sent from processor package 110 to processor package 130 in packets according to the protocol of any such architecture.

Processor package 130 includes home agent 131, cache memory 132, memory controller 133, encryption proxy agent 134, and link unit 135. Home agent 131 may represent any processor as set forth above, which in this embodiment serves as a home agent for purposes of this description. Cache memory 132 may represent any one or more levels of cache memory in a memory hierarchy of system 100, implemented in static random access memory or any other memory technology. Cache memory 132 may include any combination of cache memories dedicated to or shared among any one or more execution cores or processors within processor package 130 according to any known approaches to caching in information processing systems.

Encryption proxy agent 134 may include any logic, circuitry, or other hardware to execute one or more encryption algorithms and the corresponding decryption algorithms and to provide the other functionalities described below. Link unit 135 may include any circuitry or other hardware with which processor package 130 may communicate with another processor package in system 100 through a point-to-point link.

Memory interface 140 may represent any type of interface between a memory and a processor. System memory 150 may include dynamic random access memory and/or any other type of medium accessible by processor 110 and/or 130, and may be used to store data and/or instructions used or generated by processor 110, processor 130, and/or any other components. Memory interface 140 is shown between processor package 130 and system memory 150; however, system memory 150 may represent a portion of a larger system memory, where the portion is locally attached to processor package 130 through memory interface 140. Similarly, a

portion of the larger system memory may also be locally attached to processor package 110 through memory interface 140 and/or another memory interface not shown. Information storage device 160 may represent any type of non-volatile information storage device, such as flash memory or a hard disk drive.

Figure 1 also illustrates secure software modules 116 and 136, which may be secure software or firmware running, executing, loaded, or otherwise present on or in caching agent 111 and home agent 131, respectively. Secure software module 116 may program encryption proxy agent 114 with a cryptographic key, and secure software module 136 may program encryption proxy agent 134 with the same or a corresponding cryptographic key , such that encryption proxy agent 134 may decrypt data encrypted by encryption proxy agent 114, and vice versa. Any type of cryptographic key or keys may be used within the scope of the present invention. Embodiments of the present invention may include using a first cryptographic key or other data provided by a secure software module to derive a second cryptographic key for encryption and decryption.

Figure 2 illustrates processor 200, an embodiment of which may serve as caching agent 111 and an embodiment of which may serve as home agent 131 in system 100. Processor 200 may include instruction unit 210, execution unit 220, processor storage 230, processor control unit 240, and secure enclave unit 250. Processor 200 may also include any other circuitry, structures, or logic not shown in Figure 2. For example, a cache memory, a memory controller, an encryption proxy agent, and/or a link unit that may serve as an embodiment of cache memory 112 or 132, memory controller 113 or 133, encryption proxy agent 114 or 134, and link unit 115 or 135, respectively, may be integrated on the substrate of processor 200.

Instruction unit 210 may represent any circuitry, structure, or other hardware, such as an instruction decoder, for fetching, receiving, decoding, and/or scheduling instructions. Any instruction format may be used within the scope of the present invention; for example, an instruction may include an opcode and one or more operands, where the opcode may be decoded into one or more micro-instructions or micro-operations for execution by execution unit 220.

Execution unit 220 may include any circuitry, structure, or other hardware, such as an arithmetic unit, logic unit, floating point unit, shifter, etc., for processing data and executing instructions, micro-instructions, and/or micro-operations.

Processing storage 230 may represent any type of storage usable for any purpose within processor 200; for example, it may include any number of data registers, instruction registers, status registers, configuration registers, control registers, other programmable or hard-coded registers or register files, or any other storage structures.

Processor control unit 240 may include any logic, circuitry, hardware, or other structures,

including microcode, state machine logic, or programmable logic, to control the operation of the units and other elements of processor 200 and the transfer of data within, into, and out of processor 200. Processor control unit 240 may cause processor 200 to perform or participate in the performance of method embodiments of the present invention, such as the method embodiments described below, for example, by causing processor 200 to execute instructions received by instruction unit 210 and micro-instructions or micro-operations derived from instructions received by instruction unit 210.

Secure enclave unit 250 may represent any logic, circuitry, hardware, or other structures for creating and maintaining a secured, protected, or isolated environment, such as a secure enclave as described herein, in which an application or other software may run, execute, be loaded, or otherwise be present within an information processing system such as system 100. For purposes of this description, each instance of such an environment may be referred to as a secure enclave, although embodiments of the present invention are not limited to those using a secure enclave as the secured, protected, or isolated environment. In one embodiment, a secure enclave may be created and maintained using instructions in the instruction set of a processor in the Intel® Core® Processor Family or other processor family from Intel® Corporation.

All or part of secure enclave unit 250 may be included within any one or more other units of processor 200, such as those corresponding to instruction unit 210, execution unit 220, processor storage 230, and processor control unit 240. Secure enclave unit 250 may include encryption unit 252, which may include any logic, circuitry, or other hardware to execute one or more encryption algorithms and the corresponding decryption algorithms, and may include logic, circuitry, or other hardware shared with another encryption unit such as encryption proxy agent 114 and/or 134.

Each secure enclave created within system 100 may be allocated a secure or protected space within the system memory space supported by system memory 150. Secure memory 152 represents one or more such secure or protected memory spaces. Each such memory space may be created, allocated, and maintained using known virtual memory, secure enclave, or other system memory addressing techniques such that the information within each such memory space may at various times be stored within any combination of information storage device 160, system memory 150, any of cache memories 112 and/or 132, any processor storage in caching agent 110 and/or home agent 130 represented by processor storage 230, and/or any other memory or storage area within information processing system 100.

Secure memory 152 may include one or more physically contiguous ranges of memory called processor reserved memory (PRM). In one embodiment, a PRM is naturally aligned and has a size that is an integer power of two. System firmware such as a basic input/output system

may reserve a PRM, for example by setting a pair of model-specific registers (MSRs), collectively known as a PRM range register (PRMRR). In the embodiment of Figure 2, secure enclave logic 250 may include PRMRR 254, embodiments of which may serve as PRMRR 116 and PRMRR 136 in Figure 1. PRMRR 116 may be used to reserve PRM 154 for caching agent 111 and PRMRR 136 may be used to reserve PRM 156 for home agent 131.

Secure enclave unit 250 may also include access control unit 256, which may include any logic, circuitry, hardware, or other structures to enforce load and access restrictions using PRMRR 254 such that the information within the memory space of a secure enclave is accessible only to the application running in that secure enclave. For example, the information on a memory page allocated to a secure enclave may be encrypted by encryption unit 252 before being stored in system memory 150, information storage device 160, or any other memory or storage external to processor 200. While stored external to processor 200, the information is protected by encryption and integrity check techniques. When the memory page is loaded into a cache memory of a processor by an application or process running on that processor within the secure enclave to which the page is allocated, it is decrypted by encryption unit 252, then the unencrypted information is accessible only by an application or process running within the secure enclave.

Figure 3 illustrates encryption proxy agent (EPA) 300, embodiments of which may serve as an EPA 114 and EPA 134 in system 100. In one embodiment, the hardware in EPA 300 is dedicated or unshared, which means that is not shared with the hardware in any processor execution core on the same substrate or in the same package. In other embodiments, hardware may be shared between an EPA and one or more processor cores.

EPA 300 may include encryption unit 310 to execute one or more encryption algorithms and the corresponding decryption algorithms. Any one or more cryptographic algorithms may be used within the scope of the present invention. Encryption unit 310 may include transmit unit 312 to encrypt content to be transmitted or otherwise sent, in one or more packets, from one processor package to another processor package directly through a point-to-point link. Encryption unit 310 may also include receive unit 314 to decrypt content received, in one or more packets, from one processor package to another processor package directly through a point-to-point link. Encryption unit 310 may also include secure key storage 316 to store a cryptographic key to be used to encrypt and decrypt content to be transmitted or otherwise sent, in one or more packets, from one processor package to another processor package directly through a point-to-point link. Encryption unit 310 may also include key derivation unit 318 to derive a second cryptographic key from a first cryptographic key or other data received by EPA 300.

EPA 300 may also include authentication unit 320 to authenticate data or other information transmitted between processor packages directly through a point-to-point link. Any authentication technique may be used within the scope of the present invention. Authentication unit 320 may include transmit unit 322 to generate and append or otherwise provide authentication metadata, such as a header or signature, to content to be transmitted or otherwise sent, in one or more packets, from one processor package to another processor package directly through a point-to-point link. Authentication unit 320 may also include receive unit 324 to verify the authenticity of content received, in one or more packets, by one processor package from another processor package directly through a point-to-point link.

EPA 300 may also include replay protection unit 330 to protect from replay attacks data or other information transmitted between processor packages directly through a point-to-point link. Any replay protection technique may be used within the scope of the present invention. Replay protection unit 320 may include transmit unit 332 to generate and append or otherwise provide replay protection information, such as a monotonic counter value, random number, and/or an integrity check value, to content to be transmitted or otherwise sent, in one or more packets, from one processor package to another processor package directly through a point-to-point link. Replay protection unit 320 may also include receive unit 334 to verify replay protection information of content received, in one or more packets, by one processor package from another processor package directly through a point-to-point link.

EPA 300 may also include EPA control unit 340, which may include any logic, circuitry, hardware, firmware, other structures, microcode, state machine logic, and/or programmable logic to control the operation of the units and other elements of EPA 300. EPA control unit 340 may cause EPA 300 to perform or participate in the performance of method embodiments of the present invention, such as the method embodiments described below.

Figure 4 illustrates method 400 for securing data transmissions between processor packages according to an embodiment of the present invention. Although method embodiments of the invention are not limited in this respect, reference may be made to elements of Figures 1, 2, and 3 to help describe the method embodiment of Figure 4.

In box 410, secure software module 116 programs EPA 114 with a cryptographic key. In box 412, secure software module 136 programs EPA 134 with the same or a corresponding cryptographic key, such that EPA 134 may decrypt data encrypted by EPA 114, and vice versa.

In box 420 of method 400, the operation of a processor within processor package 110 generates data to be stored in a first memory address. In box 422, caching agent 111 performs a cache request to determine whether the first memory address is within cache memory 112. In box 424, the cache request misses because the first memory address is not within cache memory

112. In box 426, in response to the missed cache request, a memory request to write the data to system memory 150 is initiated.

In box 430, it is determined whether the memory request is a secure memory request or a non-secure memory request. For example, it may be determined, using PRMRR 116, whether the first memory address is within the address range of secure memory 152, in which case the memory request it is determined that the memory request is a secure memory request. If the memory request is a secure memory request, then method 400 continues in box 440. If the memory request is a non-secure memory request, then method 400 continues in box 432.

In box 432, the memory request is routed to link unit 115. In box 434, link unit 115 generates one or more packets, including the encrypted data, to be transmitted. From box 434, method 400 continues to box 452.

In box 440, the memory request is routed to EPA 114. In box 442, EPA 114 encrypts the data. In box 444, EPA 114 appends authentication metadata to the encrypted data. In box 446, EPA 114 appends an anti-replay value to the encrypted data. In box 448, the memory request is routed to link unit 115. In box 450, link unit 115 generates one or more packets, including content representing the encrypted data, the authentication metadata, and the anti-replay value, to be transmitted.

In box 452, the one or more packets are transmitted through inter-package link 120. In box 454, the one or more packets are received by link unit 135. In box 456, link unit 135 determines that the one or more packets correspond to a memory request. In box 458, it is determined whether the memory request is a secure memory request or a non-secure memory request. For example, it may be determined, using PRMRR 136, whether the a memory request is to an address within the address range of secure memory 152, in which case it is determined that the memory request is a secure memory request. If the memory request is a secure memory request, then method 400 continues in box 460. If the memory request is a non-secure memory request, then method 400 continues in box 470.

In box 460, the memory request is routed to EPA 134. In box 462, EPA 134 uses the authentication data to verify the authenticity of the memory request. In box 464, EPA 134 uses the anti-replay value to verify that memory request is not associated with a replay attack. In box 466, EPA 134 decrypts the encrypted data.

In box 470, the memory request is routed to home agent 131. In box 472, home agent 131 transmits the memory request to system memory 150.

In various embodiments of the present invention, the method illustrated in Figure 4 may be performed in a different order, with illustrated boxes combined or omitted, with additional boxes added, or with a combination of reordered, combined, omitted, or additional boxes. For

example, boxes 444 and/or 446 may be performed before box 442, such that the authentication metadata and/or the anti-replay value may also be encrypted. Furthermore, many other method embodiments are possible within the scope of the present inventions, including an embodiment securing a data transmission from a home agent to a cache agent, a data transmission between cache agents, a data transmission between any other types of agents, and a data transmission corresponding to a read or other transaction.

Embodiments or portions of embodiments of the present invention, as described above, may be stored on any form of a machine-readable medium. For example, all or part of method 200 may be embodied in software or firmware instructions that are stored on a medium readable by processor 200 and/or EPA 300, which when executed by processor 200 and/or EPA 300, cause processor 200 and/or EPA 300 to execute an embodiment of the present invention. Also, aspects of the present invention may be embodied in data stored on a machine-readable medium, where the data represents a design or other information usable to fabricate all or part of processor 200 and/or EPA 300.

Thus, embodiments of an invention for securing data transmission between processor packages have been described. While certain embodiments have been described, and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative and not restrictive of the broad invention, and that this invention not be limited to the specific constructions and arrangements shown and described, since various other modifications may occur to those ordinarily skilled in the art upon studying this disclosure. In an area of technology such as this, where growth is fast and further advancements are not easily foreseen, the disclosed embodiments may be readily modifiable in arrangement and detail as facilitated by enabling technological advancements without departing from the principles of the present disclosure or the scope of the accompanying claims.

What is claimed is:

1. An apparatus comprising:
an encryption unit to encrypt first content to be transmitted from the apparatus to a processor package directly through a point-to-point link.

2. The apparatus of claim 1, wherein the first content is to be transmitted in one or more packets.

3. The apparatus of claim 1, further comprising an authentication unit to append authentication metadata to the first content.

4. The apparatus of claim 1, further comprising a replay protection unit to append an anti-replay value to the first content.

5. The apparatus of claim 1, wherein the encryption unit is also to decrypt second content received from the processor package directly through the point-to-point link.

6. The apparatus of claim 3, wherein the authentication unit is also to verify the authenticity of the second content.

7. The apparatus of claim 4, wherein the replay protection unit is also to protect the second content from a replay attack.

8. The apparatus of claim 1, further comprising logic to determine that the first content is associated with a secure memory request.

9. The apparatus of claim 1, further comprising a range register to be used to determine that the first content is associated with a request to a secure memory.

10. A method comprising:
encrypting within a first processor package content to be transmitted from a first processor package to a second processor package directly through a point-to-point link.

11. The method of claim 10, further comprising determining that the content is associated with a secure memory request before encrypting the content.

12. The method of claim 11, further comprising transmitting the encrypted content through the point-to-point link in one or more packets.

13. The method of claim 12, further comprising appending authentication metadata to the content.

14. The method of claim 12, further comprising appending an anti-replay value to the content.

15. The method of claim 12, further comprising decrypting within the second processor package the encrypted content.

16. The method of claim 12, further comprising using, within the second processor package, the authentication metadata to verify the authenticity of the content.

17. The method of claim 13, further comprising using, within the second processor package, the anti-replay value to verify that receiving the content is not associated with a replay attack.

18. A system comprising:

a first processor package;

a second processor package;

a point-to-point link between the first processor package and the second processor package;

wherein the first processor package includes a first encryption proxy agent to encrypt content to be transmitted from the first processor package to the second processor package directly through the point-to-point link; and

wherein the second processor package includes a second encryption proxy agent to decrypt the encrypted content received from the first processor package directly through the point-to-point link.

19. The system of claim 18 wherein the first processor package also includes:

a caching agent; and

logic to determine that the content is associated with a secure memory request from the caching agent.

20. The method of claim 18 wherein the second processor package also includes:

a home agent; and

logic to determine that the decrypted content is associated with a secure memory request to the home agent.

FIGURE 1

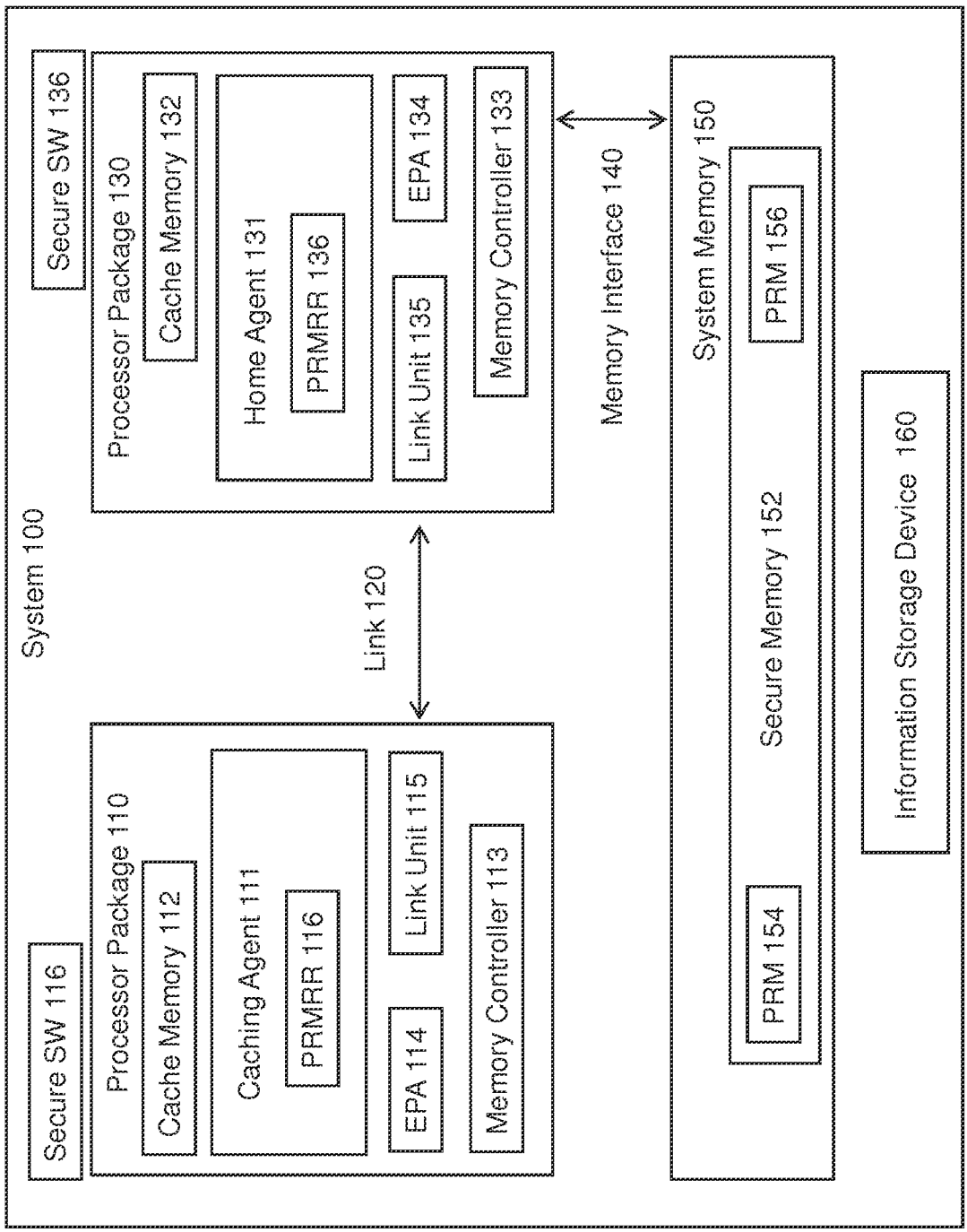

System 100
Secure SW 116
Processor Package 110
Cache Memory 112
Caching Agent 111
PRMRR 116
EPA 114
Link Unit 115
Memory Controller 113
Link 120
Secure SW 136
Processor Package 130
Cache Memory 132
Home Agent 131
PRMRR 136
Link Unit 135
EPA 134
Memory Controller 133
Memory Interface 140
System Memory 150
PRM 154
Secure Memory 152
PRM 156
Information Storage Device 160

FIGURE 2

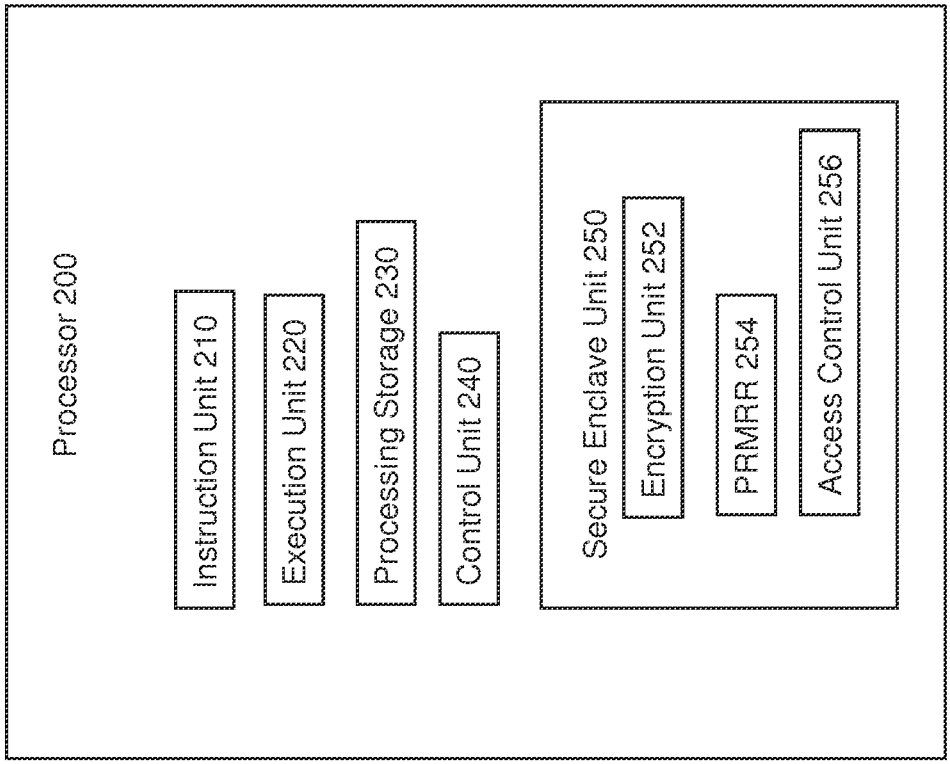

Processor 200
Instruction Unit 210
Execution Unit 220
Processing Storage 230
Control Unit 240
Secure Enclave Unit 250
Encryption Unit 252
PRMRR 254
Access Control Unit 256

FIGURE 3

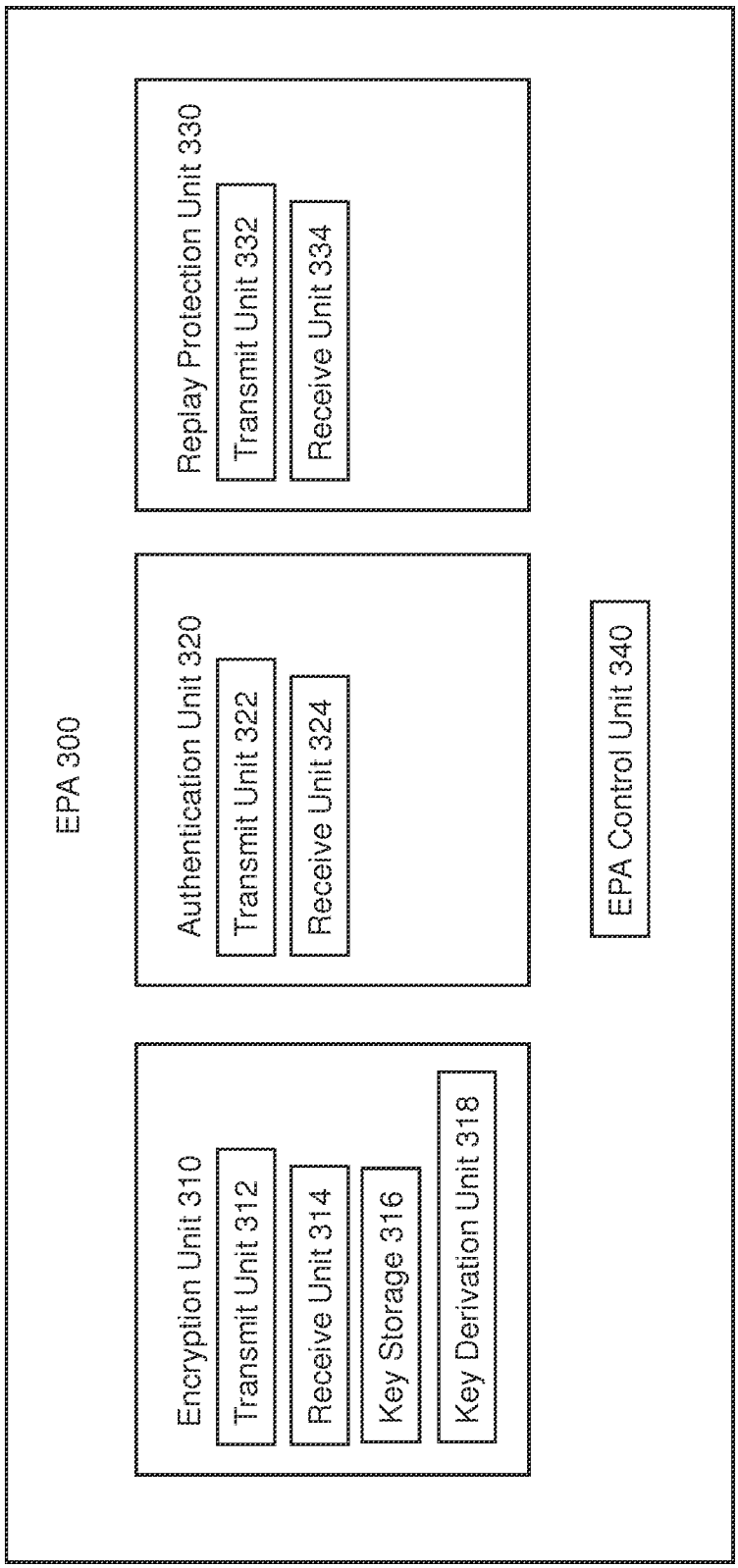
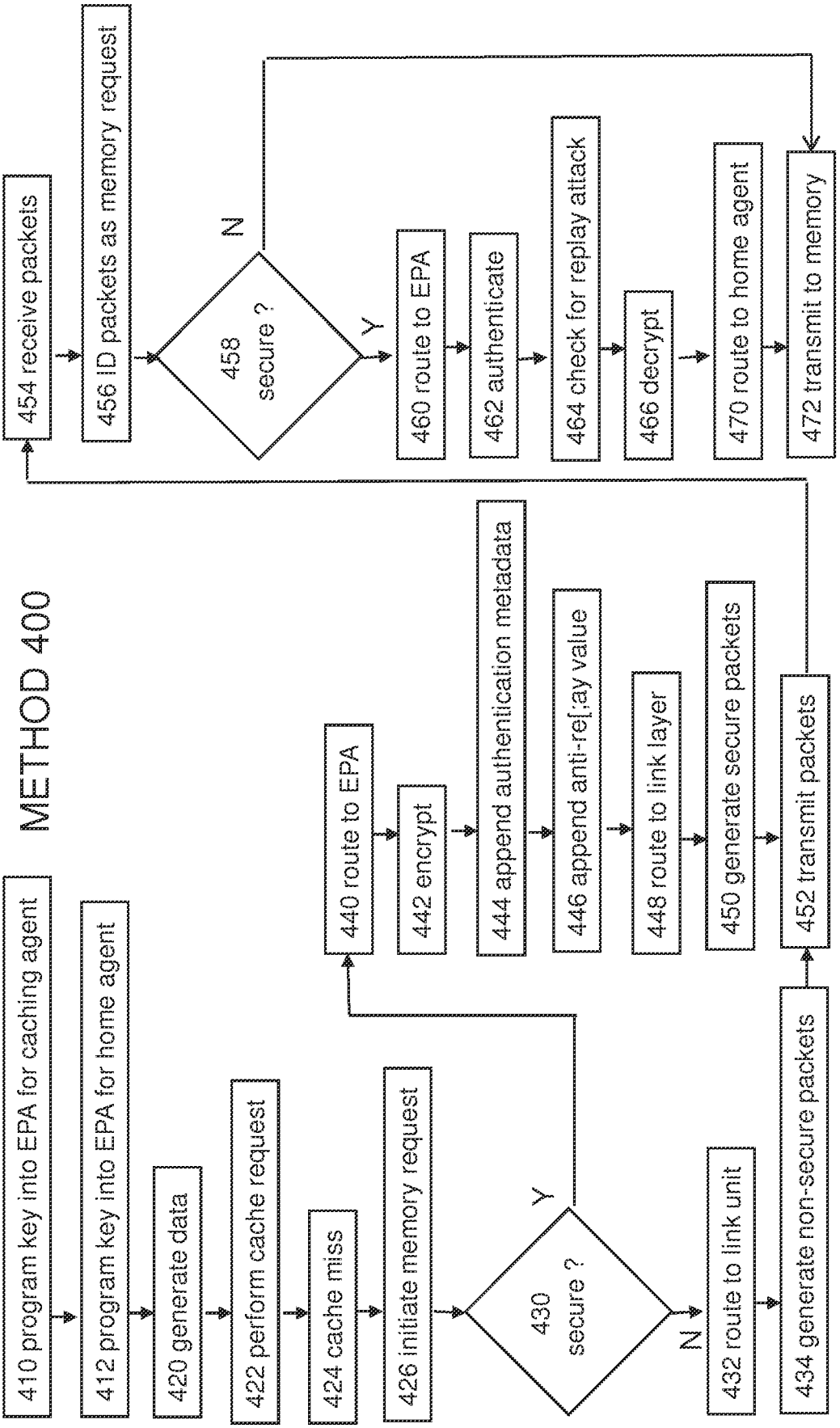

EPA 300
Encryption Unit 310
Transmit Unit 312
Receive Unit 314
Key Storage 316
Key Derivation Unit 318
Authentication Unit 320
Transmit Unit 322
Receive Unit 324
Replay Protection Unit 330
Transmit Unit 332
Receive Unit 334
EPA Control Unit 340

FIGURE 4
METHOD 400



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/047279

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60(2013.01)i

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)
G06F 21/60; G06F 9/46; H04L 9/00; G06F 21/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords:encrypt, decrypt, point-to-point, processor, packet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2004-0054914 A1 (PATRICK L. SULLIVAN) 18 March 2004 See paragraphs [0047]-[0050], [0054]-[0055]; claim 1; and figure 2.	1-2,5,10,18
A		3-4,6-9,11-17,19-20
Y	US 2007-0157211 A1 (HONG WANG et al.) 05 July 2007 See paragraphs [0055], [0068]-[0070]; and figure 7.	1-2,5,10,18
A	US 2012-0066489 A1 (HIROTSUGU OZAKI et al.) 15 March 2012 See paragraphs [0123]-[0135]; claim 1;and figures 4A-4C.	1-20
A	US 2011-0239297 A1 (YUJI UNAGAMI et al.) 29 September 2011 See paragraphs [0203]-[0251]; and figures 8-10.	1-20
A	US 2010-0174897 A1 (ALAIN SCHUMACHER) 08 July 2010 See paragraphs [0006]-[0011], [0039]-[0051]; and claims 1-2.	1-20

☐ 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 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
11 October 2013 (11.10.2013)	**15 October 2013 (15.10.2013)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. +82-42-472-7140	Authorized officer BYUN Sung Cheal Telephone No. +82-42-481-8262

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2013/047279

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004-0054914 A1	18/03/2004	AU 2003-225263 A1	17/11/2003
		AU 2003-225263 B2	17/07/2008
		CA 2483601 A1	13/11/2003
		EP 1540957 A1	15/06/2005
		EP 1540957 A4	08/07/2009
		US 7650510 B2	19/01/2010
		WO 03-094513 A1	13/11/2003
US 2007-0157211 A1	05/07/2007	CN 102081556 A	01/06/2011
		CN 1991768 A	04/07/2007
		CN 1991768 B	13/04/2011
		EP 1814026 A2	01/08/2007
		EP 1814026 A3	25/02/2009
		EP 2275926 A2	19/01/2011
		EP 2275926 A3	12/12/2012
		JP 2007-183943 A	19/07/2007
		JP 2011-146077 A	28/07/2011
		KR 10-0879825 B1	21/01/2009
		KR 10-1247407 B1	25/03/2013
		KR 10-1299286 B1	23/08/2013
		KR 10-2007-0072396 A	04/07/2007
		KR 10-2008-0096636 A	31/10/2008
		KR 10-2012-0098981 A	06/09/2012
		KR 10-2013-0023302 A	07/03/2013
		US 2013-205122 A1	08/08/2013
US 2012-0066489 A1	15/03/2012	AU 2004-302108 A1	17/02/2005
		AU 2004-302108 B2	25/02/2010
		AU 2004-302108 C1	16/09/2010
		CA 2534919 A1	17/02/2005
		CA 2534919 C	05/04/2011
		CN 1833403 A	13/09/2006
		CN 1833403 B	25/05/2011
		EP 1653660 A1	03/05/2006
		EP 1653660 A4	28/12/2011
		IL 173316 A	30/12/2010
		IL 173316 D0	11/06/2006
		JP 3783142 B2	07/06/2006
		KR 10-1055861 B1	09/08/2011
		KR 10-2006-0059908 A	02/06/2006
		NO 20056234 A	08/05/2006
		TW I362859 B	21/04/2012
		US 2006-0190720 A1	24/08/2006
		US 8041816 B2	18/10/2011
		WO 2005-015827 A1	17/02/2005
US 2011-0239297 A1	29/09/2011	CN 102272770 A	07/12/2011
		EP 2397963 A1	21/12/2011
		WO 2010-092830 A1	19/08/2010

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2013/047279

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010-0174897 A1	08/07/2010	CA 2648084 A1	11/10/2007
		CN 101411114 A	15/04/2009
		EP 1841122 A1	03/10/2007
		EP 2002594 A1	17/12/2008
		JP 2009-531728 A	03/09/2009
		WO 2007-113217 A1	11/10/2007