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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 December 2007 (13.12.2007)

PCT

(10) International Publication Number
WO 2007/143299 A1

(51) International Patent Classification:
H02J 7/00 (2006.01)

(21) International Application Number:
PCT/US2007/067749

(22) International Filing Date: 30 April 2007 (30.04.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/442,942 30 May 2006 (30.05.2006) US

(71) Applicant *(for all designated States except US)*: **SYMBOL TECHNOLOGIES, INC.** [US/US]; One Motorola Plaza, Holtsville, New York 11742 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **PAUL, Christopher R.** [US/US]; 20 Folger Street, Bayport, New York 11705 (US). **CABANA, Joseph** [US/US]; 5 Vernon Lane, Centereach, New York 11720 (US).

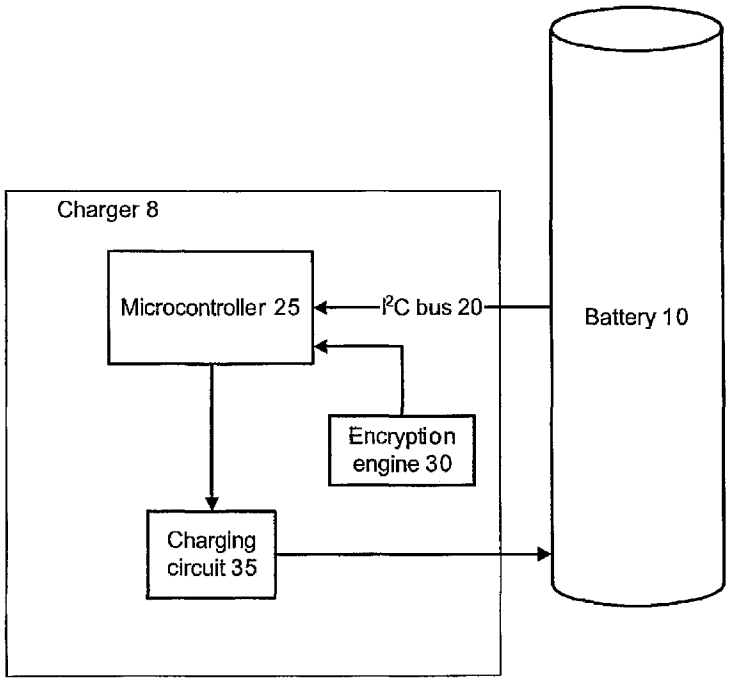
(74) Agents: **KAPLUN, Oleg, F.** et al.; 150 Broadway, Suite 702, New York, New York 10038 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, 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, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, 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,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR AUTHENTICATING A BATTERY



(57) Abstract: Described is a system and method for authenticating a power source. The system comprises a battery including a first encryption engine storing a first key, and a battery charger including a microcontroller and a second encryption engine storing a second key. When the microcontroller detects a coupling of the battery to the charger, the microcontroller issues a challenge to the first encryption engine and the second encryption engine. The first encryption engine generates a first response as a function of the challenge, the first key and a predefined algorithm, and the second encryption engine generates a second response as a function of the challenge, the second key and the predefined algorithm. The microcontroller compares the first and second responses to authenticate the battery.

WO 2007/143299 A1

FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, 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*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

System and Method for Authenticating a Battery

Inventors: Christopher PAUL and Joseph CABANA

Field of the Invention

[0001] The present invention relates generally to systems and methods for authenticating a battery.

Background

[0002] A conventional battery charger recharges a rechargeable battery which is used in a wireless electronic device. The charger may be capable of mating with and charging several types of batteries. However, if a different battery is not capable of receiving the same charging voltage and charging rate from the charger as the batteries intended to be recharged by the charger, the different battery may explode, irreparably damaging the charger and potentially causing harm to bystanders. Thus, there is a need to ensure authenticity of a battery which is coupled to the charger.

Summary of the Invention

[0003] The present invention relates to a system and method for authenticating a battery. The system comprises a battery including a first encryption engine storing a first key, and a battery charger including a microcontroller and a second encryption engine storing a second key. When the microcontroller detects a coupling of the battery to the charger, the microcontroller issues a challenge to the first encryption engine and the second encryption engine. The first encryption engine generates a first response as a function of the challenge, the first key and a predefined algorithm, and the second encryption

engine generates a second response as a function of the challenge, the second key and the predefined algorithm. The microcontroller compares the first and second responses to authenticate the battery.

Description of the Drawings

[0004] Fig. 1 shows an exemplary embodiment of a system for authenticating a battery according to the present invention.

[0005] Fig. 2 shows an exemplary embodiment of a method for authenticating a battery according to the present invention.

[0006] Fig. 3 shows an exemplary embodiment of a battery according to the present invention.

Detailed Description

[0007] The present invention may be further understood with reference to the following description and the appended drawings, wherein like elements are referred to with the same reference numerals. The present invention describes a system and method for authenticating a battery. While the exemplary embodiments of the present invention will be described with reference to a charger authenticating the battery, those of skill in the art will understand that the present invention may be utilized by any device which is coupleable to and draws power from and/or provides power to the battery.

[0008] Fig. 1 shows an exemplary embodiment of a system 5 according to the present invention in which the system 5 is implemented in a battery charger 8. The charger 8 includes electrical contacts for transferring power from, for example, a

line voltage to a battery 10. In other exemplary embodiments, the charger 8 may be wirelessly coupled to the battery 10 for wireless charging (e.g., inductive charging).

[0009] In the exemplary embodiments, the battery 10, as shown in Fig. 3, may be a smart battery which utilizes an integrated circuit to report and/or make available battery data to the charger 8. The battery 10 may include a microcontroller 305 and an encryption engine 310. As will be described further below, the encryption engine 310 executes a predetermined algorithm on a stored battery key in response to an authentication challenge from the charger 8. The battery data may include, but is not limited to, a battery type, a model number, a serial number, a manufacturer identifier, a discharge rate, a predicted remaining capacity, a temperature and a voltage.

[0010] In the exemplary embodiment, the charger 8 includes a charging circuit 35 for supplying power to the battery 10, a microcontroller 25 and an encryption engine 30 for authenticating the battery 10, and a communication bus (e.g., an I^2C bus 20) for communicating with the microcontroller 305 in the battery 10.

[0011] Fig. 2 shows an exemplary embodiment of a method 200 for authenticating the battery 10 according to the present invention. In step 205, the charger 8 detects a presence of the battery 10 by, for example, monitoring signals on the electrical contacts between the charger 8 and the battery 10. In another embodiment, the charger 8 may include a mechanical mechanism (e.g., a switch, latch, etc.) for detecting a coupling of the battery 10. For example, a two-position switch may indicate an absence of the battery 10 in a first state and a presence of the battery 10 in a

second state. Those of skill in the art will understand that any mechanical, electrical, optical, etc. means may be used to detect the coupling of the battery 10 to the charger 8.

[0012] In step 210, the microcontroller 25 generates a challenge to obtain a charger response from the encryption engine 30 and to obtain a battery response from the encryption engine 310 in the battery 10. For example, the encryption engine 30 stores a charger key, and, when instructed to do so by the microcontroller 25, generates the charger response based on the challenge, a predefined algorithm (e.g., cyclic redundancy check (CRC), secure hash algorithm (SHA-1), etc.) and the charger key. In the exemplary embodiments, the predefined algorithm is publicly known and the charger key is secret. The charger response may be strongly influenced by the charger key and the challenge, but it would be mathematically impossible to discover the charger key even with knowledge of the charger response, the challenge and the predefined algorithm.

[0013] The encryption engine 310 in the battery 10 generates the battery response based on the challenge, the predefined algorithm and a battery key. The predefined algorithm may be the same publicly known algorithm used by the encryption engine 30 to generate the charger response. As described above with reference to the charger response, the battery response may be strongly influenced by the battery key and the challenge, but it would be mathematically impossible to discover the battery key even with knowledge of the battery response, the challenge and the predefined algorithm.

[0014] In step 215, the microcontroller 25 receives the charger

response from the encryption engine 30 and the battery response from the battery 10. As described above, the microcontroller 25 in the charger 8 communicates with the microcontroller 305 in the battery 10 on the I^2C bus 20, allowing exchange of the challenge and the battery response. The microcontroller 305 transfers the challenge to the encryption engine 310 to obtain the battery response.

[0015] In step 220, the microcontroller 25 determines whether the battery response is identical to the charger response. When the responses are not identical, the microcontroller 25 may execute a predetermined action on a link between the charger 8 and the battery 10, as shown in step 225. For example, the microcontroller 25 may disable or selectively impair the charging circuit 35. If the charging circuit 25 is disabled, the battery 10 will not receive power from the charger 8. If the charging circuit 35 is selectively impaired, the charging circuit 35 may supply power to the battery 10 at a predetermined charge rate which is selected so that the battery 10 never becomes fully charged, rendering it useless as a power source. Alternatively, the predetermined charge rate may be selected to ensure that the battery 10 does not explode, *i.e.*, a very slow charge rate.

[0016] In optional step 230, an authentication failure message (e.g., LED color change/blink sequence, audible signal, etc.) may be output by the charger 8 to indicate that the battery 10 was not authenticated. The authentication failure message may prompt a user to replace the battery 10. When the charger 8 detects removal and replacement of a battery, the method 200 will repeat itself.

[0017] When the responses are identical, the microcontroller 25 may assume (without ever expressly knowing) that the battery key is identical to the charger key and authenticate the battery 10, as shown in step 240.

[0018] It will be apparent to those skilled in the art that various modifications may be made in the present invention, without departing from the spirit or scope of the invention. Thus, it is intended that the present invention cover the modifications and variations of this invention provided they come within the scope of the appended claims and their equivalents.

What is claimed is:

1. A system, comprising:

a battery including a first encryption engine storing a first key; and

a battery charger including a microcontroller and a second encryption engine storing a second key,

wherein, when the microcontroller detects a coupling of the battery to the charger, the microcontroller issues a challenge to the first encryption engine and the second encryption engine,

wherein the first encryption engine generates a first response as a function of the challenge, the first key and a predefined algorithm, and the second encryption engine generates a second response as a function of the challenge, the second key and the predefined algorithm, and

wherein the microcontroller compares the first and second responses to authenticate the battery.

2. The system according to claim 1, wherein the predefined algorithm is one of a cyclic redundancy check (CRC) and a secure hash algorithm (SHA-1).

3. The system according to claim 1, wherein, when the first and second responses are identical, the microcontroller authenticates the battery.

4. The system according to claim 3, wherein, after the battery is authenticated, the charger supplies power to the battery.

5. The system according to claim 1, wherein, when the first and second responses are different, the microcontroller executes a

predetermined action to impair a power supplied to the battery.

6. The system according to claim 5, wherein the predetermined action is at least one of (i) disabling a charging circuit in the charger which supplies power to the battery and (ii) lowering a charge current level.

7. The system according to claim 5, wherein the battery is used in a mobile computing device.

8. The system according to claim 7, wherein the mobile computing device includes at least one of a laser-based scanner, an imager-based scanner, a PDA, a mobile phone, a laptop, a tablet computer, a portable media player and a digital camera.

9. A device, comprising:

a charging circuit supplying power for recharging a battery;

an encryption engine storing a first key; and

a microcontroller issuing a challenge, upon coupling of the battery to the device, to (i) the encryption engine to obtain a first response and (ii) a further encryption engine of the battery to obtain a second response, the further encryption engine storing a second key,

wherein the encryption engine generates the first response using a predefined algorithm, the challenge and the first key, and the further encryption engine generates the second response using the predefined algorithm, the challenge and the second key, and

wherein the microcontroller compares the first and second responses to authenticate the battery.

10. The device according to claim 9, wherein the predefined algorithm is one of CRC and SHA-1.

11. The device according to claim 9, wherein, when the first and second responses are identical, the microcontroller allows the charging circuit to deliver power to the battery.

12. The device according to claim 9, wherein, when the first and second responses are different, the microcontroller one of (i) disables the charging circuit preventing it from supplying power to the battery and (ii) lowers a charge current level provided to the battery by the charging circuit.

13. The device according to claim 9, wherein the battery is used as a power source for a mobile computing device which includes at least one of a laser-based scanner, an imager-based scanner, a PDA, a mobile phone, a laptop, a tablet computer, a portable media player and a digital camera.

14. A method, comprising:

detecting a coupling of a battery to a battery charger, the charger including a first encryption engine storing a first key, the battery including a second encryption engine storing a second key;

issuing a challenge to the first encryption engine to obtain a first response to the second encryption engine to obtain a second response, the first response being generated as a function of the challenge, the first key and a predefined algorithm, the second response being generated as a function of the challenge, the second key and the predefined algorithm; and

authenticating the battery by the charger as a function of a

comparison of the first and second responses.

15. The method according to claim 14, wherein the predetermined algorithm is one of CRC and SHA-1.

16. The method according to claim 14, wherein the coupling is one of a physical coupling and a wireless coupling.

17. The method according to claim 14, further comprising:

when the first and second responses are identical, supplying power to the battery.

18. The method according to claim 14, further comprising:

when the first and second responses are different, performing one of the following substeps:

disabling a charging circuit in the charger to terminate the supply of power to the battery; and

lowering a charge current level.

19. A device, comprising:

an encryption means storing a first key; and

a processing means detecting a coupling of a battery to the device, the processing means issuing a challenge to the encryption means to obtain a first response and to a further encryption means on the battery to obtain a response, the further encryption means storing a second key,

wherein the encryption means generates the response using a predefined algorithm, the challenge and the first key, and the further encryption means generates the response using the predefined algorithm, the challenge and the second key, and

wherein the processing means compares the first and second

responses to authenticate the battery.

20. A battery, comprising:

an encryption engine storing a first key; and

a microcontroller coupled to the first encryption engine;

wherein, when the battery is coupled to a battery charger, the microcontroller receives a challenge for a first encryption engine, the first encryption engine generating a first response as a function of the challenge, the first key and a predefined algorithm, and

wherein the first response is compared to a second response to authenticate the battery, the second response being generated by the charger as a function the challenge, a second key and the predefined algorithm.

System 5

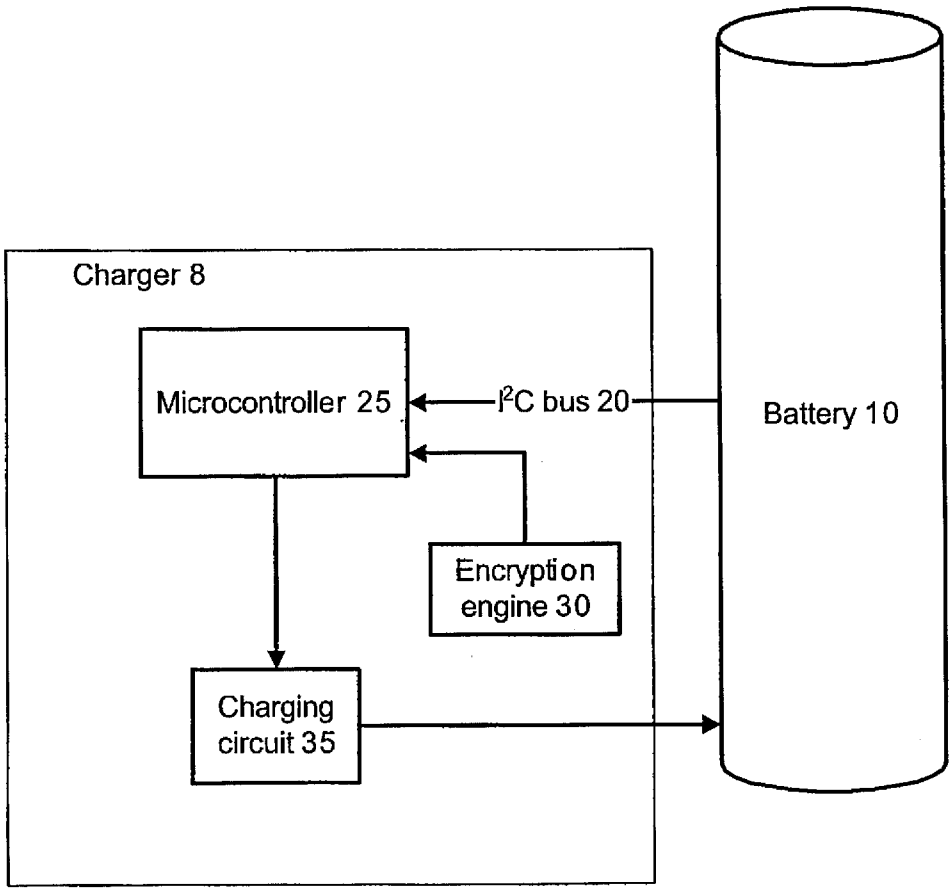


Fig. 1

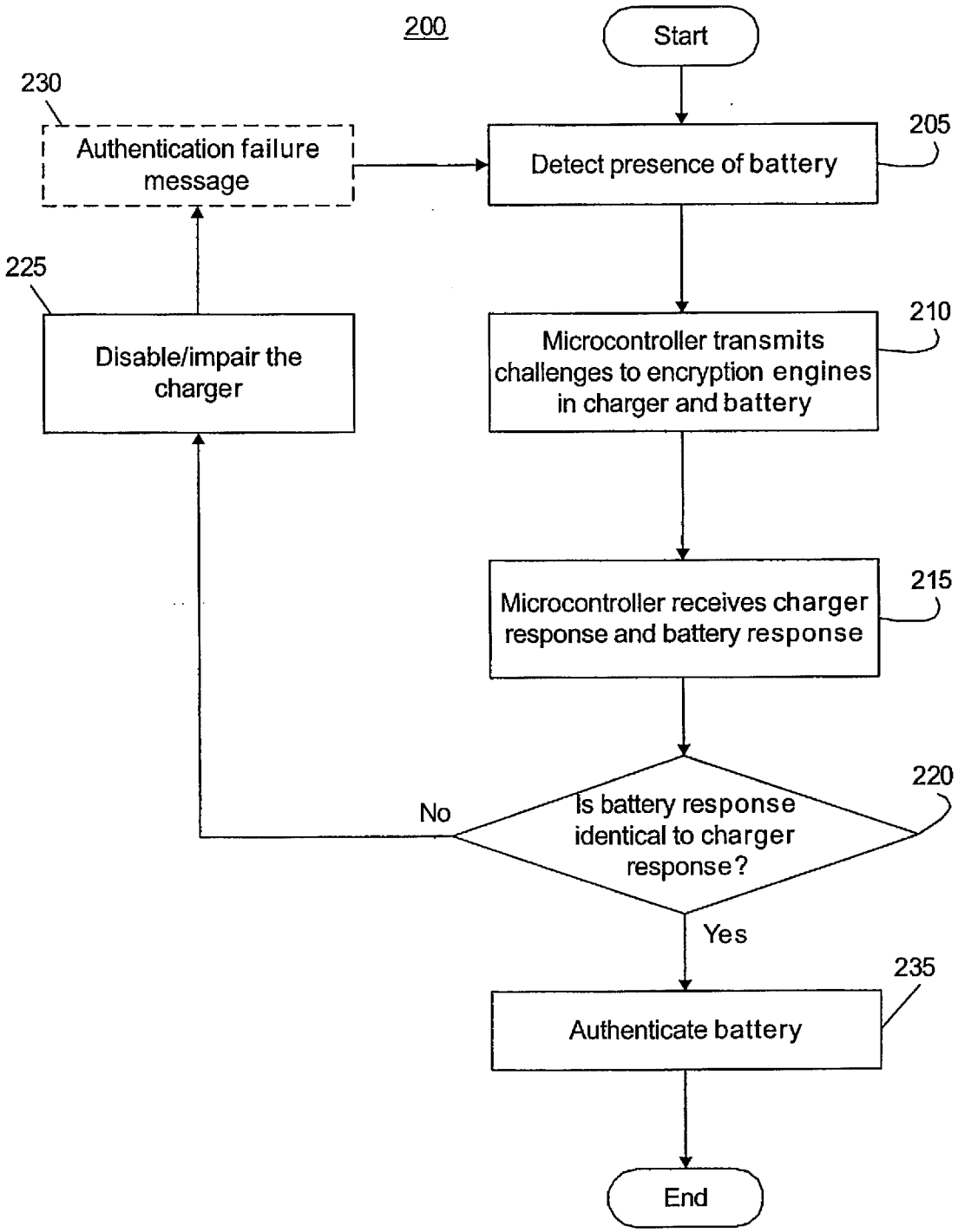

200
Start
230
Authentication failure message
205
Detect presence of battery
225
Disable/impair the charger
210
Microcontroller transmits challenges to encryption engines in charger and battery
215
Microcontroller receives charger response and battery response
220
No
Is battery response identical to charger response?
Yes
235
Authenticate battery
End

Fig. 2

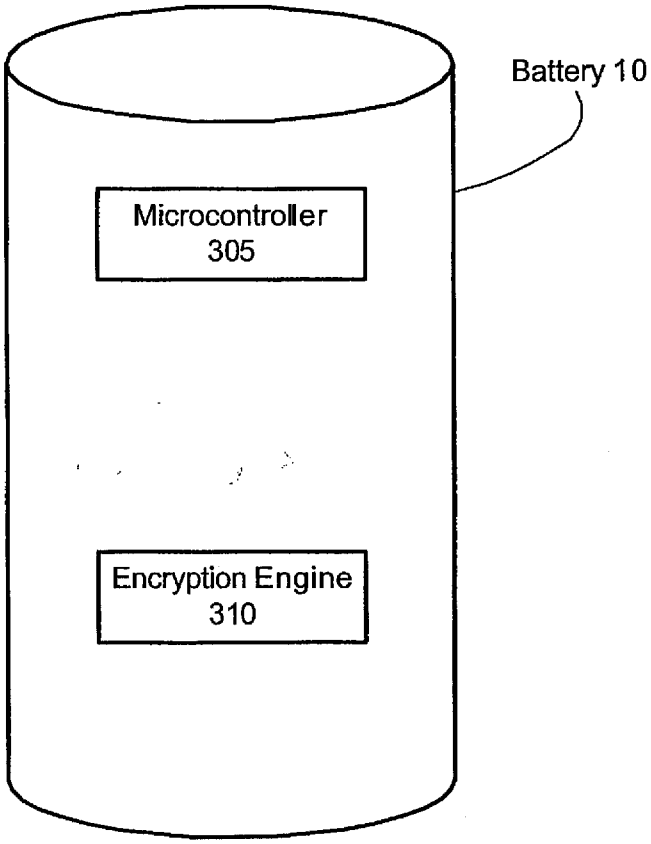


Fig. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/067749

A. CLASSIFICATION OF SUBJECT MATTER
INV. H02J7/00

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)
H02J

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 Y	US 2005/010782 A1 (OHKUBO KENICHI [JP]) 13 January 2005 (2005-01-13) paragraph [0020] - paragraph [0046]; claims 1-15; figures 2,3	1,3,9, 11,14, 19,20 2,4-8, 10,12, 13,15-18
Y	WO 99/00863 A (MOTOROLA INC [US]) 7 January 1999 (1999-01-07) claim 1	4,17
Y	US 2005/001589 A1 (EDINGTON LARRY G [US] ET AL) 6 January 2005 (2005-01-06) paragraph [0001]; claim 9	5-8,12, 13,18
Y	GB 2 416 633 A (LEAR CORP [US]) 1 February 2006 (2006-02-01) claim 1	16

-/--

[X] Further documents are listed in the continuation of Box C.

[X] 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	Date of mailing of the international search report
18 September 2007	08/10/2007

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Mapp, Graham

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/067749

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 867 006 A (DIAS DONALD R [US] ET AL) 2 February 1999 (1999-02-02) column 6, paragraphs 2,3 -----	2,10,15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2007/067749

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005010782 A1	13-01-2005	CN 1575006 A	02-02-2005
		JP 2005012663 A	13-01-2005
		KR 20040111143 A	31-12-2004
		TW 252009 B	21-03-2006
WO 9900863 A	07-01-1999	AU 8162198 A	19-01-1999
US 2005001589 A1	06-01-2005	NONE	
GB 2416633 A	01-02-2006	DE 102005033446 A1	09-03-2006
		US 2006028176 A1	09-02-2006
US 5867006 A	02-02-1999	NONE	