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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 June 2021 (24.06.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/122907 A1

(51) International Patent Classification:
G06F 21/75 (2013.01) *G11C 5/14* (2006.01)
G06F 12/14 (2006.01) *G11C 7/24* (2006.01)
G06F 21/79 (2013.01)

(21) International Application Number:
PCT/EP2020/086662

(22) International Filing Date:
17 December 2020 (17.12.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
19306678.4 18 December 2019 (18.12.2019) EP

(71) Applicants: **THALES DIS FRANCE SA** [FR/FR]; 6, rue de la Verrerie, 92190 Meudon (FR). **THALES DIS DESIGN SERVICES SAS** [FR/FR]; route de la Côte d'Azur Arteparc, Bâtiment D, 13590 Meyreuil (FR).

(72) Inventors: **LOUBET MOUNDI, Philippe**; c/o THALES DIS FRANCE SA, Intellectual Property Department, 6, rue de la Verrerie, 92190 Meudon (FR). **NAURA, David**; c/o THALES DIS FRANCE SA, Intellectual Property Department, 6, rue de la Verrerie, 92190 Meudon (FR). **COULON, Jean Roch**; c/o THALES DIS FRANCE SA, Intellectual Property Department, 6, rue de la Verrerie, 92190 Meudon (FR).

(74) Agent: **BRICKS, Amélie**; Axalto SA, 6, rue de la Verrerie, 92190 Meudon (FR).

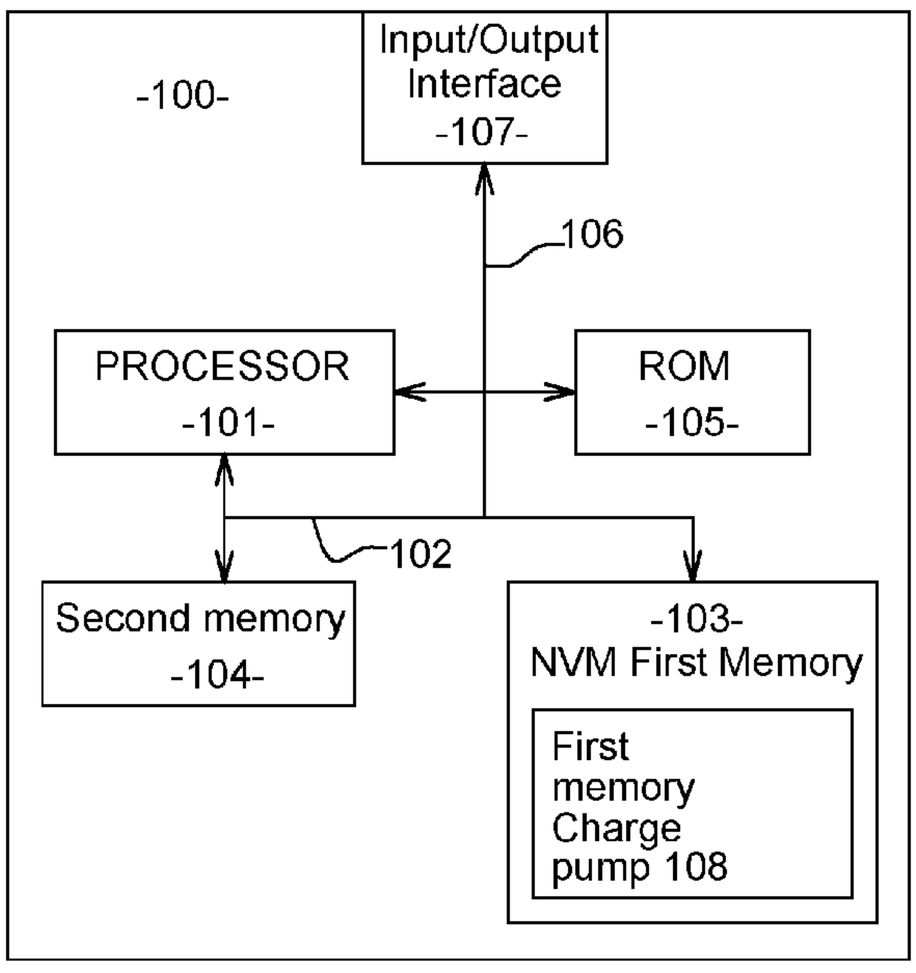
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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).

(54) Title: METHOD FOR SECURE EXECUTING OF A SECURITY RELATED PROCESS

(57) Abstract: The present invention relates to a method for executing a security related process comprising at least a first operation and a subsequent programming operation of a memory area in a first memory row of a first memory of a system and using as input security data stored in said second memory of said system, wherein said first memory is a non-volatile memory and said system comprises a first memory charge pump, said method comprising, when the execution of said security related process is triggered: - opening (S2) the first memory row - charging (S3) said first memory charge pump, - performing (S4) said first operations of the security related process, based on said security data from the second memory, - performing (S5) said programming operation of said memory area in said opened first memory row using said charged charge pump..

Fig. 2



WO 2021/122907 A1

[Continued on next page]

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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

METHOD FOR SECURE EXECUTING OF A SECURITY RELATED PROCESS

FIELD OF THE INVENTION

The present invention relates to a method for securely executing a security related process comprising Non Volatile Memory (NVM) programming, said method protecting the writing of information in a NVM memory, and more particularly preventing NVM programming detection by an attacker.

BACKGROUND OF THE INVENTION

When a security related process comprising sensitive operations such as cryptographic operations is being executed, it may be required from time to time to write some data to a non-volatile memory (NVM). For example, most secure devices and algorithms rely on hardware security sensors or software countermeasures which monitor the execution environment or the behavior of the device or algorithm to be protected. When an abnormal behavior is detected, such devices or algorithm usually keep track of such a detection by updating a security counter value in a non-volatile memory (NVM).

A problem is that writing such a value in a NVM requires charging a NVM charge pump, which induces a spike of the current consumption of the device, as shown on **Figure 1**. As a result, an attacker monitoring the power consumption may easily detect such a charging of the pump, be aware that a write operation in the NVM is being performed, and use it for his own profit. For example, in the case of a security counter update, he may trigger a power cut off in order to prevent the update of the security counter. By doing so, the counter is never updated and the attacker may perform attacks again and again until he succeeds.

Consequently, there is a need for a method for securely executing a security related process comprising NVM programming and enabling to program the NVM without any visible impact on the device power consumption.

SUMMARY OF THE INVENTION

For this purpose and according to a first aspect, this invention therefore relates to a method for executing a security related process comprising at least a first operation and a subsequent programming operation of a memory area in a first memory row of a first memory of a system and using as input security data stored in a second memory of said system, wherein said first memory is a non-volatile memory and said system comprises a first memory charge pump, said method comprising, when the execution of said security related process is triggered:

- opening the first memory row,
- charging said first memory charge pump,
- performing said first operations of the security related process, based on said security data from the second memory,
- performing said programming operation of said memory area in said opened first memory row using said charged charge pump.

By doing so, the charge pump is precharged and the row is open even before the execution of the first operations of the security related process starts. Then, when the programming operation is performed, it is performed much more quickly, without waiting for the charging of the pump and the opening of the first row, and it does not induce a current consumption spike that could be detected by an attacker.

The security data used for performing the first operations of the security related process may be copied from the first memory to the second memory before charging the first memory charge pump or opening the first memory row.

Such a copy operation ensures that this data remains available, in the second memory, while the charged state of the charge pump prevents any reading of the first memory.

In an embodiment wherein said system comprises a hardware security sensor or is configured for executing a software countermeasure, said programming operation of the method according to the first aspect may comprise writing, in said first memory,

permanent security counters logging some abnormal behavior detected by said hardware security sensor or said software countermeasure.

Said second memory may be among a cache memory, a Random Access memory (RAM), a Non Volatile memory (NVM) or a Read Only memory (ROM).

Said first memory charge pump may be charged at a predetermined frequency such that it induces no visible spike of the current consumption of the system.

By doing so, no current consumption spike occurs because of the charging of the pump, even before the execution of the first operations.

According to a second aspect, this invention therefore relates also to a computer program product directly loadable into the memory of at least one computer, comprising software code instructions for performing the steps of the method according to the first aspect when said product is run on the computer.

According to a third aspect, this invention therefore relates also to a non-transitory computer readable medium storing executable computer code that when executed by an system comprising at least one processor, a first memory, a first memory charge pump and a second memory performs the method according to the first aspect.

According to a fourth aspect, this invention therefore relates also to an system comprising at least one processor, a first memory, a first memory charge pump and a second memory configured to perform the method according to the first aspect.

BRIEF DESCRIPTION OF THE DRAWINGS

The following description and the annexed drawings set forth in detail certain illustrative aspects and are indicative of but a few of the various ways in which the principles of the embodiments may be employed. Other advantages and novel features will become apparent from the following detailed description when considered in

conjunction with the drawings and the disclosed embodiments are intended to include all such aspects and their equivalents.

- Figure 1 is a schematic illustration of an oscilloscope snapshot of a NVM programming current consumption according to the prior art;
- Figure 2 is a schematic illustration of a system according to an embodiment of the present invention;
- Figure 3 is a schematic illustration of a method according to an embodiment of the present invention;
- Figure 4 is a schematic illustration of an oscilloscope snapshot of a NVM programming current consumption of a system according to an embodiment of the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

The invention aims at securing the execution of a security related process comprising a silent programing of a memory area of a non-volatile memory (NVM), called first memory, of a system.

Figure 2 is a schematic illustration of such a system 100. It may include a processor 101 connected via a bus 102 to the NVM first memory 103 and to at least one second memory 104 among a cache memory, a random access memory (RAM), another NVM memory or a ROM. It may also include a read-only memory (ROM) 105.

The system 100 may further include a connector 106 connected to the processor.

The system 100 may also include input/output means 107 providing interfaces to the user of the system 100, such as one or more screens, loudspeakers, a mouse, tactile surfaces, a keyboard etc...

The system 100 further includes a first memory charge pump 108 operable to program memory areas of the first memory.

The invention takes place in the context of the execution of a security related process using as input security data stored in the first or second memory and performing at least a first operation. Such a security related process may for example be a cryptographic process generating a ciphered value or a signature, or an operation copying a secret key. Such security data may be sensitive data such as identity data or a secret key. It may also comprise the code to be executed to perform some operations of the security related process.

The security related process may comprise a write operation in a non-volatile memory as a routine operation, for example for updating a counter indicating a number of time a particular process or a key has been used. It may also comprise such a write operation as a counter measure when an attack is detected during the execution of the security related process. For example, if an attack is detected during the execution of this at least one operation, a NVM programming of a memory area is requested in order to update in the NVM a security counter value indicating a number of time an attack has been detected . In the following paragraphs, it is supposed that the memory area programmed by the NVM programming operation is located in a first memory row of the first memory.

The system may further comprise one or more hardware security sensors or it may be configured for executing a software countermeasure, such that these sensors or software countermeasure are able to detect an abnormal behavior likely to be the result of an attack. In such a case, the programming operation of the first memory may comprise writing, in the first memory, permanent security counters logging some abnormal behavior detected by said hardware security sensor or said software countermeasure.

As shown on Figure 1, when a programing operation of a memory area of a first row of the first memory of the system is requested, the following steps have to be performed:

- A configuration step during which operations preparing the NVM programming are executed (CPU execution).

- A row opening step during which the row to be programmed is opened. The duration of this step is called T1.
- A pump charging step during which the charging pump of the first memory is charged. The duration of this step is called T2.
- A programming step during which NVM programming is performed using the charged charge pump. The duration of this step is called T3.
- A row closing step during which the programmed row is closed. The duration of this step is called T4.

The main idea of the invention, in order to make such a programming of the first memory invisible to an attacker, is to anticipate the pump charging step and row opening step at the very beginning of the execution of the security related process. By doing so, the charging pump is already ready to program the first memory when such a programming is required and the programming step may be performed much more quickly, without inducing any power consumption spike.

The following paragraphs describe more precisely the steps of the method according to the invention, shown on **Figure 3**, performed by the system for executing a security related process comprising at least a first operation and a subsequent programming operation of a memory area of a first memory row of the first memory.

During a first step S1, the system may copy the security data from the first memory to the second memory. This operation is necessary when the security data are not already stored in the second memory, in order to keep the security data available after the charge pump of the first memory has been charged, which will be performed in the next step. Indeed, charging the charge pump makes it impossible to perform any reading operation in the first memory until the first memory programming is performed, the pump discharged and the row is closed. Copying the security data to the second memory guaranties that the processor will be available to read it when the data is needed as input for executing operations of the security related process. This first step is performed if needed as soon as the execution of the security related process is triggered.

In a second step S2, the system opens the first memory row of the first memory. At the end of this step, the system is ready to program a memory area of the first memory row despite no programming request has been issued yet.

In a third step S3, the system charges the first memory charge pump. This step may be performed either before or after the second step S2.

In a fourth step S4, the system performs the first operations of the security related process, based on the security data from the second memory. During this step, the security data, needed as input data to the first operations, may not be accessed in the first memory because the charge pump is in a charged state. Therefore, the processor of the system reads the security data in the second memory where it has been copied if needed during the first step described above. At the end of the first operations, a programming of the first memory may be requested, either by the first operations themselves, or because an abnormal behavior was detected during the execution of the first operations and because for example the update of a counter or a log in the first memory is needed.

In a fifth step S5 the programming operation of said memory area in said opened first memory row is performed using said charged charge pump.

The fifth step S5 may be skipped when no programming operation of the NVM is requested, for example when such a programming would be triggered by the detection of an attack but no attack has been detected.

In a sixth step S6 the first row may be closed.

The current consumption of the system resulting from these steps is shown on **Figure 4**. Contrarily to Figure 1, no consumption spike appears from the start of the execution of the first operations to the closing of the first row. Indeed, in the method according to the invention, the charge pump has already been charge, in the third step S3, when the first operations are performed in the fourth step S4.

In addition, the time between the issuance of the request to program the first memory, issued by the first operations or because an attack has been detected at some point during their execution, and the closing of the first row is much shorter. On Figure 1 it was at least equal to T1+T2+T3+T4 = 12 + 6.6 + 18 + 7.7 µs. On figure 4, it is close to T3+T4 = 18 + 7.7 µs since the pump charging and row opening have been performed beforehand.

A spike in the current consumption may still be visible when the charge pump is charged, before the execution of the first operations. In order to reduce or avoid such a spike, the charge pump may be charged at a predetermined lower frequency, for example up to 8 times lower than usual.

According to a second aspect, this invention therefore relates also to a computer program product directly loadable into the memory of at least one computer, comprising software code instructions for performing the steps of the methods according to the first aspect when said product is run on the computer.

According to a third aspect, this invention therefore relates also to a non-transitory computer readable medium storing executable computer code that when executed by an system 100 above described performs the methods according to the first aspect.

According to a fourth aspect, this invention therefore relates also to an system 100 above described comprising a processor 101, a first memory 103, a first memory charge pump 108 and a second memory 104 configured to perform the methods according to the first aspect.

CLAIMS

1. A method for executing a security related process comprising at least a first operation and a subsequent programming operation of a memory area in a first memory row of a first memory (103) of a system (100) and using as input security data stored in a second memory (104) of said system (100), wherein said first memory is a non-volatile memory and said system comprises a first memory charge pump (108), said method comprising, when the execution of said security related process is triggered:

- opening (S2) the first memory row,
- charging (S3) said first memory charge pump,
- performing (S4) said first operations of the security related process, based on said security data from the second memory,
- performing (S5) said programming operation of said memory area in said opened first memory row using said charged charge pump.

2. The method of claim 1, comprising, copying (S1) said security data from the first memory to the second memory before charging the first memory charge pump or opening the first memory row.

3. The method of claim 1 or 2, wherein, said system comprising a hardware security sensor or being configured for executing a software countermeasure, said programming operation comprises writing, in said first memory, permanent security counters logging some abnormal behavior detected by said hardware security sensor or said software countermeasure.

4. The method according to any of claims 1 to 3, wherein said second memory (104) is among a cache memory, a Random Access memory (RAM), a Non Volatile memory (NVM) or a Read Only memory (ROM).

5. The method according to any of claims 1 to 4, wherein said first memory charge pump is charged at a predetermined frequency such that it induces no visible spike of the current consumption of the system.

6. A computer program product directly loadable into the memory of at least one computer, comprising software code instructions for performing the steps of the method according to any one of claims 1 to 5 when said product is run on the computer.

7. A non-transitory computer readable medium storing executable computer code that when executed by an system (100) comprising at least one processor (101), a first memory (103), a first memory charge pump (108) and a second memory (104) performs the steps of the method according to any one of claims 1 to 5.

8. System (100) comprising a processor (101), a first memory (103), a first memory charge pump (108) and a second memory (104) configured to perform the steps of the method according to any one of claims 1 to 5.

Fig. 1

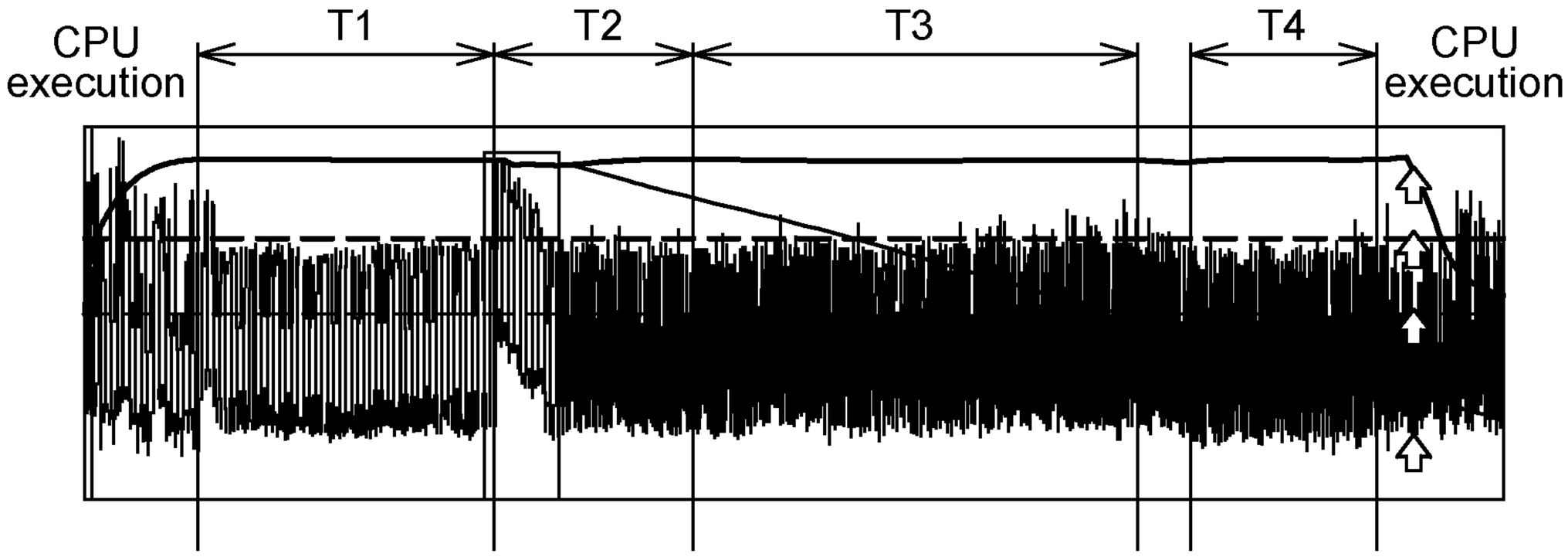

CPU execution
T1
T2
T3
T4
CPU execution

Fig. 2

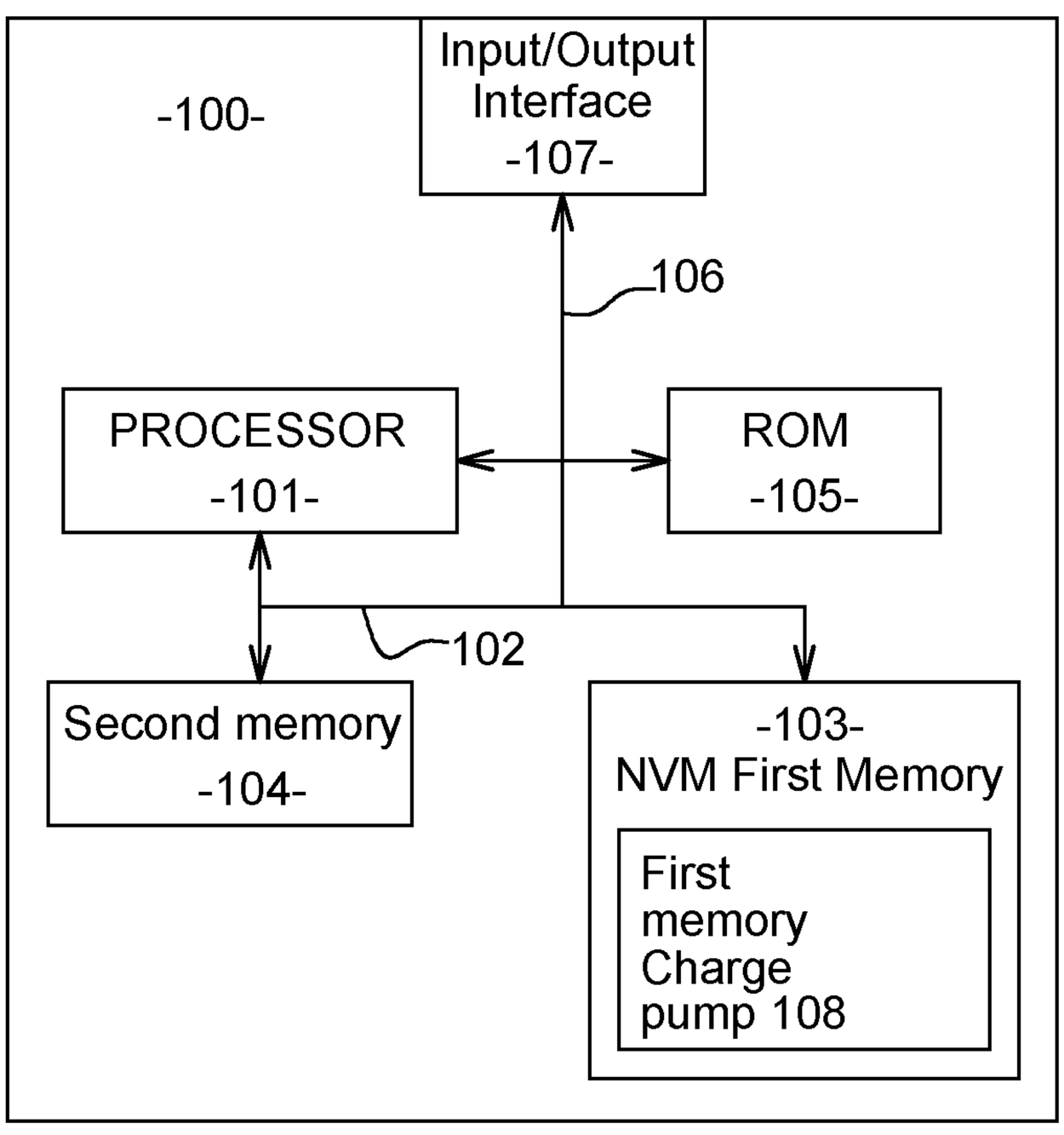

-100-
Input/Output Interface -107-
106
PROCESSOR -101-
ROM -105-
102
Second memory -104-
-103- NVM First Memory
First memory Charge pump 108

Fig. 3

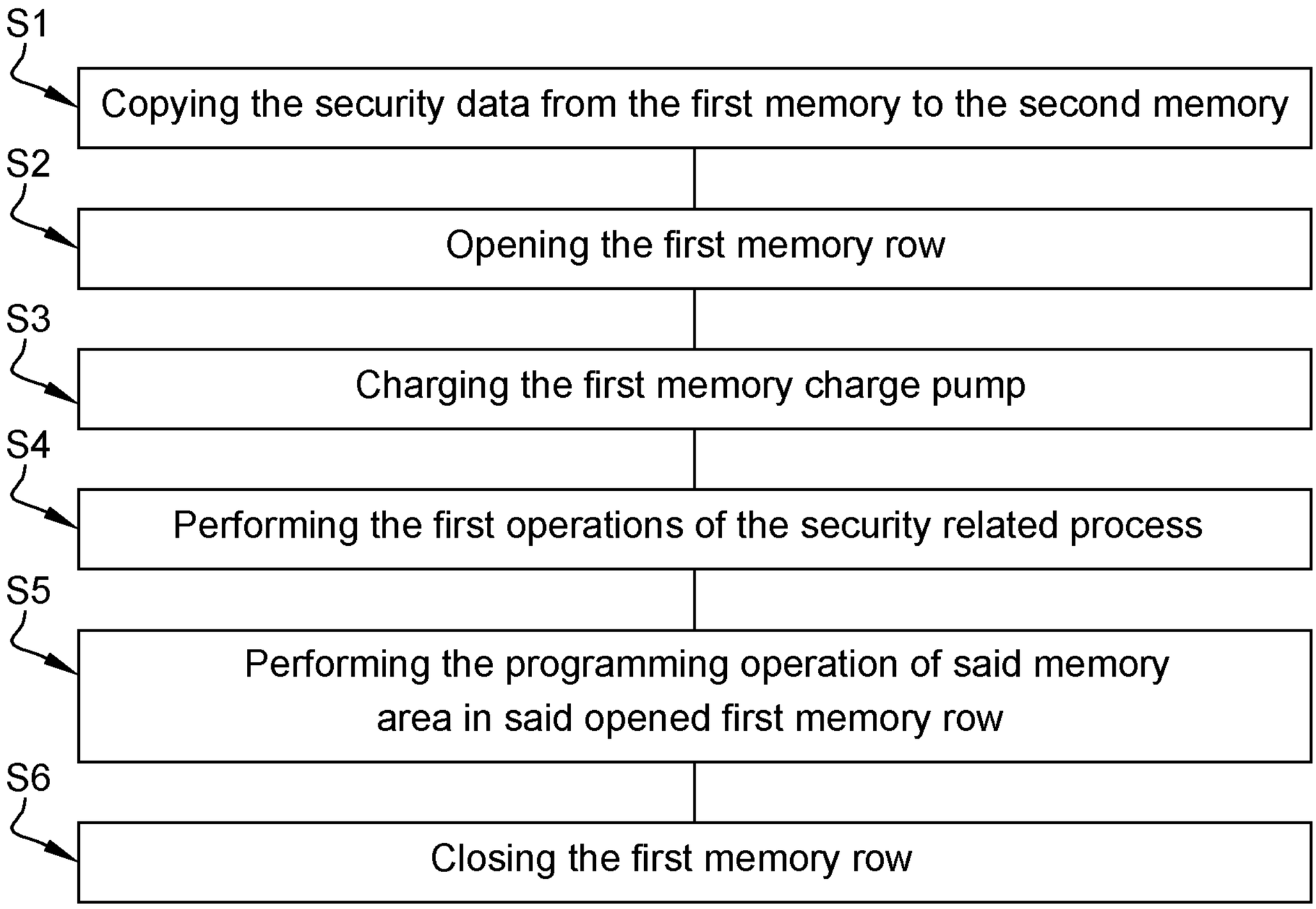
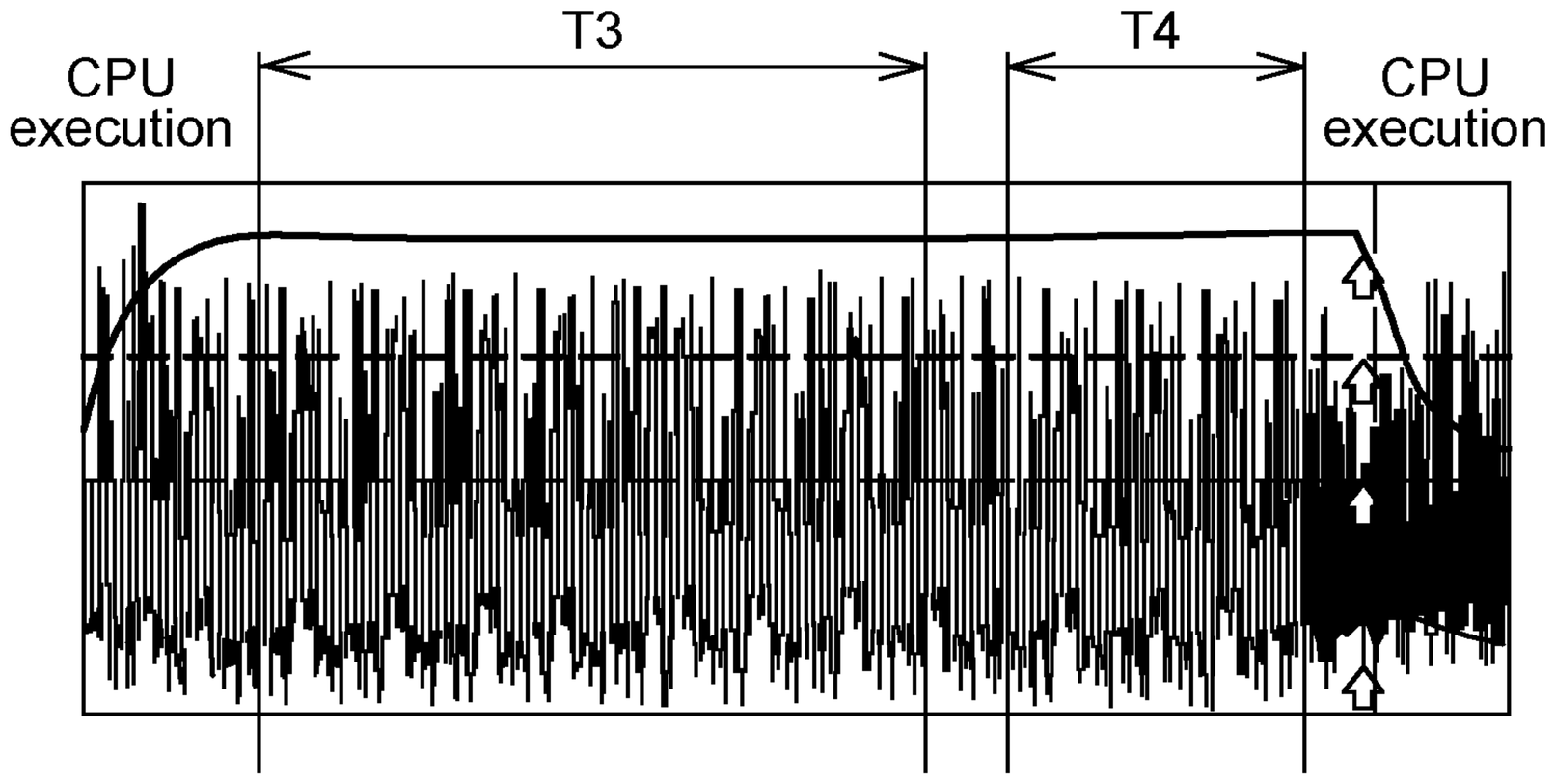

S1
Copying the security data from the first memory to the second memory
S2
Opening the first memory row
S3
Charging the first memory charge pump
S4
Performing the first operations of the security related process
S5
Performing the programming operation of said memory area in said opened first memory row
S6
Closing the first memory row

Fig. 4


T3
T4
CPU execution
CPU execution

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2020/086662

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/75 G06F12/14 G06F21/79 G11C5/14 G11C7/24
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)
G06F G11C

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2019/050602 A1 (SELA ROTEM [IL] ET AL) 14 February 2019 (2019-02-14) abstract paragraph [0023] - paragraph [0024] paragraph [0034] - paragraph [0054] paragraph [0065] paragraph [0071] - paragraph [0081] figures 2, 3, 4B, 5-7	1-8
A	US 2019/114097 A1 (TRAN HIEU VAN [US] ET AL) 18 April 2019 (2019-04-18) the whole document	1-8
A	US 2014/137271 A1 (HYDE RODERICK A [US] ET AL) 15 May 2014 (2014-05-15) the whole document	1-8

☐ 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
25 February 2021	10/03/2021
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Frank, Mario

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2020/086662

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2019050602 A1	14-02-2019	CN 109388974 A	26-02-2019
		DE 102018114266 A1	14-02-2019
		US 2019050602 A1	14-02-2019
US 2019114097 A1	18-04-2019	CN 111226279 A	02-06-2020
		EP 3673486 A1	01-07-2020
		JP 2020537280 A	17-12-2020
		KR 20200071102 A	18-06-2020
		TW 201923771 A	16-06-2019
		TW 202030736 A	16-08-2020
		US 2019114097 A1	18-04-2019
		US 2019121556 A1	25-04-2019
		WO 2019074652 A1	18-04-2019
US 2014137271 A1	15-05-2014	NONE	