



(51) International Patent Classification:
G06F 21/00 (2006.01) **G06K 19/073** (2006.01)

(21) International Application Number:
PCT/IB2009/055724

(22) International Filing Date:
13 December 2009 (13.12.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
199272 10 June 2009 (10.06.2009) IL

(71) Applicant (for all designated States except US): **NDS LIMITED** [GB/GB]; One London Road, Staines Middlesex TW18 4EX (GB).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **HALBERSTADT, Meir** [IL/IL]; P.O.Box 389 D.N. Shimshon, 99785 Nof Ayalon (IL).

(74) Agents: **ZVIEL, David** et al.; Director - Intellectual Property, NDS Technologies Israel Limited, 5 Shlomo Halevi Street, 97770 Jerusalem (IL).

(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, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (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, 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: PROTECTION OF SECRET VALUE USING HARDWARE INSTABILITY

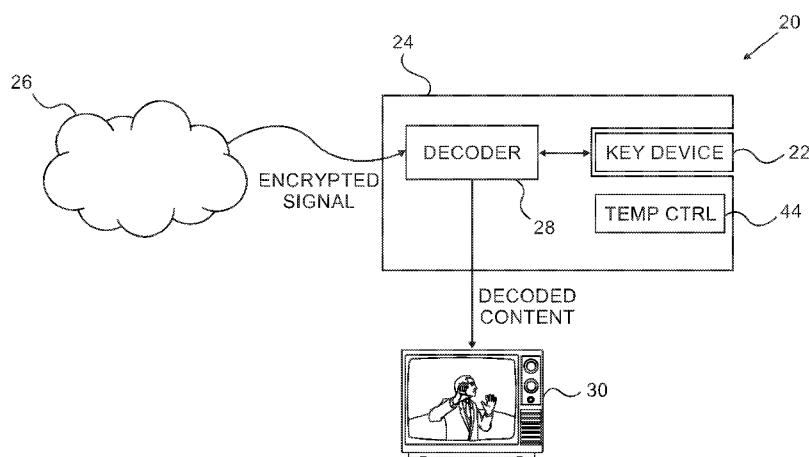


FIG. 1

(57) Abstract: A method for data security, comprising providing an electronic circuit, which has a first, stable operating mode under a first operating condition and a second, unstable operating mode under a second operating condition, different from the first operating condition, and which is configured to output a secret value in the first operating mode; maintaining the electronic circuit initially in the second operating condition; transferring the electronic circuit to the first operating condition and, while in the first operating condition, reading out the secret value; and returning the electronic circuit to the second operating condition after reading out the secret value.

PROTECTION OF SECRET VALUE USING HARDWARE INSTABILITY**FIELD OF THE INVENTION**

The present invention relates generally to electronic circuits, and specifically to circuits that are used to store secrets.

BACKGROUND OF THE INVENTION

A flip-flop is an electronic circuit that has two stable states and thus is capable of serving as one bit of memory. (The term "flip-flop" is used, in the context of the present patent application and in the claims, to denote both clocked flip-flops and transparent flip-flops, commonly known as latches.) Violation of the prescribed operating conditions of a flip-flop can cause metastability, in which the logical state of the flip-flop oscillates unpredictably before settling in a random stable state. For example, metastability may occur if the data input of a clocked flip-flop changes during the prescribed setup time period before the triggering clock transition and/or the prescribed hold time period following a given clock transition.

Generally, digital logic circuits are designed to avoid metastable conditions. In some applications, however, a circuit may be designed intentionally for metastability. For example, U.S. Patent 7,302,458, whose disclosure is incorporated herein by reference, describes a random number generator using metastable elements that are synchronized by a set of flip-flops. The output of the stabilizing flip-flops is compared and used to generate counter events.

P-353-WO-tobefiled.doc P-353 SK 10December2009

SUMMARY OF THE INVENTION

Embodiments of the present invention that are described hereinbelow use circuit instabilities in a novel way to protect a secret value that is held or generated by the circuit.

There is therefore provided, in accordance with an embodiment of the present invention, a method for data security that includes providing an electronic circuit, which has a first, stable operating mode under a first operating condition and a second, unstable operating mode under a second operating condition, different from the first operating condition, and which is configured to output a secret value in the first operating mode. The electronic circuit is maintained initially in the second operating condition. The electronic circuit is transferred to the first operating condition and, while in the first operating condition, the secret value is read out. The electronic circuit is returned to the second operating condition after reading out the secret value.

In one embodiment, the first and second operating conditions correspond to application of different, respective, first and second operating voltages to the electronic circuit, and transferring the electronic circuit includes switching from the second to the first operating voltage. In another embodiment, the first and second operating conditions correspond to application of clock pulses at different, respective, first and second clock rates to the electronic circuit, and transferring the electronic circuit includes switching from the second to the first clock rate. Additionally or alternatively the first and second operating conditions correspond to

P-353-WO-tobefiled.doc P-353 SK 10December2009

different, respective, first and second operating temperatures of the electronic circuit, and transferring the electronic circuit includes changing from the second to the first operating temperature.

In some embodiments, transferring the electronic circuit includes receiving a control signal requesting the secret value, and switching momentarily from the second to the first operating condition in response to the control signal.

In a disclosed embodiment, the electronic circuit includes a flip-flop, which is metastable in the second operating mode and stable in the first operating mode.

There is also provided, in accordance with an embodiment of the present invention, a data security device, including an electronic circuit, which has a first, stable operating mode under a first operating condition and a second, unstable operating mode under a second operating condition, different from the first operating condition, and which is configured to output a secret value in the first operating mode. Means for controlling the operating condition of the electronic circuit maintain the electronic circuit initially in the second operating condition, transfer the electronic circuit to the first operating condition so as to cause the electronic circuit to output the secret value, and return the electronic circuit to the second operating condition after the secret value has been output.

The present invention will be more fully understood from the following detailed description of the embodiments thereof, taken together with the drawings in which:

P-353-WO-tobefiled.doc P-353 SK 10December2009

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram that schematically illustrates a system for data security, in accordance with an embodiment of the present invention; and

Fig. 2 is a block diagram that schematically shows details of data protection device, in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS

Secret values, such as keys used in encryption and decryption functions, are commonly stored in electronic memory. There are means known in the art for preventing unauthorized readout of secret values while the memory is intact, but hackers have become increasingly sophisticated in their ability to overcome these means, including by opening up and physically reading out the secret contents of memory chips.

Embodiments of the present invention use variable physical conditions and circuit instabilities to conceal a secret value in an electronic circuit. The circuit in these embodiments is designed to have a stable operating mode under certain operating conditions but to be unstable under other operating conditions. The correct secret value is generated and output by logic in the circuit only in the stable operating mode. Typically, ambient conditions of the circuit result in unstable operation, so that the secret value is unavailable. The operating condition of the circuit is transferred to the stable mode only when needed in order to read out the secret value. The time during which the circuit operates stably may be very short - as little as a single clock cycle, and the circuit may be returned to the ambient conditions and unstable operation immediately thereafter.

P-353-WO-tobefiled.doc P-353 SK 10December2009

Thus, the secret value cannot be found by opening the circuit, nor can it be extracted in normal, ambient operation of the circuit. Even reverse-engineering analysis of the circuit will still fail to reveal the secret, as long as the analysis does not take the detailed effects of the operating conditions of the circuit into account. The variable operating conditions that may be used in hiding the secret in the circuit may comprise the operating voltage, clock rate, or temperature of the circuit, for example, as well as other factors, or a combination of these factors.

Fig. 1 is a block diagram that schematically illustrates a system 20 for data security, in accordance with an embodiment of the present invention. System 20 uses a data protection device 22 to provide a secret key for use by a computing device 24 in decoding encrypted signals received from a network 26. For example, device 24 may comprise a media player, such as a set-top box, which receives digital video programs over a wireless or terrestrial network. In this sort of application, the programs are encrypted to prevent unauthorized viewing or copying, and device 22 may comprise a smart card, USB key, or other plug-in unit that is distributed to subscribers to enable decryption and viewing of the programs on a video display 30.

Alternatively, device 24 may comprise substantially any other type of computer or other electronic device that uses secret values for decryption, encryption, access control, or any other suitable application. Data protection device 22 may be made as a plug-in unit, as shown in Fig. 1, or it may alternatively be an integral part of the computing device that it enables.

P-353-WO-tobefiled.doc P-353 SK 10December2009

Returning to the application shown in Fig. 1, encrypted signals from network 26 are received by a decoder 28 in device 24. Decoder 28 reads a secret key value from device 22 and uses this value in decrypting the signals. The key value may be fixed, or it may change from time to time, as is known in the art. As noted above, device 22 is controlled to output the correct key value only under certain conditions that cause device 22 to operate in a stable mode. The appropriate conditions may be invoked momentarily, for example, in response to a trigger signal from decoder 28, indicating that the key value is needed.

Additionally or alternatively, the appropriate conditions for stable operation of device 22 may be provided by the operating environment within device 24, while such conditions generally do not prevail in the ambient environment outside device 24. For example, device 24 may comprise a temperature controller 44, which holds device 22 at a specific design temperature, at which device 22 operates in the stable mode. Typically (although not necessarily) the design temperature for stable operation is cooler than the ambient temperature. Outside a narrow temperature window around the design temperature, device 22 may operate unstably. Therefore, a hacker who attempts to extract a secret value from device 22 at a temperature outside the window will be unable to do so.

Fig. 2 is a block diagram that schematically shows details of data protection device 22, in accordance with an embodiment of the present invention. The circuit elements shown in this figure may be fabricated, for example, as components of an application-specific

P-353-WO-tobefiled.doc P-353 SK 10December2009

integrated circuit (ASIC), comprising an array of logic gates with suitable interconnections. Alternatively, any other suitable type of integrated circuit may be used for this purpose, such as a full-custom device or a field-programmable gate array (FPGA).

An input generator 32 produces a starting value for input to a combinatorial logic network 34. The input generator may simply comprise a set of registers, which hold fixed values, or it may be configured to generate a variable output, in either a deterministic fashion (such as a sequence of constants or a one-time password function) or a random fashion. For example, input generator 32 may comprise a random number generator or a physical unclonable function (PUF) circuit. Network 34 may comprise a complex design, with many gates, in order to make reverse engineering more difficult. Additionally or alternatively, the network may comprise long conductors, which contribute to the instability of its operation.

Logic network 34 outputs a secret value to an output register 36, comprising an array of flip-flops 38. This secret value is read out of device 22 by decoder 28 at the appropriate time. A power supply 42 supplies operating voltage to elements of device 22, including particularly logic network 34 and flip-flops 38. The timing of the flip-flops (as well as of the logic network) is controlled by a clock generator 40. Either the power supply or the clock generator, or both, as well as the temperature of the logic network, may be used to switch the operating condition of device 22 between unstable and stable operating modes, as is explained further hereinbelow.

P-353-WO-tobefiled.doc P-353 SK 10December2009

In embodiments of the present invention, logic network 34, including its connections to flip-flops 38, is designed intentionally with marginal timing. This timing may be determined at the "place and route" step of the design of network 34, using electronic design automation (EDA) tools that are known in the art. The actual timing depends on the operating conditions of the circuits and typically varies with operating voltage and temperature, in a way that EDA tools are able to model. Thus, the designer of logic network 34 may, for example, choose the lengths of the conductors in the network so that at a certain operating voltage, such as 1.8 volts, the logic network outputs the secret value for a period that satisfies the setup time and hold time constraints of flip-flops 38, but does not satisfy these constraints at other operating voltages, such as 3.3 volts. Thus, register 36 will contain the correct secret value only when power supply 42 is set to 1.8 volts, whereas at 3.3 volts, at least some of the flip-flops will contain a random value due to their metastable condition.

Typically, decoder 28 provides a control input to device 22 when it is ready to receive a secret value. Power supply 42 may normally operate at 3.3 volts, so that register 36 contains a random value. In response to the control input, however, power supply 42 may switch to supplying 1.8 volts, whereupon the correct secret value will be loaded into the register for readout by the decoder. The power supply may, for example, comprise a dual-output regulator with a switch, which switches the voltage supplied to all or part of the logic network and flip-flops on command. Alternatively, a voltage divider or other switched load, or any other suitable means known

P-353-WO-tobefiled.doc P-353 SK 10December2009

in the art, may be used for this purpose. If only a part of the logic network operates at the lower voltage, buffering may be needed in order to separate the high- and low-voltage parts of the network, so as to prevent DC current flow through the network, for example. The voltage may be switched momentarily, only for as long as is needed to read out the secret value - possibly for just a single clock cycle, in order to make it harder for an unauthorized party to discover the value.

As another alternative, the rate of clock generator 40 may be switched briefly from one frequency at which flip-flops 38 are metastable, to another frequency at which they stably provide the correct secret value.

The voltage or clock switching described above may be applied to all of logic network 34, or it may alternatively be applied only to certain components, particularly flip-flops 38 and possibly other associated components.

In another embodiment, as noted above, network 34 may be designed so that at ambient operating temperatures, flip-flops 38 are metastable, and become stable only when device is held at the appropriate design temperature. (This approach, however, is less suitable for applications in which it is desired that the secret value appear only momentarily on the output of device 22.)

Thus, to summarize, power supply 42, clock generator 40 and temperature controller 44 may serve, individually or in combination, as means for controlling the operating condition of the electronic circuits in device 22. Other means will be apparent to those skilled in the art upon

P-353-WO-tobefiled.doc P-353 SK 10December2009

reading the present patent application and are considered to be within the scope of the present invention.

It will thus be appreciated that the embodiments described above are cited by way of example, and that the present invention is not limited to what has been particularly shown and described hereinabove. Rather, the scope of the present invention includes both combinations and subcombinations of the various features described hereinabove, as well as variations and modifications thereof which would occur to persons skilled in the art upon reading the foregoing description and which are not disclosed in the prior art.

P-353-WO-tobefiled.doc P-353 SK 10December2009

CLAIMS

1. A method for data security, comprising:
providing an electronic circuit, which has a first, stable operating mode under a first operating condition and a second, unstable operating mode under a second operating condition, different from the first operating condition, and which is configured to output a secret value in the first operating mode;
maintaining the electronic circuit initially in the second operating condition;
transferring the electronic circuit to the first operating condition and, while in the first operating condition, reading out the secret value; and
returning the electronic circuit to the second operating condition after reading out the secret value.
2. The method according to claim 1, wherein the first and second operating conditions correspond to application of different, respective, first and second operating voltages to the electronic circuit, and wherein transferring the electronic circuit comprises switching from the second to the first operating voltage.
3. The method according to claim 1, wherein the first and second operating conditions correspond to application of clock pulses at different, respective, first and second clock rates to the electronic circuit, and wherein transferring the electronic circuit comprises switching from the second to the first clock rate.
4. The method according to claim 1, wherein the first and second operating conditions correspond to different, respective, first and second operating temperatures of the electronic circuit, and wherein transferring the

P-353-WO-tobefiled.doc P-353 SK 10December2009

electronic circuit comprises changing from the second to the first operating temperature.

5. The method according to claim 1, wherein transferring the electronic circuit comprises receiving a control signal requesting the secret value, and switching momentarily from the second to the first operating condition in response to the control signal.

6. The method according to claim 1, wherein the electronic circuit comprises a flip-flop, which is metastable in the second operating mode and stable in the first operating mode.

7. A data security device, comprising:

an electronic circuit, which has a first, stable operating mode under a first operating condition and a second, unstable operating mode under a second operating condition, different from the first operating condition, and which is configured to output a secret value in the first operating mode; and

means for controlling the operating condition of the electronic circuit, so as to maintain the electronic circuit initially in the second operating condition, to transfer the electronic circuit to the first operating condition so as to cause the electronic circuit to output the secret value, and to return the electronic circuit to the second operating condition after the secret value has been output.

8. The device according to claim 7, wherein the first and second operating conditions correspond to application of different, respective, first and second operating voltages to the electronic circuit, and wherein the means for controlling the operating condition comprise a power

P-353-WO-tobefiled.doc P-353 SK 10December2009

supply, which is configured to switch from the second to the first operating voltage.

9. The device according to claim 7, wherein the first and second operating conditions correspond to application of clock pulses at different, respective, first and second clock rates to the electronic circuit, and wherein the means for controlling the operating condition comprise a clock generator, which is configured to switch from the second to the first clock rate.

10. The device according to claim 7, wherein the first and second operating conditions correspond to different, respective, first and second operating temperatures of the electronic circuit, and wherein the means for controlling the operating condition comprise a temperature controller, which is configured to switch the electronic circuit from the second to the first operating temperature.

11. The device according to claim 7, wherein the means for controlling the operating condition are configured to switch momentarily from the second to the first operating condition in response to a control signal requesting the secret value.

12. The device according to claim 7, wherein the electronic circuit comprises a flip-flop, which is metastable in the second operating mode and stable in the first operating mode.

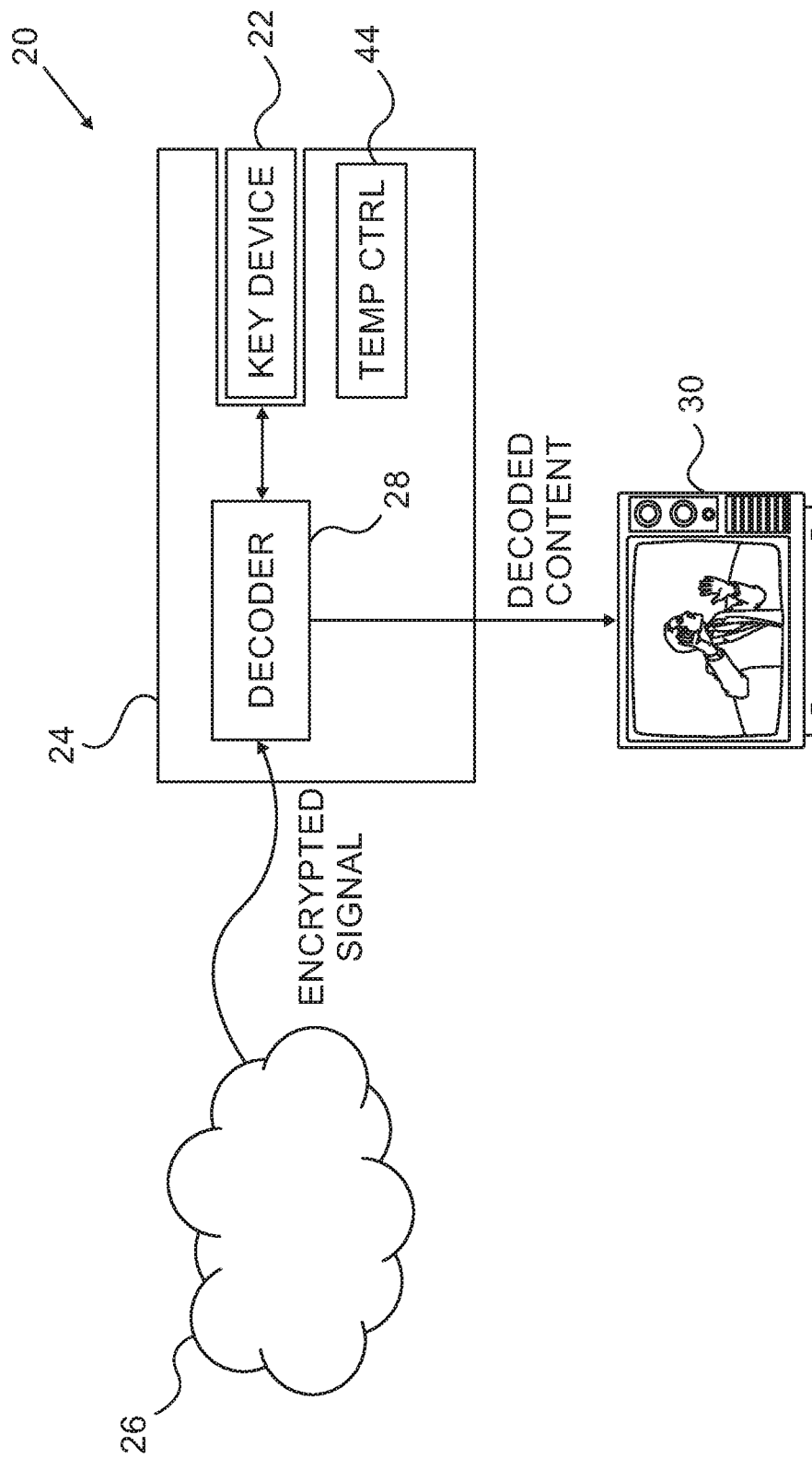


FIG. 1

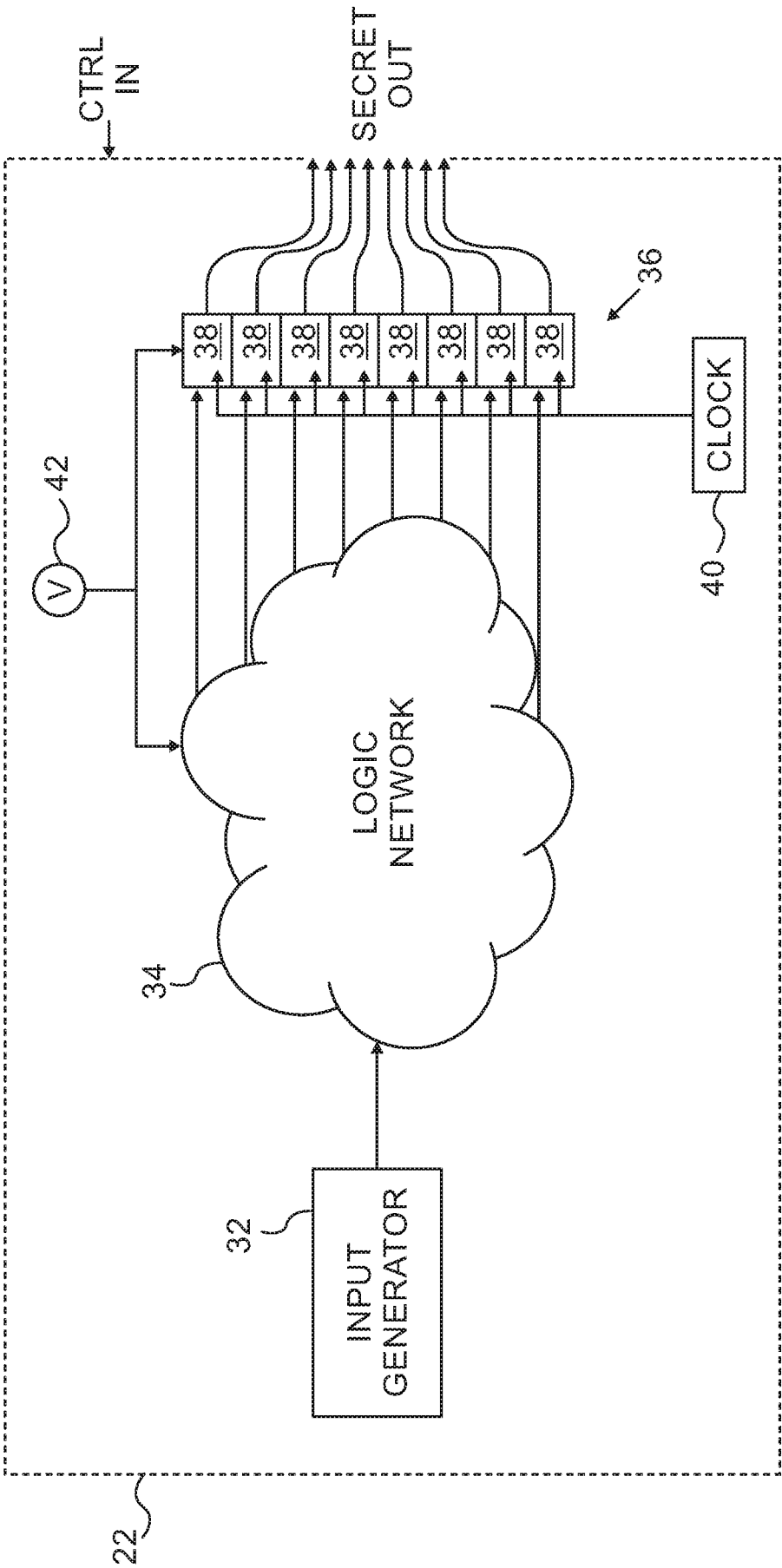


FIG. 2

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2009/055724

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/00 G06K19/073

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 G06K

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 practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/264273 A1 (POCKRANDT WOLFGANG [DE]) 30 December 2004 (2004-12-30) paragraphs [0003], [0004], [0008]; claim 9	1-12
Y	EP 1 650 696 A1 (SAMSUNG ELECTRONICS CO LTD [KR]) 26 April 2006 (2006-04-26) paragraph [0032]; figure 5	1-12
Y	US 6 927 580 B2 (WUIDART SYLVIE [FR] ET AL) 9 August 2005 (2005-08-09) abstract column 2, line 1 - column 3, line 29	1-12
A	EP 1 429 227 A2 (RENESASTECHNOLOGY CORP [JP] RENESAS TECH CORP [JP]) 16 June 2004 (2004-06-16) paragraphs [0129] - [0131]	1-12
	-/--	



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 document 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

24 March 2010

Date of mailing of the international search report

06/04/2010

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

Kerschbaumer, J

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2009/055724

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2003/133241 A1 (FEUSER MARKUS [DE] ET AL) 17 July 2003 (2003-07-17) paragraphs [0021] - [0030] -----	1-12

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IB2009/055724

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 2004264273	A1	30-12-2004	WO	03054789 A1	03-07-2003
			DE	10161046 A1	03-07-2003
			EP	1454293 A1	08-09-2004
EP 1650696	A1	26-04-2006	CN	1763772 A	26-04-2006
			KR	20060034995 A	26-04-2006
			US	2006085655 A1	20-04-2006
US 6927580	B2	09-08-2005	DE	60220975 T2	13-03-2008
			EP	1291817 A1	12-03-2003
			FR	2829265 A1	07-03-2003
			JP	2003243525 A	29-08-2003
			US	2003117148 A1	26-06-2003
EP 1429227	A2	16-06-2004	DE	60319051 T2	05-02-2009
			JP	2004206680 A	22-07-2004
			KR	20040053803 A	24-06-2004
			US	2007189051 A1	16-08-2007
			US	2004120195 A1	24-06-2004
US 2003133241	A1	17-07-2003	CN	1430153 A	16-07-2003
			DE	10164419 A1	17-07-2003
			EP	1326203 A2	09-07-2003
			JP	2003233790 A	22-08-2003