

(51) International Patent Classification:
H04L 9/00 (2006.01)(21) International Application Number:
PCT/US2013/022501(22) International Filing Date:
22 January 2013 (22.01.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/353,462 19 January 2012 (19.01.2012) US(71) Applicant: **TEXAS INSTRUMENTS INCORPORATED** [US/US]; P.O.Box 655474, Mail Station 3999, Dallas, TX 75265-5474 (US).(71) Applicant (for JP only): **TEXAS INSTRUMENT JAPAN LIMITED** [JP/JP]; 24-1, Nishi-shinjuku 6-chome, Shinjuku-ku Tokyo 160-8366 (JP).(72) Inventors: **SEOK, Mingoo**; 606 W. 116th St. #62, New York, NY 10027 (US). **REN, Jing-Fei**; 3316 Grand Mesa Drive, Plano, TX 75025 (US). **GOEL, Manish**; 4417 Helston Drive, Plano, TX 75024 (US).(74) Agents: **FRANZ, Warren, L.** et al.; Texas Instruments Incorporated, Deputy General Patent Counsel, P.O. Box 655474, Mail Station 3999, Dallas, TX 75265-5474 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

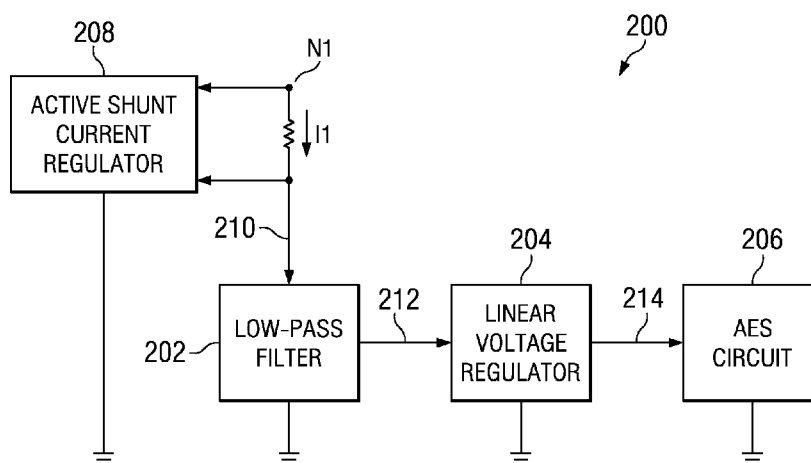
Declarations under Rule 4.17:

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))

Published:

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

(54) Title: APPARATUS AND METHODS TO HIDE POWER SIGNATURE IN CRYPTOGRAPHIC CIRCUITS

**FIG. 2**

(57) **Abstract:** A cryptographic device (200) reduces risk of external analysis of power consumed by an encryption circuit (206) by maintaining a substantially current draw on an external power input node (N1) during operation. An active shunt current regulator (208) draws current to ground when not drawn by the encryption circuit (206). A low-pass filter (202) and a linear voltage regulator (204) smoothes power spikes and keeps power supply voltage constant at an input to the encryption circuit (206).

APPARATUS AND METHODS TO HIDE POWER SIGNATURE IN CRYPTOGRAPHIC CIRCUITS

[0001] This relates to apparatus and methods for improving security of cryptographic devices against differential power analysis by hiding external power signature.

BACKGROUND

[0002] Cryptography is the practice and study of techniques for secure communication in the presence of unauthorized third parties. More generally, cryptography is about constructing and analyzing protocols that avoid unauthorized access by third parties and which are related to various aspects in information security such as data confidentiality, data integrity and authentication. Applications of cryptography include ATM cards, computers and personal digital assistants (PDAs).

[0003] Encryption is the process of converting ordinary information (often called plain text) into unintelligible information (often called cipher text). Decryption is the reverse; moving from the unintelligible cipher text back to plain text. A cipher involves a pair of algorithms that create both the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithms and in each instance by a key. A key is a non-public parameter (ideally known only to the communicants) for a specific message exchange context. Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. Cryptanalysis is the study of methods for obtaining the meaning of encrypted information without having access to the key normally required to do so (i.e., the study of how to crack encryption algorithms or their implementations).

[0004] The advanced encryption standard (AES), adopted by the US government, is one of the most popular algorithms used for symmetric key cryptography. Because of its theoretical strength and because it is relatively simple to implement in hardware, it has been adopted in many portable electronics (e.g., smart cards and readers). While the AES

algorithm itself has been considered to provide adequate security for today's applications, physical implementations of the algorithm on integrated circuits (ICs), for example, may leak information such that the security information may be compromised.

[0005] Power analysis attacks have been used to obtain secure information from cryptographic devices without authorization. The power analysis attacks may exploit the fact that the behavior of power consumption (i.e., side-channel information) of a cryptographic device is related to the computations performed by the cryptographic device. FIG. 1 is a normalized power trace showing the power consumed during a single AES operation performed on an IC over multiple clock cycles. Otherwise secure information is vulnerable to unauthorized capture through analysis of single or multiple power traces.

[0006] A differential power analysis (DPA) attack is one form of a power analysis attack. A DPA attack uses a large number of power traces (sometimes more than 100000 traces) to correlate them to a hypothetical power model of a cryptographic algorithm. The risk that DPA attacks may obtain otherwise secure information creates a security problem. A DPA attack can reveal a key to the AES algorithm by analyzing less than 2000 power traces from a circuit on an IC that implements the AES algorithm (i.e., an AES core). Therefore, it is important that an AES circuit not leak a power signature that may be used by DPA attacks to retrieve secure information from the AES circuit.

SUMMARY

[0007] The drawings and description, in general, disclose a method and device for reducing the probability that secure information may be obtained by unwanted third parties from a cryptographic device.

[0008] In a described example implementation, a cryptographic device includes an active shunt current regulator, a low-pass filter, a linear voltage regulator and an AES (advanced encryption standard) circuit. The AES circuit encrypts information using the advanced encryption standard algorithm. The cryptographic device, in general, hides the power consumed by the AES circuit by preventing power spikes (see FIG. 1) on the electrical node that provides power to the AES circuit. For example, the electrical node that provides power to the AES circuit may be an external pin on an integrated circuit, a solder bump on integrated circuit or an electrical trace on a printed circuit board (PCB).

[0009] The low-pass filter smoothes the power spikes on the electrical node that provides power to the AES circuit by providing charge when the AES is operating. The active shunt current regulator shunts current to ground when the AES is not drawing significant amounts of current keeping the current drawn through the electrical node substantially constant (i.e., prevents power spikes). The linear voltage regulator acts as a low-pass filter and keeps the power supply voltage on the AES circuit reasonably constant.

[0010] The cumulative effect of the low-pass filter, the linear voltage regulator and the active shunt current regulator is to smooth the power spikes on the electrical node that provides power to the AES circuit. Smoothing the power spikes on the electrical node reduces the probability that secure information created by the AES circuit may be obtained by unwanted third parties. The operation of the low-pass filter, the linear voltage regulator and the active shunt current regulator will be explained in more detail later in the specification.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] FIG. 1 is a normalized power trace showing the power consumed during a single AES operation performed on an IC over multiple clock cycles.

[0012] FIG. 2 is a block diagram of a first embodiment of a cryptographic device for reducing the probability that secure information may be obtained by unwanted third parties.

[0013] FIG. 3 is a schematic drawing of an embodiment of a passive low-pass filter.

[0014] FIG. 4 is a schematic drawing of an embodiment of an active shunt current regulator.

[0015] FIG. 5 is a schematic drawing of an embodiment of a linear voltage regulator.

[0016] FIG. 6 is a block diagram of a second embodiment of a cryptographic device for reducing the probability that secure information may be obtained by unwanted third parties.

[0017] FIG. 7 is a schematic drawing of an embodiment of a noise generator.

[0018] FIG. 8 is a flow chart illustrating an embodiment of a method for reducing the probability that secure information may be retrieved from a cryptographic device.

DETAILED DESCRIPTION OF EXAMPLE EMBODIMENTS

[0019] FIG. 2 is a block diagram of a first example embodiment of a cryptographic device for reducing the probability that secure information may be obtained by unwanted third parties. In this first embodiment, an accessible electrical node N1 is connected to a first terminal of a sensing resistor R1 and an input to the active shunt current regulator 208. The accessible electrical node N1 can be any electrical node accessible to unwanted third parties. For example, the accessible electrical node may be a power pin located on an integrated circuit, a solder bump located on an integrated circuit or an electrical trace located on a printed circuit board. Unwanted third parties may use accessible electrical nodes to perform differential power analysis in order to obtain secure information.

[0020] The second terminal of the sensing resistor R1 is connected to an input of the active shunt current regulator 210 and the input of the low-pass filter 202. The output 212 of the low-pass filter 202 is connected to the input of the linear voltage regulator 204. The output 214 of the linear voltage regulator 204 is connected to the input of the AES circuit 206.

[0021] FIG. 3 is a schematic drawing of an embodiment of a passive low-pass filter 202. In this embodiment, a first terminal of the resistor R2 is connected to the input of the passive low-pass filter 202 and a second terminal of the resistor R2 is connected to the output of the passive low-pass filter 202. Also in this embodiment, a first terminal of the capacitor C1 is connected to the output of the passive low-pass filter 202 and a second terminal of the capacitor C1 is connected to ground. The low-pass filter 202 reduces the change in current (di/dt) of current I1 being drawn through the sensing resistor R1. As a consequence, the power peaks on accessible node N1 are reduced making it more difficult to perform successful differential power analysis.

[0022] FIG. 4 is a schematic drawing of an embodiment of an active shunt current regulator 208. In this embodiment of an active shunt current regulator 208, a first input 404 of the active shunt current regulator 400 is connected to the first terminal of a resistor R3. The second input 406 of the active shunt current regulator 208 is connected to the

drain of NFET1 (n-type field-effect transistor) and to a first input of an operational amplifier 402.

[0023] A reference voltage V_{ref1} is created at the second input of the operational amplifier 402 by connecting a first terminal of variable resistor R4 to the second terminal of resistor R3. The reference voltage V_{ref1} can be adjusted by varying the resistance of resistor R3. The output 408 of the operational amplifier 402 is directly connected to the gate of NFET1. The source of NFET1 is connected to ground.

[0024] The voltage on node 408 is proportional to the voltage V_{dif1} between the inputs 406 and V_{ref1} . When the voltage V_{in} between the inputs 404 and 406 increases, the voltage on node 408 decreases thereby decreasing the current drawn through NFET1. When the voltage V_{in} between the inputs 404 and 406 decreases, the voltage on node 408 increases thereby increasing the current drawn through NFET1. This feedback mechanism in the active shunt current regulator 208 helps to maintain the current I_1 drawn through node N1 (see FIG. 1) at a substantially constant value. Because the current I_1 drawn through node N1 is held at a substantially constant value, it becomes more difficult to perform successful differential power analysis and obtain secure information from the AES circuit 206.

[0025] FIG. 5 is a schematic drawing of an embodiment of a linear voltage regulator 204. In this embodiment of a linear voltage regulator 204, the input 508 of the linear voltage regulator 204 is connected to the source of a PFET1 (p-type field-effect transistor). The drain of PFET1 is connected to the output V_{reg} of the voltage regulator 204. The output V_{reg} of the voltage regulator 204 provides a substantially constant voltage to the AES circuit 206. Providing a substantially constant voltage to the AES circuit 206 helps the AES circuit 206 function properly.

[0026] A capacitor C2 is also directly connected to the output V_{reg} of the voltage regulator 204. The capacitor C2 acts as a low-pass filter helping to maintain a substantially constant voltage on the output V_{reg} of the voltage regulator 204. A first terminal of resistor R5 is connected to the output V_{reg} . The second terminal of resistor R5 is connected to a first input 506 of an operational amplifier 502 and to the first terminal of variable resistor R6. Varying the resistance of resistor R6 makes it possible to adjust the voltage on the first input 506 of the operational amplifier 502.

[0027] A reference voltage V_{ref2} is provided to the second input of the operational amplifier 502. The reference voltage V_{ref2} remains substantially constant. The difference voltage V_{dif2} determines the voltage 504 provided to the gate of PFET1. The feedback from node 506 changes the difference voltage V_{dif2} and as a result helps to maintain a substantially constant voltage on the output V_{reg} of the voltage regulator 204.

[0028] FIG. 6 is a block diagram of a second example embodiment of a cryptographic device 600 for reducing the probability that secure information may be obtained by unwanted third parties. In this second embodiment, an accessible electrical node N1 is connected to a first terminal of a sensing resistor R1 and an input to the active shunt current regulator 208. The accessible electrical node N1 can be any electrical node accessible to unwanted third parties. For example, the accessible electrical node may be a power pin located on an integrated circuit, a solder bump located on an integrated circuit or an electrical trace located on a printed circuit board. Unwanted third parties may use accessible electrical nodes to perform differential power analysis in order to obtain secure information.

[0029] The second terminal of the sensing resistor R1 is connected to an input of the active shunt current regulator 210 and the input of the low-pass filter 202. The output 212 of the low-pass filter 202 is connected to the input of the linear voltage regulator 204. The output 214 of the linear voltage regulator 204 is connected to the input of the AES circuit 206 and to a first input of the noise generator 216. A second input of the noise generator 602 is directly connected to node N1.

[0030] The cumulative effect of the low-pass filter 202, the linear voltage regulator 204 and the active shunt current regulator 208 is to smooth the power spikes on the electrical node N1 that provides power to the AES circuit. Smoothing the power spikes on the electrical node N1 reduces the probability that secure information created by the AES circuit may be obtained by unwanted third parties.

[0031] The noise generator 602 shown in FIG. 6 does not smooth the power spikes on the electrical node N1. The noise generator 602 adds random noise to node N1. When random noise is added to node N1, it becomes more difficult to determine the secure information produced by the AES circuit.

[0032] FIG. 7 is a schematic drawing of an embodiment of a noise generator 602. In this embodiment, the noise generator 602 consists of a linear feedback shift register (LFSR) 702 and an array of transistors, NFET1, NFET2 – NFETN. The LFSR generates random signals on nodes 704, 706 and 708 based on the seed used. Because the output (nodes 704, 706 and 708) of the LFSR randomly changes, the power consumed through the array of transistors is modulated, increasing the noise on node N1. The seed of the random signal generator can be updated frequently to make it more difficult for a third party to track the random patterns.

[0033] FIG. 8 is a flow chart illustrating an embodiment of a method for reducing the probability that secure information may be retrieved from a cryptographic device. During a first step 802, the current drawn from a power supply is measured. After the current is measured, it is determined during step 804 when the current drawn is too low. When the current drawn is not too low, the method returns to measuring the current drawn from the power supply. When the current is too low, additional current is shunted to ground from the power supply (step 806). Shunting additional current to ground when current from the power supply is low causes the overall current drawn from the power supply to be substantially constant. When the overall current drawn from the power supply is substantially constant it is more difficult to obtain secure information from the AES circuit 206.

[0034] Those skilled in the art to which the foregoing relates will appreciate that modifications may be made to the described examples, and also that many other embodiments are possible, within the scope of the claimed invention.

CLAIMS

What is claimed is:

1. A cryptographic device, comprising:
 - a resistor, the first resistor having first and second terminals wherein the first terminal is directly connected to an accessible electrical node wherein the accessible electrical node provides power to the cryptographic device;
 - an active shunt current regulator having first and second inputs wherein the first input is directly connected to the first terminal of the resistor and the second input is directly connected to the second terminal of the resistor;
 - a low-pass filter having an input and an output wherein the input is directly connected to the second terminal of the first resistor;
 - a linear voltage regulator having an input and an output wherein the input of the linear voltage regulator is directly connected to the output of the low-pass filter; and
 - an AES (advanced encryption standard) circuit having an input wherein the input is directly connected to the output of the linear voltage regulator;wherein the device is configured so that current drawn from the accessible electrical node remains substantially constant; and
wherein the device is further configured so that a voltage on the input of the AES circuit remains substantially constant.
2. The device of claim 1, further comprising a noise generator connected to the accessible electrical node.
3. The device of claim 1, wherein the low-pass filter is passive.
4. The device of claim 3, wherein the low-pass filter comprises:
 - a resistor having a first and a second terminal wherein the first terminal is directly connected to the input of the low-pass filter and the second terminal is directly connected to the output of the low-pass filter; and

a capacitor having a first and a second terminal wherein the first terminal of the capacitor is directly connected to the output of the low-pass filter and the second terminal of the capacitor is directly connected to ground.

5. The device of claim 1, wherein the linear voltage regulator comprises:

a PFET (p-type field-effect transistor) having a gate, drain and source wherein the source is directly connected to the input of the linear voltage regulator and the drain is directly connected to the output of the linear voltage regulator;

a capacitor having a first and a second terminal wherein the first terminal is directly connected to the output of the linear voltage regulator and the second terminal is directly connected to ground;

a resistor having a first and a second terminal wherein the first terminal is connected to the output of the linear voltage regulator;

a variable resistor having a first and a second terminal wherein the first terminal of the variable resistor is directly connected to the second terminal of the first resistor and the second terminal of the variable resistor is directly connected to ground; and

an operational amplifier having a first input, a second input and an output wherein the first input of the operational amplifier is directly connected to the second terminal of the resistor, wherein the second input of the operational amplifier is directly connected to a first voltage reference and wherein the output of the operational amplifier is directly connected to the gate of the PFET.

6. The device of claim 1, wherein the active shunt current regulator comprises:

an NFET (n-type field-effect transistor) having a gate, drain and source wherein the drain is directly connected to the second input of the active shunt current regulator and the source is directly connected to ground;

a resistor having a first and a second terminal wherein the first terminal is connected to the first input of the active shunt current regulator;

a variable resistor having a first and a second terminal wherein the first terminal of the variable resistor is directly connected to the second terminal of the first resistor and the second terminal of the variable resistor is directly connected to ground; and

an operational amplifier having a first input, a second input and an output wherein the first input of the operational amplifier is directly connected to the second terminal of the resistor, wherein the second input of the operational amplifier is directly connected to the drain of the NFET and wherein the output of the operational amplifier is directly connected to the gate of the NFET.

7. The device of claim 2, wherein the noise generator comprises:

a plurality of NFETs (n-type field-effect transistor) wherein each NFET in the plurality of NFETs has a gate, source and drain, wherein the plurality of NFETs are connected in parallel wherein the source of each NFET in the plurality of NFETs is directly connected to ground, wherein the drain of each NFET in the plurality of NFETs is directly connected to the accessible electrical node; and

a linear feedback shift register (LFSR) having a first input, a second input and a plurality of outputs wherein the first input is directly connected to the output of the linear voltage regulator, wherein the second input is connected to a signal that provides a seed value for the LFSR, and wherein each output of the plurality of outputs is connected to a gate in the plurality of NFETs; and

wherein the noise generator creates noise on the accessible electrical node to reduce the probability that secure information may be retrieved from the cryptographic device.

8. The device of claim 1, wherein the accessible electrical node is selected from a group consisting of a power pin located on an integrated circuit, a solder bump located on an integrated circuit and an electrical trace located on a printed circuit board.

9. A method for reducing the probability that secure information may be retrieved from a cryptographic device, comprising:

maintaining a substantially constant current from a power supply that supplies current to the cryptographic device.

10. The method of claim 9, wherein maintaining a substantially constant current comprises:

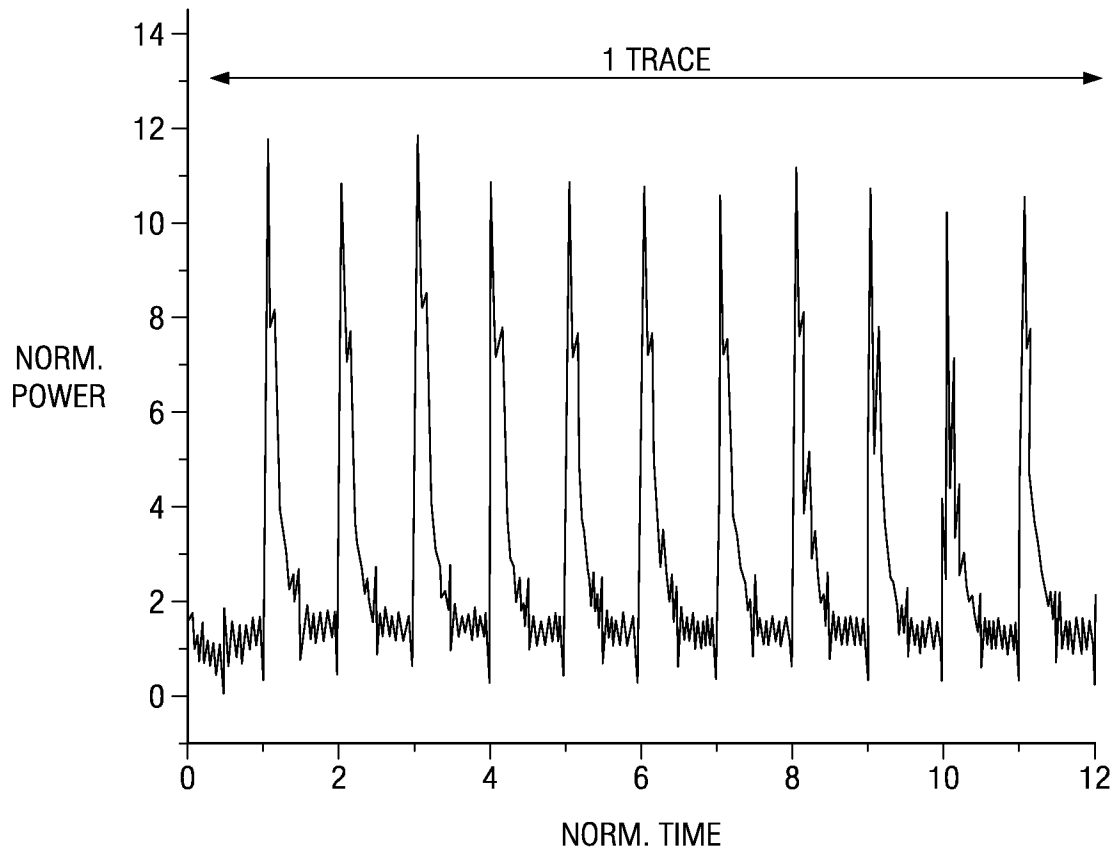
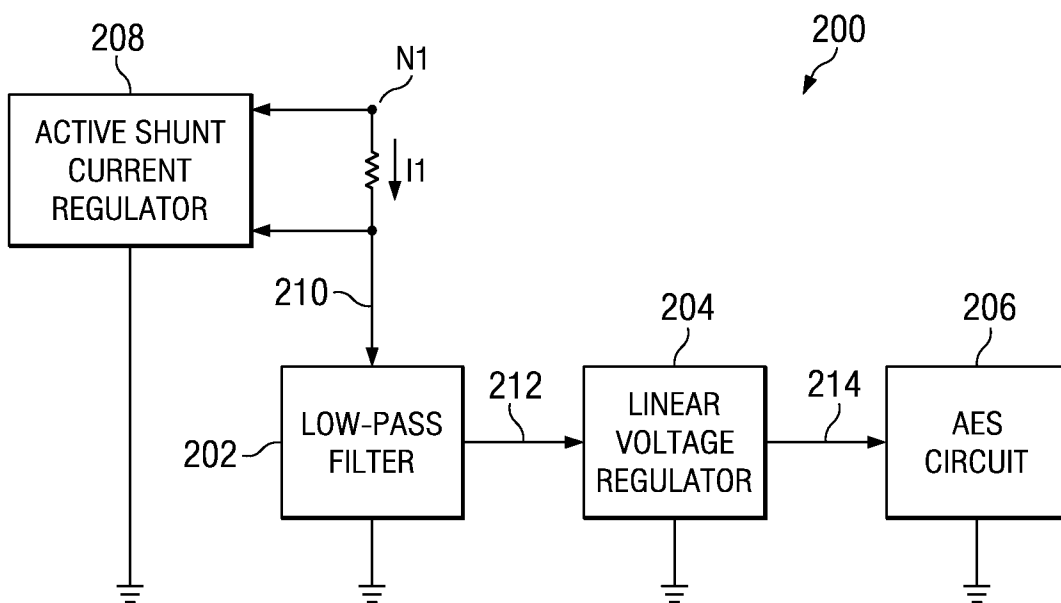
measuring current drawn from the power supply that supplies current to the cryptographic device; and

shunting additional current from the power supply to ground when the current drawn from the power supply is too low.

11. The method of claim 9, wherein maintaining a substantially constant current comprises storing charge on a capacitor to provide current when a drop in voltage occurs on the power supply.

12. The method of claim 9, wherein maintaining a substantially constant current comprises regulating the voltage of the power supply at a substantially constant voltage using a linear voltage regulator.

1/3

*FIG. 1**FIG. 2*

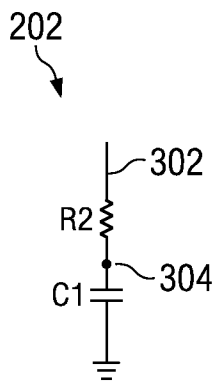


FIG. 3

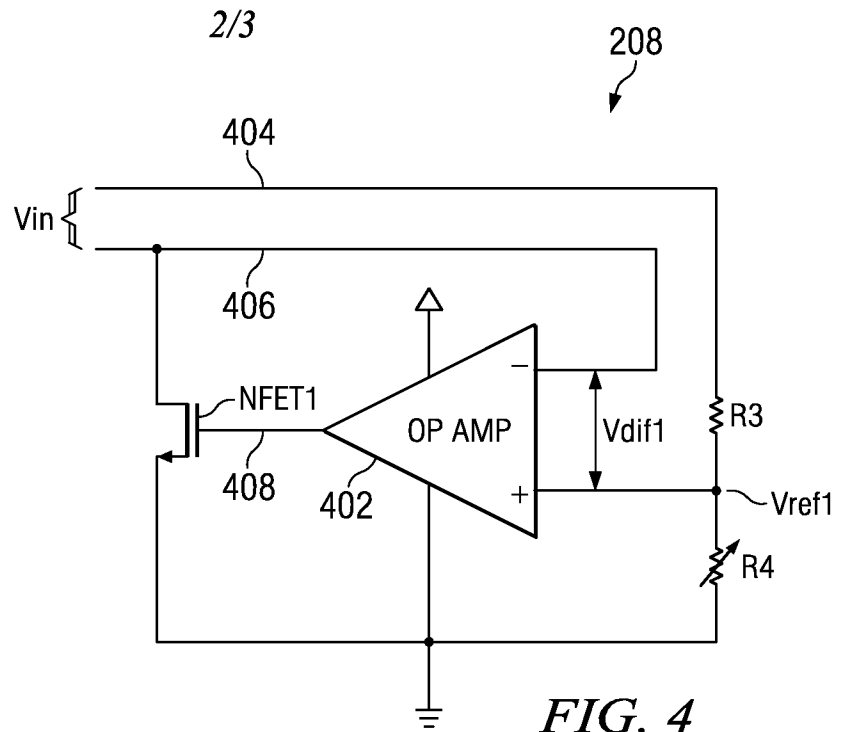


FIG. 4

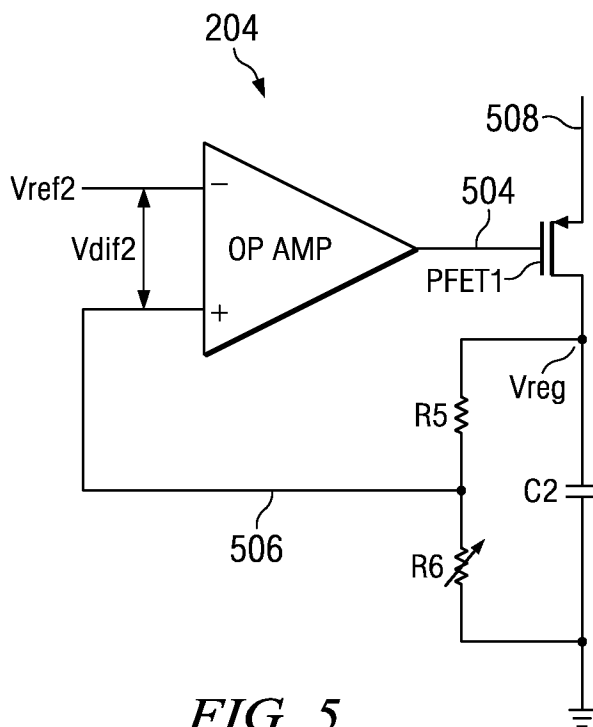


FIG. 5

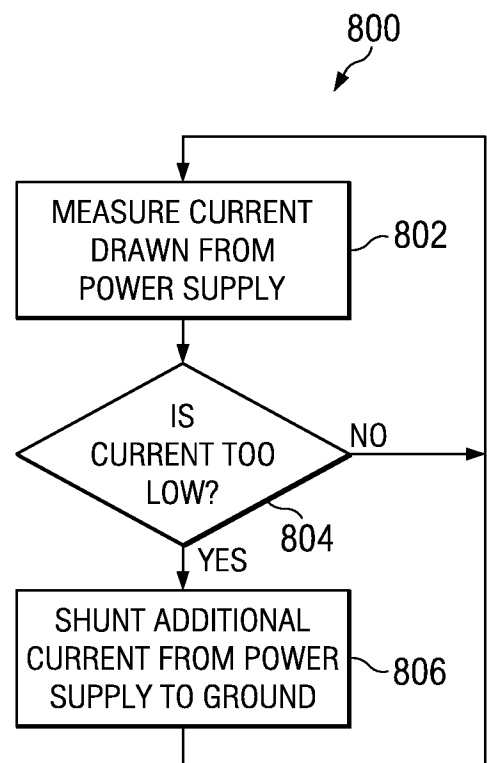


FIG. 8

3/3

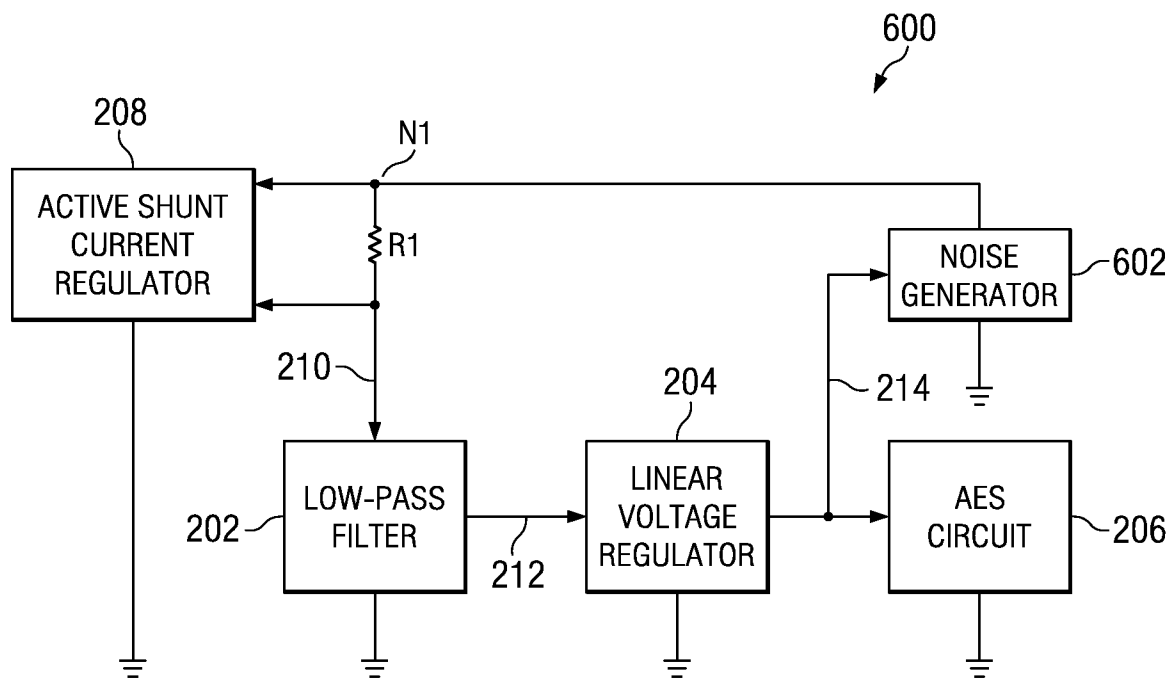


FIG. 6

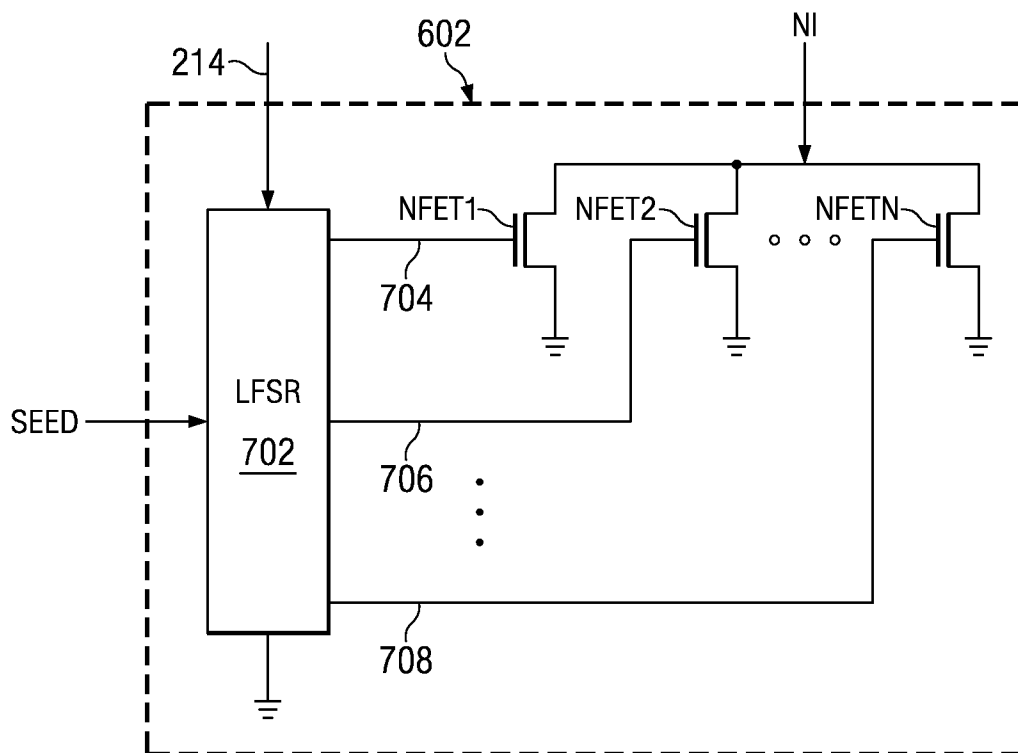


FIG. 7

A. CLASSIFICATION OF SUBJECT MATTER***H04L 9/00(2006.01)i***

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 9/00; G06F 11/30; G05F 1/00; H04K 1/02; G05F 1/40; G06F 17/00; H03K 19/00; G06F 1/26; G05F 3/16

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & keywords: cryptography, AES, regulator, supply, voltage, current, constant, filter, resister

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6766455 B1 (RYAN, JR., FREDERICK W.) 20 July 2004 See column 4, lines 29-33; column 6, lines 1-56; claims 12 and 14; and figures 1-2.	1-12
Y	US 2007-0035285 A1 (BALAKRISHNAN, BALU et al.) 15 February 2007 See paragraphs [0029] and [0031]-[0038]; claim 1; and figures 4 and 6.	1-12
A	US 2005-0218872 A1 (WICH, MATHEW T.) 06 October 2005 See paragraphs [0010]-[0027]; claim 1; and figure 2.	1-12
A	US 2005-0240782 A1 (HUBERT, GERARDUS T.M.) 27 October 2005 See paragraphs [0017]-[0036]; claims 1-2 and 7; and figure 1.	1-12
A	US 2004-0150382 A1 (TAKABAYASHI, YASUTAKA) 05 August 2004 See paragraphs [0034]-[0044]; claim 1; and figure 1.	1-12
A	US 2011-0085662 A1 (MYERS, BRENT A. et al.) 14 April 2011 See paragraphs [0073]-[0076]; claim 1; and figure 22.	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 application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

29 April 2013 (29.04.2013)

Date of mailing of the international search report

30 April 2013 (30.04.2013)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan
City, 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

KANG, Hee Gok

Telephone No. 82-42-481-8264



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2013/022501

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6766455 B1	20.07.2004	CA 2327974 A1 EP 1107502 A2 EP 1107502 A3	09.06.2001 13.06.2001 07.05.2003
US 2007-0035285 A1	15.02.2007	EP 1468485 A1 EP 1468485 B1 JP 04416510 B2 JP 05017319 B2 JP 2005-516569 A JP 2009-201353 A US 2003-0132738 A1 US 2005-0088161 A1 US 2006-0028190 A1 US 6833692 B2 US 6967472 B2 US 7148671 B2 US 7301319 B2 WO 03-063328 A1	20.10.2004 14.03.2007 04.12.2009 15.06.2012 02.06.2005 03.09.2009 17.07.2003 28.04.2005 09.02.2006 21.12.2004 22.11.2005 12.12.2006 27.11.2007 31.07.2003
US 2005-0218872 A1	06.10.2005	CN 1965277 A CN 1965277 C0 EP 1735674 A1 EP 1735674 A4 US 6963188 B2 WO 2005-103855 A1	16.05.2007 16.05.2007 27.12.2006 31.10.2007 08.11.2005 03.11.2005
US 2005-0240782 A1	27.10.2005	AU 2003-259494 A1 AU 2003-259494 A8 CN 1682175 A CN 1682175 B EP 1552368 A2 GB 0221240 D0 JP 2005-538641 A US 7571492 B2 WO 2004-025444 A2 WO 2004-025444 A3	30.04.2004 30.04.2004 12.10.2005 08.12.2010 13.07.2005 23.10.2002 15.12.2005 04.08.2009 25.03.2004 10.09.2004
US 2004-0150382 A1	05.08.2004	EP 1282072 A1 EP 1282072 B1 EP 1622067 A1 EP 1622067 B1 JP 03539940 B2 JP 2003-044151 A US 2003-0030417 A1 US 6696822 B2 US 6967470 B2	05.02.2003 28.06.2006 01.02.2006 27.02.2008 07.07.2004 14.02.2003 13.02.2003 24.02.2004 22.11.2005
US 2011-0085662 A1	14.04.2011	EP 2489127 A2 KR 10-2012-0098679 A	22.08.2012 05.09.2012

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2013/022501Patent document
cited in search reportPublication
datePatent family
member(s)Publication
date

US 8330493 B2

11.12.2012

WO 2011-047035 A3

28.07.2011