



- (51) International Patent Classification:
G06F 21/00 (2006.01)
- (21) International Application Number:
PCT/EP2012/054826
- (22) International Filing Date:
19 March 2012 (19.03.2012)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
11160420.3 30 March 2011 (30.03.2011) EP
- (71) Applicant (for all designated States except US): **IRDETO CORPORATE B.V.** [NL/NL]; 105 Taurus Avenue, NL-2132 LS Hoofddorp (NL).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): **DOUMEN, Jeroen Mathias** [NL/NL]; Irdeto Corporate B.V., 105 Taurus Avenue, NL-2132 LS Hoofddorp (NL).
- (74) Agents: **PELLY, Jason Charles** et al.; Boulton Wade Tenant, Verulam Gardens, 70 Gray's Inn Road, London WC1X 8BT (GB).

- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, 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, KM, 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, 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.
- (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, MD, 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, ML, MR, NE, SN, TD, TG).

Published:

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

(54) Title: ENABLING A SOFTWARE APPLICATION TO BE EXECUTED ON A HARDWARE DEVICE

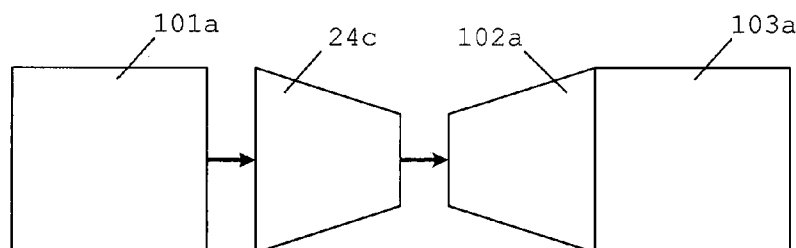


Fig. 5

(57) Abstract: The invention provides a method, a hardware circuit and a hardware device for enabling a software application to be executed on a hardware device in dependence of the hardware circuit, while preventing the execution of a binary copy of the application in another hardware device. Challenge data originating from the software application is input to a hardware circuit of the hardware device, wherein the hardware circuit is configured to perform a deterministic function. Response data is generated by the hardware device, which is used to manipulate at least a part of the software application to thereby enable the software application to be executed.



Enabling a software application to be executed on a hardware device

FIELD OF THE INVENTION

The present invention relates to protecting software applications. More specifically, the invention relates to enabling a software application to be executed on a hardware device.

BACKGROUND

Software obfuscation is a known technology for implementing software programs such that they are hard to reverse engineer. This technology typically includes the replacing of software functions with a sequence of table lookup operations and merging the function lookup with transform functions that make it substantially infeasible to discover the function and the function parameters. The resulting secured software program performs input and/or output operations that consist of transformed parameters. These transformed parameters may require specific adaptations in modules interfacing with the secured software program.

Data and software obfuscation techniques make use of transformation functions to obfuscate intermediate results. The concept of transformation functions differs from encryption, which is clarified in general with reference to Fig.1.

Assume that there exists an input domain ID with a plurality of data elements in a non-transformed data space. An encryption function E using some key is defined that is configured to accept the data elements of input domain ID as an input to deliver a corresponding encrypted data element in an output domain OD. By applying a decryption function D using a key that corresponds to the key used by the encryption function E, the original data elements of input domain ID can be obtained by applying the decryption function D to the data elements of output domain OD. In a non-secure environment (typically referred to as "whitebox"), an adversary is assumed to know input and output data elements and have access to internals of

encryption function E during execution. Unless extra precautions are taken in this environment, the key can be derived.

Additional security can be obtained in a non-secured environment by applying transformation functions to the input domain ID and output domain OD , i.e. the transformation functions are input- and output operations. Transformation function T_1 maps data elements from the input domain ID to transformed data elements of transformed input domain ID' of a transformed data space. Similarly, transformation function T_2 maps data elements from the output domain OD to the transformed output domain OD' . Transformed encryption and decryption functions E' and D' can now be defined between ID' and OD' . In case inverse transformations are to be performed, e.g. when results are to be communicated to the non-transformed space, T_1 and T_2 are injections.

Using transformation functions T_1 , T_2 , together with encryption techniques implies that, instead of inputting data elements of input domain ID to encryption function E to obtain encrypted data elements of output domain OD , transformed data elements of domain ID' are input to transformed encryption function E' by applying transformation function T_1 . Transformed encryption function E' combines the inverse transformation function T_1^{-1} and the transformation function T_2 in the encryption operation to protect the confidential information, such as the key. Then transformed encrypted data elements of domain OD' are obtained. Keys for encryption functions E or decryption function D cannot be retrieved when analyzing input data and output data in the transformed data space.

One of the transformation functions T_1 , T_2 should be a non-trivial function. In case, T_1 is a trivial function, the input domains ID and ID' are typically the same domain. In case, T_2 is a trivial function, the output domains are typically the same domain.

In general, secured software applications use transformed intermediate results which are unusable when intercepted. This property enables the protection of confidential data in secured software applications. In order to enable the secured software application to limit its

functionality to a few (or one) particular devices, several technologies are known.

The transformation technology can be used to secure a wide range of software programs. Fig.2 and Fig.3 illustrate a known example of how a physical smart card used in a digital TV environment (see Fig.2) can be replaced by a secured software implementation of the smart card functionality (see Fig.3). It is to be understood that the present invention is not limited to the field of digital TV.

Fig.2 schematically shows an example of a typical digital TV receiver 2a that receives encrypted digital TV content from a head-end 1 and outputs a signal to an output device 4 for displaying the digital TV content to an end-user. Arrows indicate a data flow in the direction as indicated. The head-end 1 transmits the digital TV content to a large number of receivers 2a. The receiver 2a uses an input module 21 to acquire the transmitted digital TV signal, which is subsequently provided to a content processing module 22a. The content processing module 22a is typically based on a general purpose processing unit 23a (e.g. using a 32 bit CPU) extended with a secured electronic circuit 24a to implement security functions such as encryption, decryption and secure key storage. Such processing may involve processing steps implemented in a detachably attached smart card 3. The result of the content processing is a signal suitable for rendering on the output device 4 such as a TV set.

The head-end 1, secured circuit 24a and smart card 3 are secured modules that are implemented such that it is difficult for an attacker to modify its intended operation. The input module 21, processing unit 23a, output device 4 and the interfaces between the modules are typically accessible to an attacker, so their proper operation cannot be relied upon.

Fig.3 schematically shows an alternative example of a known digital TV receiver 2b that receives encrypted digital TV content from a head-end 1 and outputs a signal to an output device 4 for displaying the digital TV content to an end-user. Arrows indicate a data flow in the direction as indicated. The head-end 1 transmits the digital TV content to a large number of receivers 2b. The receiver 2b uses an input module 21 to acquire

the transmitted digital TV signal, which is subsequently provided to a content processing module 22b. The content processing module 22b is typically based on a general purpose processing unit 23b (e.g. using a 32 bit CPU) extended with a secured electronic circuit 24b to implement security functions such as encryption, decryption and secure key storage.

Given the common availability of a secured circuit module 24b, the smart card 3 of Fig.2 can be replaced by a secured software implementation running in the content processing module 22b. Hereto the processing unit 23b is configured with additional software for the functions that used to be implemented by the smart card.

As in the example of Fig.2, the head-end 1 and secured circuit 24b are secured modules that are implemented such that it is difficult for an attacker to modify its intended operation. The input module 21, processing unit 23b, output device 4 and the interfaces between the modules are typically accessible to an attacker, so their proper operation cannot be relied upon. In order to secure the smart card functions in the to the attacker accessible environment of the processing unit 23b, the functions are implemented using secured software technology. The secured circuit 24b contains a memory for a set of secret keys that are used together with the output of the processing unit 23b to derive content keys for use in a descrambling circuit of the secured circuit 24b. One of the secret keys is installed during the manufacturing process. This so called Chip Secret Key is used to securely load other secret keys. A key loading message is embedded in the secured software and it is used to load a known secret key in the secure module. The secured software also has the fixed key encryption routine to encrypt a content key with the secret key that is stored in encrypted form in the key loading message. The fixed key encryption routine in the secured software application limits the application to execute on the device that can decrypt the key loading message associated with the secured software application.

The known technologies for enabling an obfuscated software application to be executed on a particular hardware device, also known as node locking, have in common that the

output of a processing unit running obfuscated software is used by a secured circuit as an input to one or more security functions of the secured circuit. If the output of the processing unit is incorrect, then the secured circuit will not be able to perform the security function correctly. It is not prevented though that the software application itself can be executed. E.g. in the examples of Fig.2 and Fig.3 the output of the processing unit 23a,23b is used by the secured circuit 24a,24b as an input key enabling the decryption of the digital TV content or as a qualifier that the receiver 2a,2b has knowledge about a (secret) key.

It is known that a software application running in a processing unit may poll predefined memory locations and use the resulting data in the further execution of the application. If the resulting data is incorrect then the software application will stop functioning correctly. The memory location is e.g. a specific hardware register containing e.g. unique values or cryptographic keys. The security provided by this polling method is limited, because the content of the memory locations may be modified.

It is known that a probing function implemented in a processing unit may e.g. activate a physically unclonable function (PUF) that produces a response result based on a challenge input provided to the function. PUFs are difficult to implement, because they have an initialisation problem. A further problem associated with PUFs is that a sender of a challenge input needs to know the possible response output of the PUF when triggered by the challenge input beforehand, because each PUF in each receiver is unique and produces an unpredictable response to a challenge. The PUF can only be characterised by a suitably large set of challenge-response pairs which may be obtained at manufacturing time or at a later stage in the deployment of the device by measuring responses to challenges.

There is a need for an improved technology for enabling the execution of a general purpose software application in a hardware device, while preventing the execution of the application or a binary copy of the application in another

hardware device, without the above identified drawbacks of the prior art.

SUMMARY OF THE INVENTION

5 It is an object of the invention to provide for a technology enabling a software application to be executed in a hardware device, while preventing the execution of the application or a binary copy of the application in another hardware device.

10 According to an aspect of the invention a computer-implemented method is proposed for enabling a software application to be executed on a hardware device in dependence of a hardware circuit in the hardware device. The method comprises inputting challenge data originating from the software
15 application to a hardware circuit of the hardware device. The hardware circuit is configured to perform a deterministic function. The method further comprises generating response data using function with the challenge data as input to the function. The method further comprises using the response data to
20 manipulate at least a part of the software application to thereby enable the software application to be executed.

According to an aspect of the invention a hardware circuit is proposed for enabling a software application to be executed on a hardware device comprising the hardware circuit
25 and in dependence of the hardware circuit. The hardware circuit is configured to perform a deterministic function that uses challenge data originating from the software application as input to the function to generate response data for manipulating at least a part of the software application to thereby enable
30 the software application to be executed.

Deterministic functions differ from non-deterministic functions such as PUFs. Deterministic functions typically return the same result any time they are called with a specific set of input values. Non-deterministic functions typically return
35 different results each time they are called with a specific set of input values. Moreover, deterministic functions can typically be expressed mathematically, whereas a non-deterministic function such as a PUF cannot be expressed mathematically.

The operation of the software application (or at least some aspects of its operation) depends on the presence of the hardware circuit with the deterministic function. Hence, it is the presence of the hardware circuit that enables the hardware device to unlock the use of the software application. Thus, the execution of a software application is anchored to a hardware circuit, hereby enabling the software application to be executed only on the particular hardware device comprising the hardware circuit with the deterministic function.

It is to be understood that enabling the software application to be executed means that the software application can be executed correctly or as intended. The response data from a hardware circuit that is not intended to be used with the software application may be used to manipulate the software application, but in this case the software application will be manipulated incorrectly, resulting in e.g. the execution of the software application to produce meaningless output or to be disruptive.

The embodiments of claims 2 and 15 advantageously enable the execution of the software application in a limited number of hardware devices. If the function is unique to one hardware circuit then only the one hardware device comprising the hardware circuit with the unique function can execute the software application. If the function is unique to a group of hardware circuit then only the hardware devices comprising a hardware circuit from the group of hardware circuits can execute the software application.

The embodiments of claims 3-6 and 16 advantageously enable the use of cryptographic functions embedded in hardware, which are known as such, in the hardware circuit. Examples of suitable cryptographic functions are an encryption function, a decryption function, a keyed hash function and a pseudo random number generator.

The embodiment of claim 7 advantageously enables a software application to be anchored to the hardware circuit when being executed in the hardware device. It is possible that the inverted response data is data enabling the challenge data to be derived or data wherein the challenge data is already further processes by e.g. the hardware circuit.

The embodiment of claim 8 advantageously enables cryptographic functions in a software application to be anchored to the hardware circuit when being executed in the hardware device.

5 The embodiment of claim 9 advantageously enables a software application to be anchored to the hardware circuit using fixed-key cryptographic functions when being executed in the hardware device.

10 The embodiment of claim 10 advantageously enables a software application to be anchored to the hardware circuit in an alternative manner when being executed in the hardware device. The inverse function compares the output of the function in the hardware device with the output of the further function in the secured software module and uses the comparison result to
15 generate the inverted response data. If the comparison result is incorrect, then the inverted response data will be generated such that it is different from the challenge data to thereby disable further execution of the software application.

20 The embodiment of claim 11 enables an alternative to the embodiments of claims 7-10.

 The embodiment of claim 12 advantageously enables the decryption of an encrypted software application to be anchored to the hardware circuit.

25 According to an aspect of the invention a computer-implemented method is proposed for adding a random data block to an encrypted software application. The method comprises dividing a software image of the encrypted software application into equal length blocks. The method further comprises determining a replacement block being one of the blocks to be replaced by the
30 random data block. The method further comprises applying a block cipher-based message authentication code (CMAC) function to the blocks until the replacement block. The method further comprises applying a reversed block cipher-based message authentication code (CMAC) function to the blocks starting from the last block
35 until the block after the replacement block. Tag T equals the encryption key used to encrypt the encrypted software. The tag T is decrypted using CMAC key K . The decrypted tag T is added to CMAC key dependent value V_1 and the last block to obtain an intermediate result. The intermediate result is decrypted using

the CMAC key K . The decrypted intermediate result is added to the preceding block to obtain a further intermediate result and repeating the decrypting and adding of further intermediate results until the replacement block. The method further
5 comprises adding the last result from the block cipher-based message authentication code (CMAC) function to the last result of the reverse block cipher-based message authentication code (CMAC) function to obtain the random data block. The method
10 further comprises replacing the replacement block with the random data block. The CMAC key K corresponds to a further CMAC key K in a hardware circuit of an hardware device.

Thus, an encrypted software application can be obtained, which decryption is anchored to a hardware circuit of a particular hardware device.

15 The embodiment of claim 17 advantageously enables the hardware circuit to be embedded in existing chips or chipsets.

According to an aspect of the invention a hardware device is proposed comprising a hardware circuit having one or more of the above described features.

20 The embodiments of claims 18 and 19 advantageously enable the software application to be executed on frequently used hardware devices.

According to an aspect of the invention a software application is proposed, which, when being executed by a
25 processor, is adapted to manipulate at least a part of the software application to thereby enable the software application to be executed on a hardware device in dependence of a hardware circuit in the hardware device, by using response data that is generated using a deterministic function in the hardware circuit
30 that uses challenge data as input to the function, wherein the challenge data originates from the software application.

Hereinafter, embodiments of the invention will be described in further detail. It should be appreciated, however, that these embodiments may not be construed as limiting the
35 scope of protection for the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

Aspects of the invention will be explained in greater detail by reference to exemplary embodiments shown in the drawings, in which:

Fig.1 is a diagram clarifying transformation functions and encryption in general terms;

Fig.2 is a schematic illustration of a prior art digital TV receiver system for processing encrypted digital TV content;

Fig.3 is a schematic illustration of another prior art digital TV receiver system for processing encrypted digital TV content;

Fig.4 is a schematic illustration of a digital TV receiver system for processing encrypted digital TV content according to an exemplary embodiment of the invention;

Fig.5 is a schematic illustration of a software application that is anchored to a hardware circuit according to an exemplary embodiment of the invention;

Fig.6 is a schematic illustration of a CMAC function as used in a hardware circuit according to an exemplary embodiment of the invention;

Fig.7 is a schematic illustration of a CMAC function as used in hardware circuit according to another exemplary embodiment of the invention;

Fig.8 is a schematic illustration of a CMAC function as used in hardware circuit according to another exemplary embodiment of the invention;

Fig.9 is a schematic illustration of a software application that is anchored to a hardware circuit according to another exemplary embodiment of the invention;

Fig.10 is a schematic illustration of a software application that is anchored to a hardware circuit according to another exemplary embodiment of the invention;

Fig.11 is a schematic illustration of a software application that is anchored to a hardware circuit according to another exemplary embodiment of the invention;

Fig.12 is a schematic illustration of a software application that is anchored to a hardware circuit according to another exemplary embodiment of the invention;

Fig.13 is a schematic illustration of a CMAC function for creating an encrypted software application that is anchored to a hardware circuit according to an exemplary embodiment of the invention;

Fig.14 is a schematic illustration of an encryption function as used in hardware circuit according to an exemplary embodiment of the invention.

DETAILED DESCRIPTION OF THE DRAWINGS

The invention enables a software application to be executed in a hardware device, while preventing the execution of the application or a binary copy of the application in another hardware device. Challenge data originating from the software application is input to a hardware circuit of the device. The challenge data comprises e.g. runtime data such as state information or parameter values of the application when being executed in a processing unit. Alternatively the challenge data comprises at least a part of the software image of the application itself. The hardware circuit processes the challenge data using a deterministic function, which is preferably uniquely defined for a particular hardware circuit, and returns the response data for further processing of the software application.

Various techniques can be used to implement the hardware circuit. The hardware circuit can e.g. be implemented using a transistor network on a chip. Another example is an implementation by a separate microcontroller on the same chip or using software in an isolated process. Another example is an implementation in a software process using a cryptography co-processor. Another example is to use a node-locking chip on the same printed circuit board (PCB), but external to the main chip containing the CPU. It is to be understood that the implementation of the hardware circuit is not limited to these examples and that other known techniques can be used to implement a hardware circuit that can be configured to perform a deterministic function.

Deterministic functions differ from non-deterministic functions such as PUFs. Deterministic functions typically return the same result any time they are called with a specific set of input values. Non-deterministic functions typically return
5 different results each time they are called with a specific set of input values. Moreover, deterministic functions can typically be expressed mathematically, whereas a non-deterministic function such as a PUF cannot be expressed mathematically. It is known that the output of PUFs may be made deterministic by
10 applying e.g. error correction mechanisms to the output, but this does not make the PUF itself deterministic.

Both secured and non-secured software applications can benefit from the invention, but for optimal results the software application is secured using e.g. software obfuscation
15 techniques as non-secured software applications could be modified to ignore the hardware circuit.

In case of the execution of a secured software application a first module of the secured software application sends runtime data as challenge data to the hardware circuit.
20 The hardware circuit processes the challenge data using the preferably unique function and returns the response data to a second module of the secured software application to perform an inverse operation of the preferably unique function to undo the effects of the hardware circuit. Herewith the software
25 application is effectively anchored to the hardware circuit.

In case of the challenge data comprising at least a part of the software image of the application itself, the challenge data is input to the hardware circuit. The hardware circuit processes the data using the preferably unique function
30 and returns the response data, which, possibly after some conversion operation, is used as a decryption key to decrypt the software image. Herewith the software application is effectively anchored to the hardware circuit.

The unique properties of the hardware circuit and the
35 associated further processing of its output make it substantially impossible to run the software application on a different device than the device it is intended for.

The hardware circuit can be included in a wide range of CPU's (including embedded devices), GPU's and programmable I/O peripherals.

Fig.4 schematically shows an example of how the invention can be used in a digital TV environment. It is to be understood that the present invention is not limited to the field of digital TV and may be used to anchor any software application to a CPU containing the hardware circuit. The hardware circuit allows whitebox attack resistant software to be strongly coupled to a single device. The invention extends the uniqueness of the hardware circuit to the software application that effectively is anchored to the hardware circuit. Such anchored software applications can be used in e.g. embedded devices such as digital TV receivers or in e.g. PC's, tablet PC's, smart phones, Internet (cloud) servers, graphics cards, or any other I/O device.

In the example of Fig.4, a digital TV receiver 2c receives encrypted digital TV content from a head-end 1 and outputs a signal to an output device 4 for displaying the digital TV content to an end-user. Arrows indicate a data flow in the direction as indicated. The head-end 1 transmits the digital TV content to a large number of receivers 2c. The receiver 2c uses an input module 21 to acquire the transmitted digital TV signal, which is subsequently provided to a content processing module 22c. The content processing module 22c is based on a general purpose processing unit 23c (e.g. using a 32 bit CPU) extended or embedded with a hardware circuit 24c. A secured software application for processing the encrypted digital TV content runs in the processing unit 23c. The result of the content processing is a signal suitable for rendering on the output device 4 such as a TV set.

The head-end 1 and hardware circuit 24c are implemented such that it is difficult for an attacker to modify or observe its operation. The input module 21, software executing on the processing unit 23c, output device 4 and the interfaces between the modules are typically accessible to an attacker, so their proper operation cannot be relied upon.

The hardware circuit 24c implements a unique function that processes challenge data containing e.g. state information

from the secured software application. The inverse operation of the function implemented by the hardware circuit 24c is implemented in a module of the secured software application to recover the initial state. Alternatively, data enabling the initial state to be derived or data wherein the initial state is further processed is output by the module. The secured software module inherits the uniqueness of the function implemented by the secured circuit 24c. As the secured software module is preferably unique, other devices with a different hardware circuit are not capable of executing a binary copy of the software application. Replacing the secured software module with another implementation requires knowledge of the preferably unique function implemented by the hardware circuit 24c or the knowledge of the inverse function implemented by the secured software module. Both types of knowledge can only be acquired by reverse engineering. As the implementation of both the hardware circuit 24c and the secured software module is very hard to reverse engineer, it will be very difficult to execute a copy or modified copy of the application on another device.

Fig.5 shows an exemplary embodiment of a software application that is anchored to a hardware circuit. The software application, or a part of the software application, is implemented as a sequence of secured software modules, i.e. secured software module i indicated by 101a and secured software module $i+1$ indicated by 103a in Fig.5. Each secured software module 101a,103a exchanges parameters and/or state information in a transformed domain. The secured software application is anchored to a specific device by anchoring the application to the hardware circuit 24c of the device.

The hardware circuit 24c is configured with a preferably unique function or preferably unique secret data that drives a common function that corresponds to an inverse function implemented in an inverse secured software module 102a. As the interfaces between the secured software modules are protected by transformations, the secured software application will not operate correctly if the output of secured software module i 101a is input directly into the inverse secured software module 102a. In other words, bypassing the hardware anchor is not

possible as it results in a non-functional secured software application.

The inverse secured software module 102a and the secured software module $i+1$ 103a can be implemented as a single module combining the functionalities of the two.

In an alternative exemplary embodiment, which is not shown in a figure, the order of the hardware circuit 24c and the inverse secured software module 102a is reversed. In this embodiment the inverse secured software module performs the function of the hardware circuit 24c and the hardware circuit performs the function of the inverse secured software module 102a. In this embodiment the inverse secured software module and the secured software module i 101a can be implemented as a single module combining the functionalities of the two.

The hardware circuit can be realised using e.g. an existing crypto coprocessor with an integrated block cipher such as AES. A keyed hash function, also known as message authentication code (MAC), can be used as an anchor function. These and other cryptographic functions are made unique by putting a unique (or uniquely derivable) key in each individual chipset during the personalization of hardware circuits. Other key loading mechanisms are possible as well. A block cipher-based MAC function such as Cipher-based MAC (CMAC) is particularly suitable. The CMAC standard works with any block cipher, such as e.g. AES. The CMAC standard is also known as RFC-4493.

The following examples show an implementation of a hardware anchor using the CMAC standard. It is to be understood that the invention is not limited to keyed hash functions such as CMAC and that the invention is not limited to the AES block cipher.

Fig.6 shows an example of a flow chart of a CMAC calculation for a b -bit message M , i.e. the block size of the cipher is b and the message M has a length of b bits. The output of the CMAC is called a tag T . As the block cipher is used as basic building block, the tag T will also be b bits in size. The message M is added to a key-dependent value V_1 using add function \oplus and then encrypted with a key K using an Encrypt function.

If the message block is shorter than b bits, the message M is padded as shown in Fig.7. The padding bits are indicated by $10\dots0$. In this case, a different key-dependent value V_2 is used.

5 With reference to Fig.8, to calculate the CMAC for an arbitrary-length input message M , the message is first divided into message blocks M_i of length b . In the example of Fig.8 message M has a length of $l \times b$ bits and the message M is thus divided into message blocks $M_1, M_2 \dots M_l$. Each block M_i is
10 encrypted by the chosen block cipher under the same key K , with the output of the Encrypt function being added to the next message block. For the final block M_l , the key-dependent value V_1 is also added before this encryption.

15 If the length of the message M is not an exact multiple of b , then the last message block M_l is padded as shown in Fig.7. In this case, the key-dependent value V_2 will be used instead of V_1 .

20 The derivation of V_1 and V_2 are defined as follows, wherein 'Encrypt $_K$ ' denotes an encryption (e.g. AES-128 encryption) using key K , ' 0^b ' denotes an all-zero vector of b -bits, 'MSB' denotes the most significant bit, '<<' denotes a leftwards bit rotation, and \oplus denotes an exclusive-OR.

- 25 1. Let $L = \text{Encrypt}_K(0^b)$
2. If $\text{MSB}(L)=0$, then $V_1 = L \ll 1$;
 Else $V_1 = (L \ll 1) \oplus R_b$
3. If $\text{MSB}(V_1)=0$, then $V_2 = V_1 \ll 1$;
 Else $V_2 = (V_1 \ll 1) \oplus R_b$

30 In step 1, AES-128 with key K is applied to the all-zero input block. In step 2, V_1 is derived through the following operation: If the most significant bit of L is equal to 0, V_1 is the left-shift of L by 1 bit. Otherwise, V_1 is the exclusive-OR of R_b and the left-shift of L by 1 bit. In step 3, V_2 is derived
35 through the following operation: If the most significant bit of V_1 is equal to 0, V_2 is the left-shift of V_1 by 1 bit. Otherwise, V_2 is the exclusive-OR of R_b and the left-shift of V_1 by 1 bit. Herein R_b is a constant predefined in the CMAC standard. For example for $b=128$ $R_{128}=0^{120}10000111$.

As V_1 and V_2 only depend on the key K , they can be pre-computed once and subsequently used for many CMAC calculations. V_1 and V_2 can e.g. be stored in non-volatile memory or computed once on first use.

5 Key K must be securely available to the hardware circuit implementing the cryptographic function such as e.g. the CMAC function. It is to be understood that the invention is not limited to the following examples and that other alternative solutions may be used to securely make the key K available to
10 the hardware circuit.

 Key K can be implemented as an additional key, personalized into the silicon. Alternatively, key K can be derivable from an existing unique chipset key (CSUK) in some fashion, for instance by using a Davies-Meyer type of
15 construction. Alternatively, the key K can be provided to the hardware circuit using a key ladder solution known from securely sending control words to a descrambler module using a session key, which key ladder is adapted to securely send the key K to the hardware circuit instead. Alternatively, a key transport
20 protocol can be used as disclosed in applicant's co-pending European patent application titled "Key Transport Protocol" and having reference number 15464, which is herewith incorporated by reference in its entirety.

 The key transport protocol enables a sender to transmit
25 a key loading message to the receiver. Next, the key is loaded onto the receiver. To create the key loading message, the sender first generates a virtual key, denoted as K^* . Second, the sender secures the virtual key to protect the virtual key's authenticity and confidentiality, thereby producing a secured
30 virtual key. The secured virtual key is then transported as part of a key loading message from the sender to the receiver. The virtual key may be encrypted using a public key associated with the receiver. The secured virtual key may be created by adding a signature using a signature key associated with the sender. The
35 virtual key K^* generated by the sender and a signature verification key associated with the sender are used as inputs to a cryptographic function to produce an output. The cryptographic function is typically a part of the cryptographic

function of the hardware circuit. Said output includes the key K .

Fig.14 shows an example of a flow chart of a calculation of an output value T for a b -bit message M , which is a simplified version of the example of Fig.6. The b -bit message M is directly encrypted with a key K using an Encrypt function. The big advantage of this variant is that it can be supported on existing silicon, by leveraging a memory-to-memory encryption using the standard key ladder. However, it is less flexible as it cannot handle an arbitrary-length input.

In the following example a secured part of a software application is anchored to a hardware circuit using lookup tables as used in e.g. AES cryptography. The hardware circuit anchor is realised using CMAC and an AES crypto coprocessor. The invention is not limited to AES. Any other block cipher may be used in the crypto coprocessor.

Software obfuscation typically implements cryptographic functions as a sequence of lookup tables. With reference to Fig.5, in this example the hardware anchor 24c is implemented as an additional lookup table, between two "regular" secured software tables 101a and 103a. This effectively binds the secured software to the hardware uniquely.

Secured software table i 101a and secured software table $i+1$ 103a represent a part of the secured software application that is anchored to the hardware. The output from secured software table i 101a is used as challenge data to the hardware anchor 24c, which provides a wider output. In this example the response data from secured software table i 101a is 8 bits and the output of the hardware anchor 24c is 128 bits. The secured software table $i+1$ 103a of the secured software implementation is expanded with an inverse secured software table 102a, which transforms the wide output of the anchor 24c back to the expected input.

The inverse secured software table 102a and secured software table $i+1$ 103a are preferably integrated to obtain a higher level of obfuscation.

Each secured software application is personalized according to the coupled hardware circuit 24c that contains a unique hardware key K . It would also be possible to give a batch

of hardware circuits the same key. This action reduces the number of unique implementations.

With the hardware anchor 24c having an input of 8 bits and an output of 128 bits, the inverse table 102a has a table size of $2^{128} \times 8$.

It is possible to use CMAC to produce shorter outputs T, e.g. by using the 32 most significant bits instead of the full 128 bits. This would lead to a smaller inverse table 102a, i.e. an inverse table size of $2^{32} \times 8$ (≈ 4096 megabytes) in the above example. Even smaller inverse table sizes may be used with even shorter outputs. The following table illustrates the table size for different output sizes (in bits) and inputs of 8 bits.

Input	Output	Table size
8	10	$2^{10} \times 8 \approx 1$ kilobytes
8	12	$2^{12} \times 8 \approx 4$ kilobytes
8	14	$2^{14} \times 8 \approx 16$ kilobytes
8	16	$2^{16} \times 8 \approx 64$ kilobytes
8	32	$2^{32} \times 8 \approx 4096$ megabytes

It is possible to optimize the inverse table 102a. For an 8-bit input, there are only 2^8 possible (128-bit) output vectors. This means that the inverse table 102a only needs to contain those 128-bit vectors, together with their 8-bit original inputs. In this way, the inverse table size becomes $2^8 \times (128+8)$ bits, or about 4.25 kilobytes. The following table illustrates the table size for different input sizes (in bits) and outputs of 128 bits.

Input	Output	Table size
8	128	$2^8 \times (128+8)$ bits ≈ 4 kilobytes
10	128	$2^{10} \times (128+10)$ bits ≈ 17 kilobytes
12	128	$2^{12} \times (128+12)$ bits ≈ 70 kilobytes
14	128	$2^{14} \times (128+14)$ bits ≈ 284 kilobytes
16	128	$2^{16} \times (128+16)$ bits ≈ 1152 kilobytes

Fig.9 shows an exemplary embodiment of an obfuscated software application comprising a secured software part that is

anchored to a hardware circuit 24d which is used during runtime. Arrows indicate data flows.

An original secured software application consisting of a first part 101b and a second part 103b is split at an arbitrary point. At this point, the execution of the first part 101b of the original secured software application is halted, and 5 $b=128$ bits (in case of AES in the hardware anchor 24d) of its output are extracted and fed as challenge data to the hardware anchor 24d. The rest of the output of the original secured software application is kept as-is, which is shown as arrow 104. In order to invert the response data of the hardware anchor 24d, instead of a lookup table as shown in Fig.5 an inverse fixed-key secured software module 102b is used. After this process, the execution continues with the second part 103b of the original secured software application using the output of the first part 101b as reconstructed by the inverse fixed-key secured software module 102b combined with the rest of the internal state 104. 15

For increase security, preferably the transformation space between the first part 101b and the hardware anchor 24d differs from the transformation space between the inverse fixed-key secured software module 102b and the second part 103b. 20

Fig. 10 shows an alternative exemplary embodiment of a secured software application comprising a secured software part that is anchored to a hardware circuit 24d which is used during runtime. Arrows indicate data flows. 25

An original secured software application consisting of a first secured software part 101b and a second secured software part 103b is split at an arbitrary point. At this point, the execution of the first secured software part 101b of the original secured software application is halted, and its state is extracted and input as challenge data to the hardware anchor 24d. The state is further input to a software CMAC secured software module 105. In order to invert the response data of the hardware anchor 24d, a property-dependent transform (PDT) module 102c or any other known comparison mechanism is used, which compares the output of the CMAC secured software module 105 with the response data of the hardware anchor 25d. After this process, the execution continues in the second part 103b of the 35

original secured software application using the state of the first part 101b as received from the PDT transform module 102c.

The advantage of the example of Fig.10 is that any size of state vector can be handled as input. To do this, the whole CMAC construction of Fig.8 is incorporated into the CMAC secured software module 105, which repeatedly calls a secured software encryption module just like the hardware circuit 24d.

In the end, both the CMAC secured software module 105 and the hardware circuit 24d have computed the tag T. In order to compare the result, the property-dependent transform (PDT) or other comparison mechanism is used.

It is to be understood that the state that is fed as challenge data to the hardware circuit 24d can be in a transformed form. There is no need for the hardware to learn the clear (non-transformed) values.

Fig. 11 shows an exemplary embodiment enabling a secure transmission or storage of a (secured) software application in encrypted form, wherein the hardware circuit 24e is used to compute the software-application-unique decryption key for decrypting the encrypted part of the software application.

The software application comprises a loader code part 101c and an encrypted software part 103c and is created to be used on a particular device with a hardware circuit 24e. The software application is e.g. downloaded or bought from an app store.

A part of or the complete loader code 101c is input as challenge data to the hardware anchor 24d. The resulting device-unique response data is used as the decryption key for decrypting the encrypted software part 103c. When an AES coprocessor is used as shown in the previous exemplary embodiments, the decryption key will be a 128-bit value.

Fig. 12 shows an alternative exemplary embodiment enabling a secure transmission or storage of a software application in encrypted form, wherein the hardware circuit 24e is used to compute the software-application-unique decryption key for decrypting the encrypted part of the software application.

The software application comprises a loader code part 106 and an encrypted software part 103c and is created to be

used on a particular device with a hardware circuit 24e. A random data block 107 is part of the encrypted software part 103c, making the encrypted software part 103c unique.

5 A part of or the complete encrypted software part 103c is input to the hardware circuit 24d. When an AES coprocessor is used as shown in the previous exemplary embodiments, the decryption key will be a 128-bit value.

10 The random data block 107 in the encrypted software part 103c can be created by the provider of the encrypted software application as follows. Initially the encryption key is picked at random, and then it is backtracked what the (ciphertext) value of the random data block 107 should be.

15 Fig.13 shows an example of a calculation of the random data block 107 by a provider. As example, assume that a second block C_2 of the software application is to be used as random data block 107 to insert an arbitrary ciphertext block and pick the key T. It is to be understood that any and multiple blocks may be used as random data block 107.

20 The first block C_1 is processed similar to block M_1 as shown in Fig.8. For the other blocks $C_2 \dots C_1$, the calculation is reversed compared to Fig.8: first the key T (with which the software is encrypted) is decrypted with the hardware anchor key K , which is then added to the key-dependent value V_1 and the last block of the encrypted software. The result is decrypted again, 25 and added to the previous block of the encrypted software, and so on. In this way, the two calculations meet and are added up to produce the "missing" block C_2 . The thus calculated block C_2 is inserted in the encrypted software part 103c as random data block 107.

30 The correct decryption key can be derived by the end-user device with the hardware circuit 24d that is configured with the hardware anchor key K .

35 It is to be understood that runtime protection such as e.g. shown in Fig.9 and Fig.10 may be applied in conjunction with the decryption protection such as e.g. shown in Fig.11 and Fig.12.

In the exemplary embodiments shown Figs. 5, 9 and 10 the hardware circuit 24c,24d and inverse module 102a,102b,102c are used in between two parts of the software application. It is

to be understood that the hardware circuit and inverse module may be used at the very beginning or at the very end of the software application. If located at the very beginning, e.g. a first input to the software application is used as challenge data. If located at the very end, e.g. a final output of the software application is used as challenge data.

One embodiment of the invention may be implemented as a program product for use with a computer system. The program(s) of the program product define functions of the embodiments (including the methods described herein) and can be contained on a variety of non-transitory computer-readable storage media. Illustrative computer-readable storage media include, but are not limited to: (i) non-writable storage media (e.g., read-only memory devices within a computer such as CD-ROM disks readable by a CD-ROM drive, ROM chips or any type of solid-state non-volatile semiconductor memory) on which information is permanently stored; and (ii) writable storage media (e.g., flash memory, floppy disks within a diskette drive or hard-disk drive or any type of solid-state random-access semiconductor memory) on which alterable information is stored.

CLAIMS

1. A computer-implemented method for enabling a software application to be executed on a hardware device in dependence of a hardware circuit in the hardware device, the method comprising:

5 inputting challenge data originating from the software application to the hardware circuit of the hardware device, wherein the hardware circuit is configured to perform a deterministic function;

10 generating response data using the function with the challenge data as input to the function; and

using the response data to manipulate at least a part of the software application to thereby enable the software application to be executed.

15 2. The method according to claim 1, wherein the function is unique to one or more hardware circuits

20 3. The method according to claim 1 or claim 2, wherein the function is a cryptographic function.

25 4. The method according to claim 3, wherein the cryptographic function uses a key that is one of a key preconfigured in a memory of the hardware circuit and a key derived from a unique key preconfigured in a memory of the hardware circuit.

30 5. The method according to claim 4, wherein the cryptographic function uses a key derived from a key loading message received from an external source.

6. The method according to claim 5, wherein the key loading mechanism is unique to the hardware device.

35 7. The method according to any one of the claims 1-6, wherein the software application comprises a first secured software part, a second secured software part and an inverse module configured to perform an inverse function to inverse the

function of the hardware circuit, wherein the challenge data comprises at least a part of runtime data of the software application at the end of the first secured software part when being executed in a processing unit, and wherein the using of the response data comprises:

- 5 inputting the response data to the inverse function in the inverse module to thereby obtain an inverted response data, wherein the inverted response data is equal to the challenge data if the inverse function in the inverse module matched the function in the hardware circuit; and
- 10 providing the inverted response data to the second secured software part for further execution of the software application.

8. The method according to claim 7, wherein the first secured software part comprises a first part of a cryptographic function, wherein the second secured software part comprises a second part of the cryptographic function, and wherein the runtime data represents an intermediate result of the cryptographic function as output by the first part of the cryptographic function.

9. The method according to claim 7, wherein the function in the hardware circuit comprises a fixed-key cryptographic function configured to use a fixed key, and wherein the inverse function comprises an inverse fixed-key cryptographic function configured to use the fixed key.

10. The method according to claim 7, wherein the software application further comprises a secured software module configured to perform a further function identical to the function in the hardware circuit, the method further comprising:

30 inputting the challenge data to the secured software module; generating further response data from the further function using the challenge data as input to the further function; and

35 inputting the further response data to the inverse function in the inverse module to thereby obtain a further inverted response data, wherein the further inverted response data is equal to the challenge data if the inverse function in the

inverse module matched the further function in the secured software module,
and wherein the inverse function comprises a comparison function to compare the response data with the further response data.

5

11. The method according to any one of the claims 7-10, wherein the order of the hardware circuit and the inverse module is reversed, wherein the hardware circuit is configured to perform the inverse function, and wherein the inverse module is configured to perform the deterministic function.

10

12. The method according to any one of the claims 1-6, wherein the software application is an encrypted software application, wherein the challenge data comprises as least a part of a software image of the software application, and wherein the using of the response data comprises:

15

using the response data as a decryption key to decrypt at least a part of the encrypted software application.

13. A computer-implemented method for adding a random data block to an encrypted software application, the method comprising:

20

dividing a software image of the encrypted software application into equal length blocks;

25

determining a replacement block being one of the blocks to be replaced by the random data block;

applying a block cipher-based message authentication code (CMAC) function to the blocks until the replacement block;

30

applying a reversed block cipher-based message authentication code (CMAC) function to the blocks starting from the last block until the block after the replacement block, wherein tag T equals the encryption key used to encrypt the encrypted software, wherein the tag T is decrypted using CMAC key K , wherein the decrypted tag T is added to CMAC key

35

dependent value V_1 and the last block to obtain an intermediate result, wherein the intermediate result is decrypted using the CMAC key K , wherein the decrypted intermediate result is added to the preceding block to obtain a further intermediate result

and repeating the decrypting and adding of further intermediate results until the replacement block;

adding the last result from the block cipher-based message authentication code (CMAC) function to the last result of the reverse block cipher-based message authentication code (CMAC) function to obtain the random data block; and

replacing the replacement block with the random data block, wherein the CMAC key K corresponds to a further CMAC key K in a hardware circuit of an hardware device.

10

14. A hardware circuit for enabling a software application to be executed on a hardware device comprising the hardware circuit and in dependence of the hardware circuit, wherein the hardware circuit is configured to perform a deterministic function that uses challenge data originating from the software application as input to the function to generate response data for manipulating at least a part of the software application to thereby enable the software application to be executed.

15. The hardware circuit according to claim 14, wherein the function is unique to one or more hardware circuits of respective hardware devices to enable the software application to be executed on the respective hardware devices.

16. The hardware circuit according to claim 14 or claim 15, wherein the function is a cryptographic function using a key that is one of

a key preconfigured in a memory of the hardware circuit, a key derived from a unique key preconfigured in a memory of the hardware circuit, and

a key derived from a key loading message received from an external source.

17. The hardware circuit according to any one of the claims 14-16, wherein the hardware circuit is embedded in one of a CPU, a GPU and programmable I/O peripheral.

18. A hardware device comprising a hardware circuit according to any one of the claims 14-17.

19. The hardware device according to claim 18, wherein the hardware device is one of a digital TV receiver, a PC, a tablet PC, a smart phone, an Internet (cloud) server and a graphics
5 card.

20. A software application which, when being executed by a processor, is adapted to manipulate at least a part of the software application to thereby enable the software application
10 to be executed on a hardware device in dependence of a hardware circuit in the hardware device, by using response data that is generated using a deterministic function in the hardware circuit that uses challenge data as input to the function, wherein the challenge data originates from the software application.

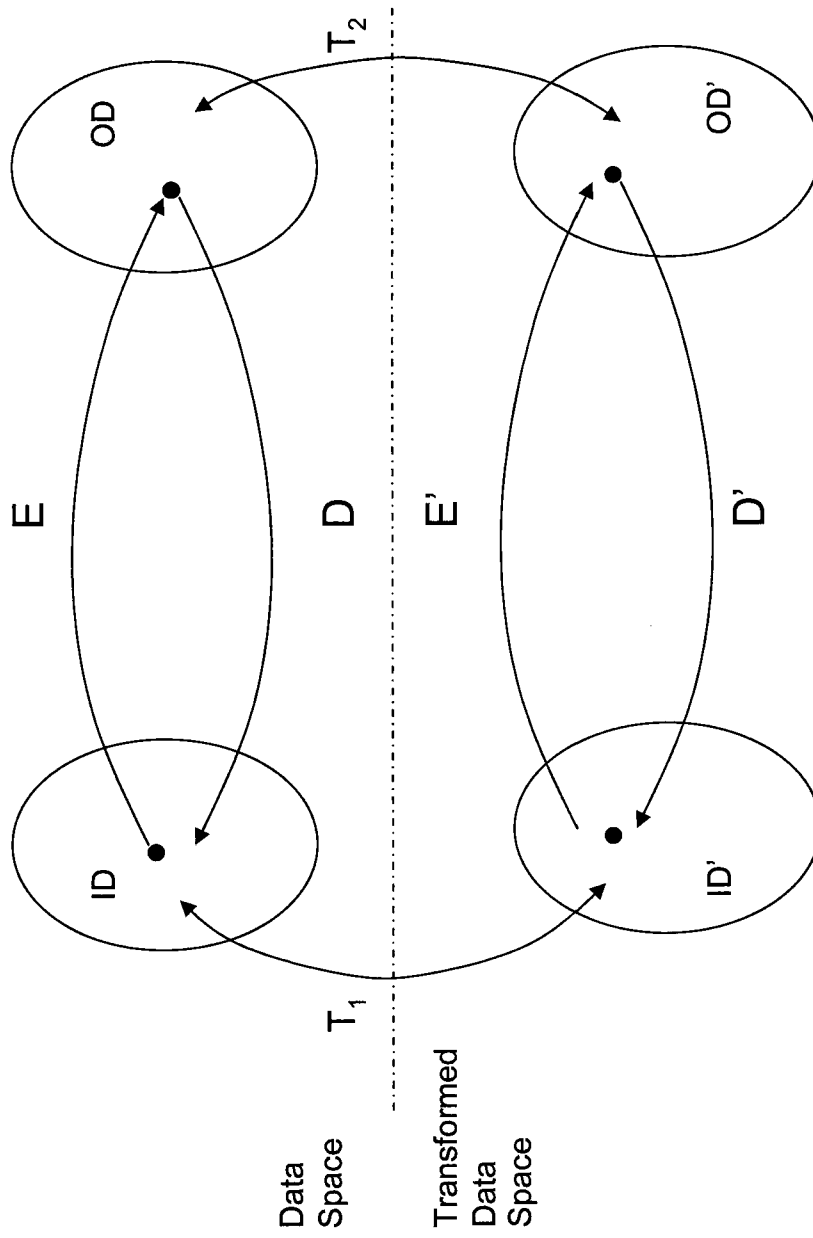


Fig.1
(prior art)

2/8

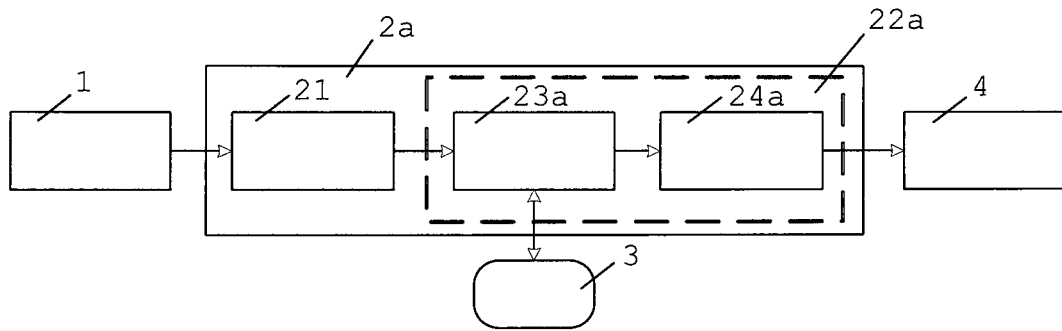


Fig. 2
(prior art)

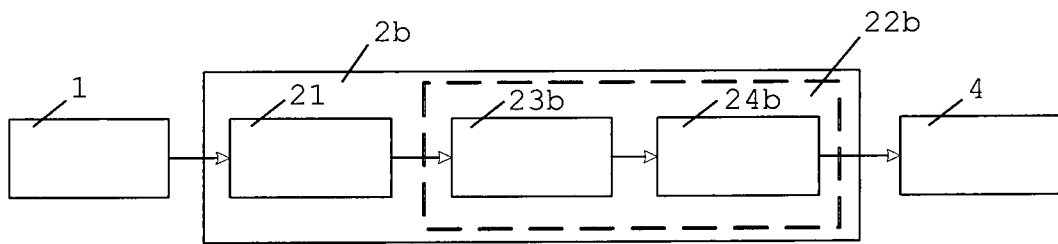


Fig. 3
(prior art)

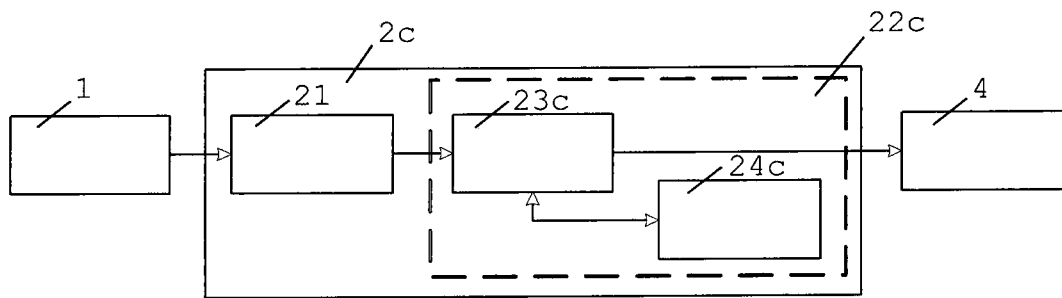


Fig. 4

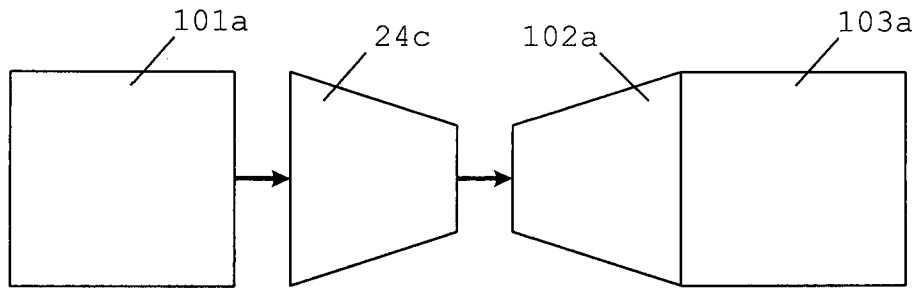


Fig. 5

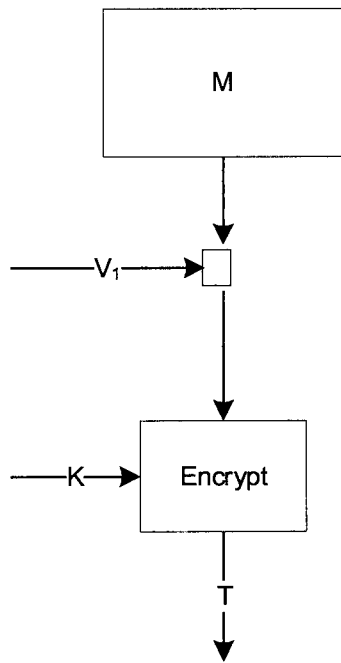


Fig. 6

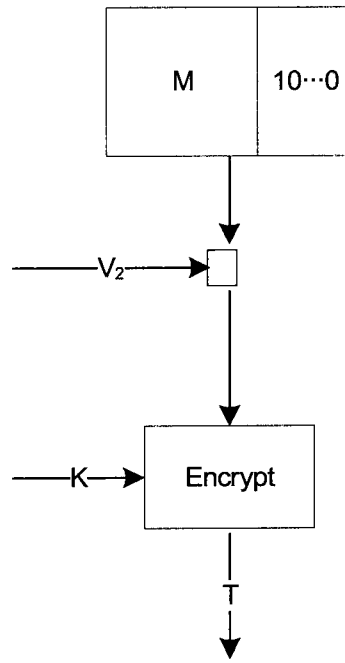


Fig. 7

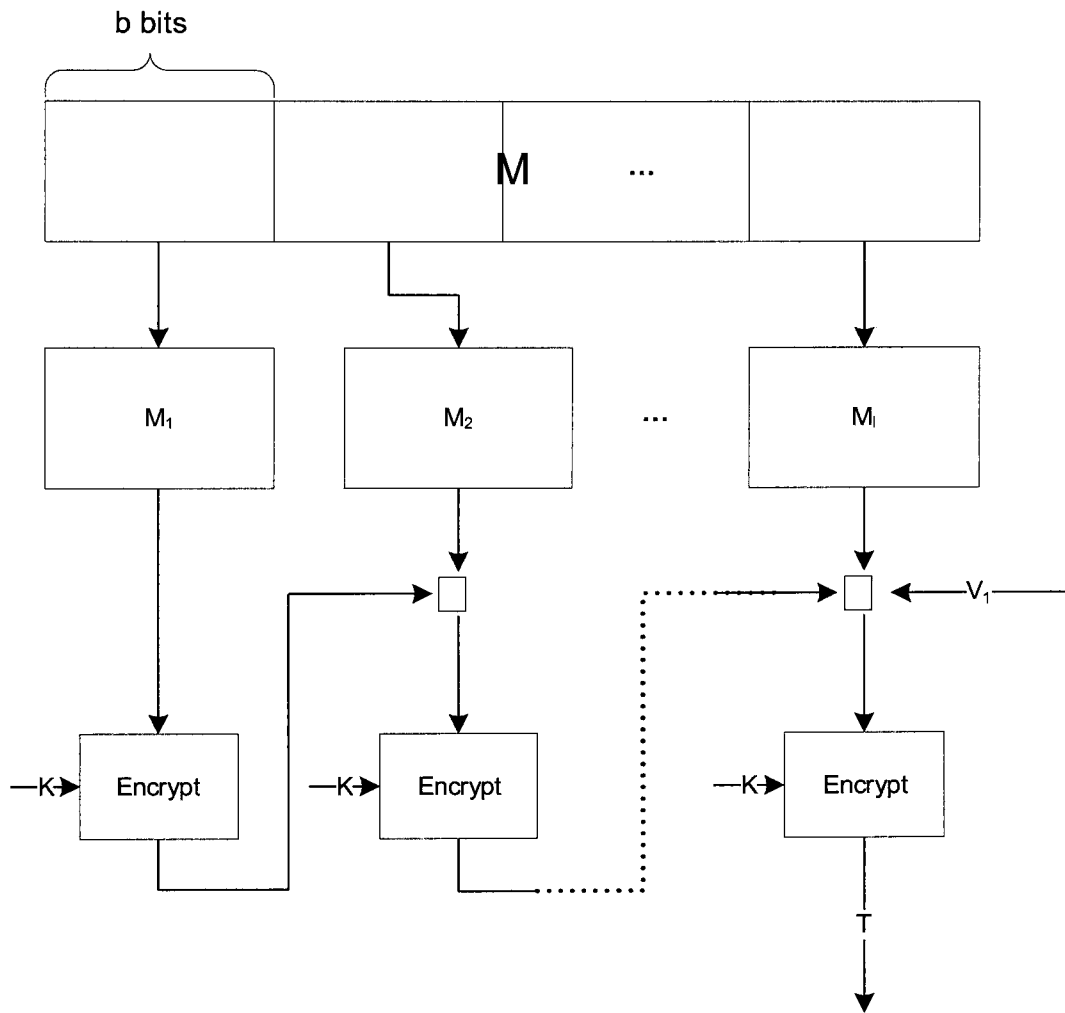


Fig. 8

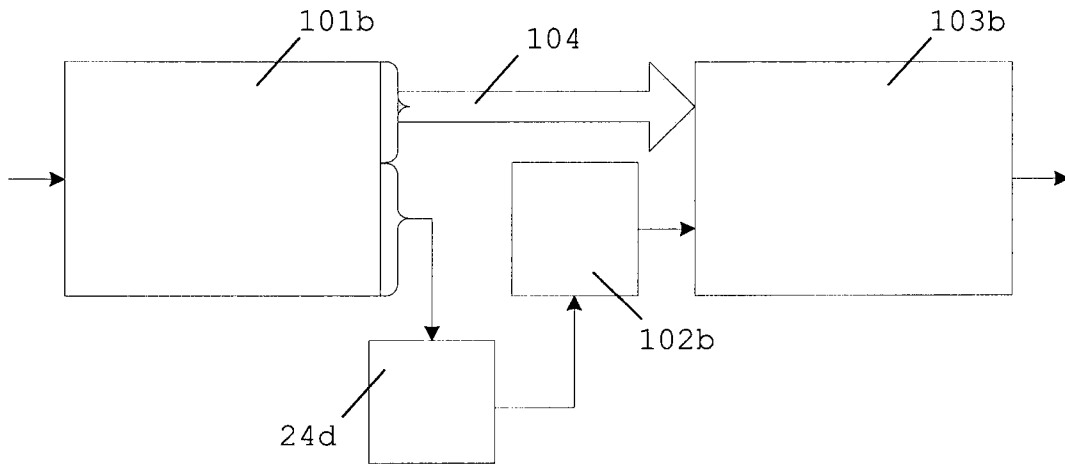


Fig. 9

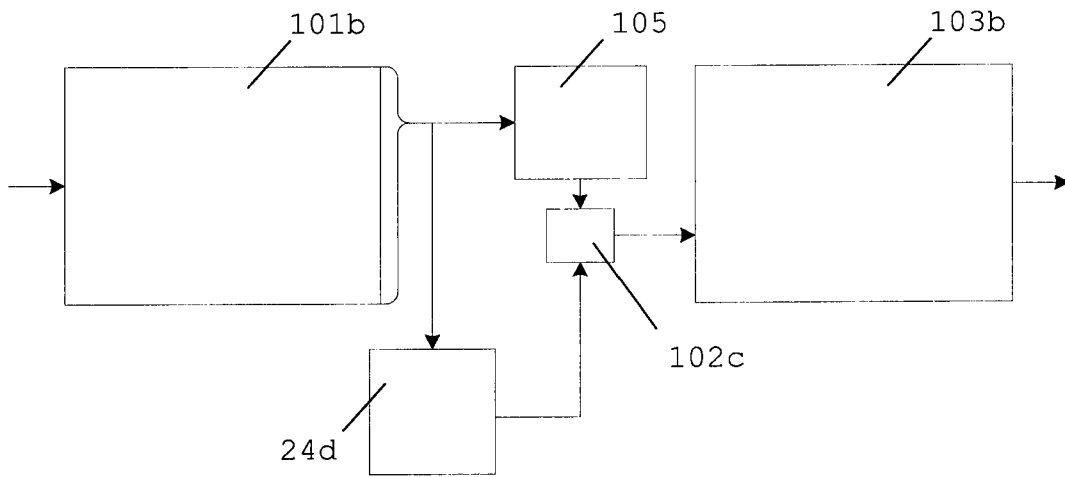


Fig. 10

6/8

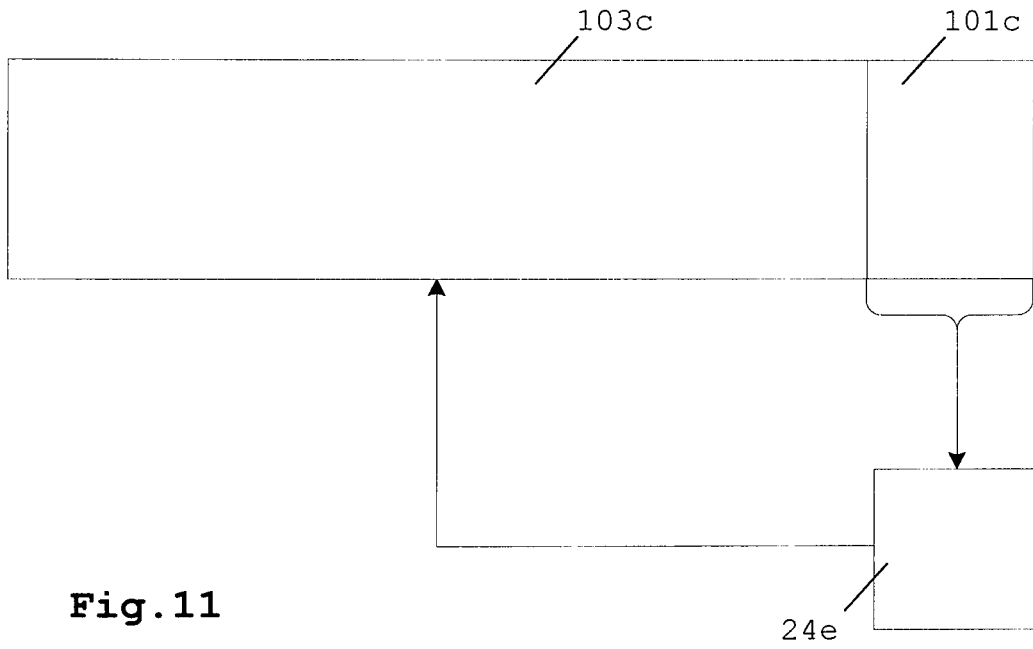


Fig. 11

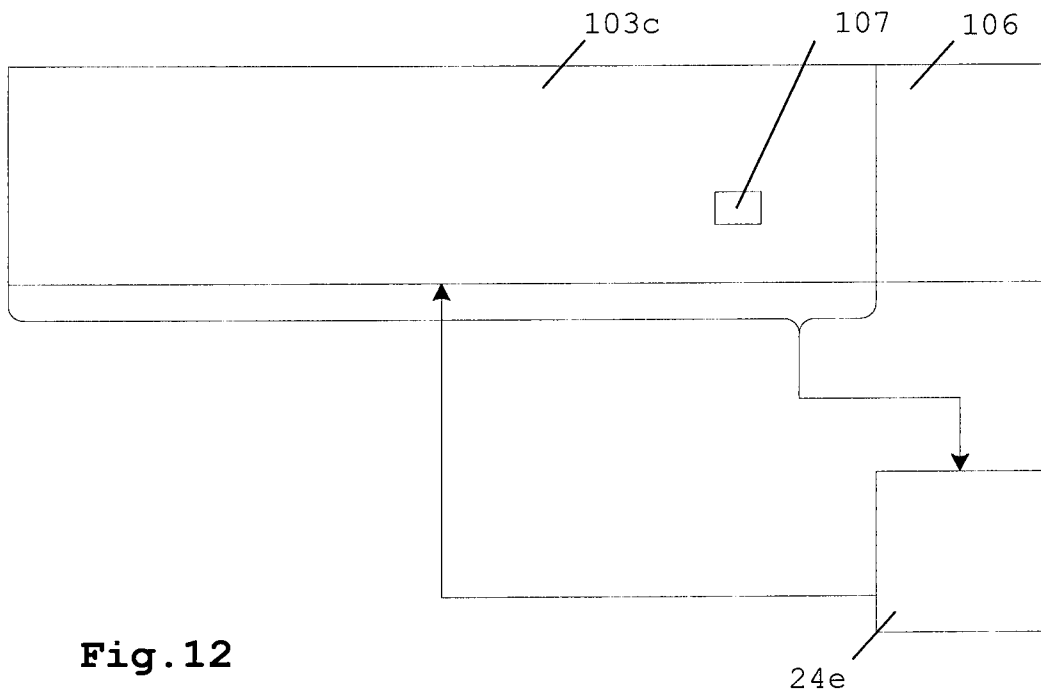


Fig. 12

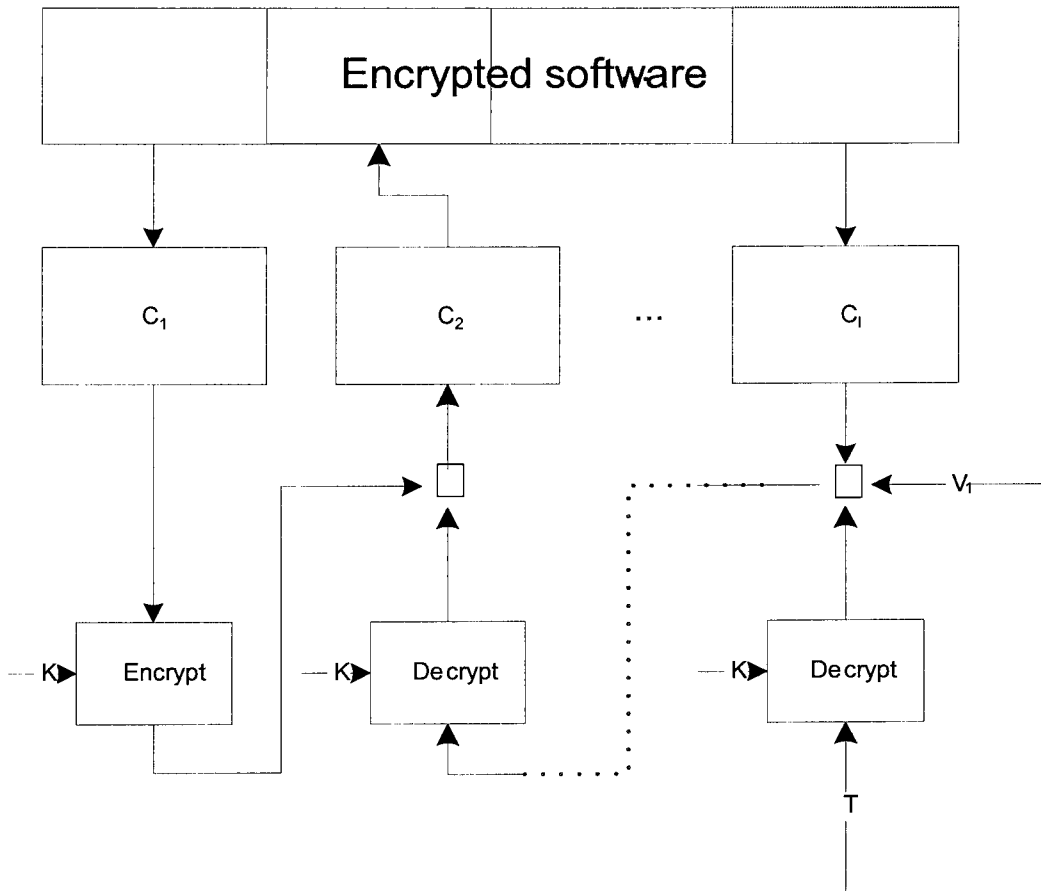


Fig. 13

8/8

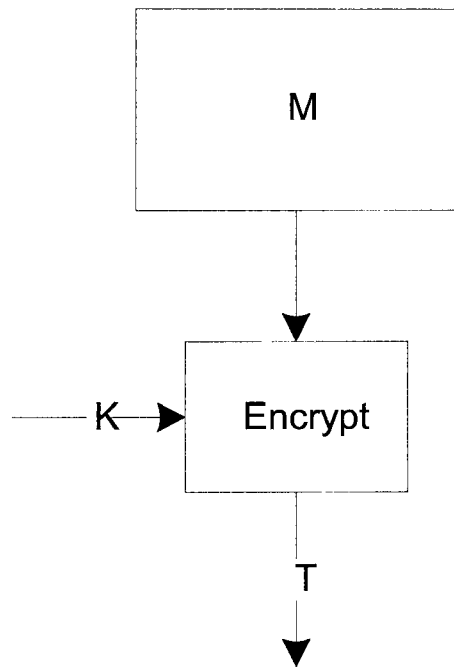


Fig.14

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/054826A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00
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)
G06F

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

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

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2005/064433 A1 (KONINKL PHILIPS ELECTRONICS NV [NL]; GIDALOV NIKOLCO [NL]) 14 July 2005 (2005-07-14)	1-6, 12-20
Y	page 1, line 2 - line 4 page 2, line 22 - line 25 page 8, line 6 - line 24 page 9, line 5 - line 10 page 9, line 30 - line 31 page 10, line 25 - page 11, line 5 page 11, line 15 - page 12, line 4 figures 4,5	7-11
X	----- US 6 480 959 B1 (GRANGER MARK J [US] ET AL) 12 November 2002 (2002-11-12)	1-6, 13-20
Y	column 4, line 1 - line 62; figures 1A, 1B	7-11
A	column 5, line 26 - line 36 column 6, line 14 - line 65 column 9, line 61 - column 11, line 21 -----	12
	-/--	

 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

1 June 2012

Date of mailing of the international search report

18/06/2012

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

Vinck, Bart

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2012/054826

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>US 5 473 692 A (DAVIS DEREK L [US]) 5 December 1995 (1995-12-05) column 1, line 59 - column 2, line 7 column 2, line 58 - column 3, line 31 column 9, line 2 - line 31; figure 7C</p> <p style="text-align: center;">-----</p>	5,6
A	<p>JH SONG R POOVENDRAN UNIVERSITY OF WASHINGTON J LEE SAMSUNG ELECTRONICS T IWATA NAGOYA UNIVERSITY: "The AES-CMAC Algorithm; rfc4493.txt", 20060601, 1 June 2006 (2006-06-01), XP015054998, ISSN: 0000-0003 the whole document</p> <p style="text-align: center;">-----</p>	13
A	<p>US 2008/263366 A1 (G MAURUTHI [IN]) 23 October 2008 (2008-10-23) paragraph [0062] - paragraph [0070]; figures 10,11</p> <p style="text-align: center;">-----</p>	1-12, 14-20
A	<p>US 2007/113103 A1 (YE HANG J [CN] ET AL) 17 May 2007 (2007-05-17) abstract claim 1 paragraph [0007] - paragraph [0009] paragraph [0012] - paragraph [0022]</p> <p style="text-align: center;">-----</p>	1-12, 14-20

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2012/054826

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.:

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.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

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

1. claims: 1-12, 14-20

how to limit the execution of a software application to a particular hardware device, in an alternative manner

2. claim: 13

how to protect a long-term cryptographic key against unauthorised disclosure through cryptanalysis

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2012/054826

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2005064433	A1	14-07-2005	
		CN 1898623 A	17-01-2007
		EP 1700181 A1	13-09-2006
		JP 2007515723 A	14-06-2007
		KR 20060127007 A	11-12-2006
		US 2007198857 A1	23-08-2007
		WO 2005064433 A1	14-07-2005

US 6480959	B1	12-11-2002	NONE

US 5473692	A	05-12-1995	
		AU 3583295 A	27-03-1996
		EP 0780039 A1	25-06-1997
		JP 4294728 B2	15-07-2009
		JP H10507324 A	14-07-1998
		RU 2147790 C1	20-04-2000
		US 5473692 A	05-12-1995
		US 5568552 A	22-10-1996
		WO 9608092 A1	14-03-1996

US 2008263366	A1	23-10-2008	NONE

US 2007113103	A1	17-05-2007	
		CN 1904793 A	31-01-2007
		US 2007113103 A1	17-05-2007
		US 2009019290 A1	15-01-2009
