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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 June 2004 (24.06.2004)

PCT

(10) International Publication Number
WO 2004/053721 A1

(51) International Patent Classification[7]: G06F 17/00

(21) International Application Number:
PCT/US2003/038609

(22) International Filing Date: 2 December 2003 (02.12.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/432,293 10 December 2002 (10.12.2002) US

(71) Applicant and
(72) Inventor: WERTSBERGER, Shalom [IL/US]; 30 Fern Lane, South Portland, ME 04106 (US).

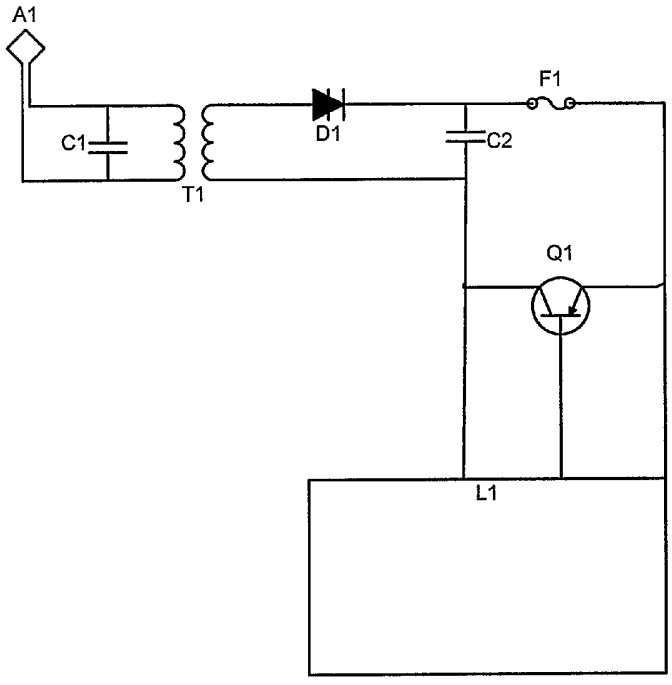
(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, EG, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT (utility model), PT, RO, RU, SC, SD, SE, SG, SK (utility model), SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

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.

(54) Title: DEACTIVATION OF RADIO FREQUENCY IDENTIFICATION TAGS



(57) Abstract: In regular operation, the tag receives energy from antenne (A1), which is fed resonant circuit comprising of capacitor C1 and an inductor which is a portion of (T1). Energy captured from the secondary winding of (T1) is rectified by diode (D) and filtered by capacitor (C2). The energy collected is used to power the tag. It should be noted that this power supply arrangement is but one simplified arrangement of many known methods of providing power to the tag.

WO 2004/053721 A1

Deactivation of Radio Frequency Identification tags

Field of the invention

[0001] The invention is directed to the field of RFID tags and more particularly to deactivation of such tags.

Background

[0002] Attaching tags containing information to products is becoming increasingly popular. Technologies such a RFID (Radio Frequency Identification) tags allow relatively large amount of information to be attached or embedded within an item. Tags may be broadly divided into two categories: passive or active tags. Active tags contain a power source, while passive tags are being supplied energy from an external source for their operation. The tag may be interrogated by a device that will be referred to in these specifications as an interrogator.

[0003] The interrogator generates an interrogation signal that both energizes passive tags, and queries the tag without the need for direct contact. The interrogation signal has predetermined characteristics, e.g. a preset frequency or data content, which activates the tag. Passive tags receive energy from the interrogation signal e.g. by use of a resonant circuit tuned to resonate at the preset frequency, where the energy derived from the circuit is used to power the tag. A small transmitter in the tag transmits data stored in the tag, responsive to activation or other interrogation. Other methods of transmitting the data such as back scatter and the like are also known. Passive tags may be energized and activated by several methods, however a passive tag has to receive the energy from an interrogator or from another source external thereto. Thus a passive tag must have circuitry to collect energy from a remote source.

[0004] The use of such tags offers a wide range of advantages to manufacturers and retailers, such as ease of stock management, and prevention of theft in stores. Many other uses have also been contemplated, including a 'global

tag' (GTAG) standard for presenting information in a uniform manner to operators worldwide. For simplicity of demonstrating the present invention, the use of tracking consumer products will be used by way of non-limiting example, as deactivation of tags may be useful in many other applications within the envisioned uses of such tags.

[0005] The use of tags in this context suffers from two major disadvantages: the first is the effects of undesirable interrogation after a product is purchased. As the information in the tag may be read unbeknown to the purchaser, a significant threat to personal privacy is presented. By way of example, the tag may be attached to an article of clothing, and include such data as size and price information. If a person wearing the article of closing is being interrogated by a competitor's interrogator, a significant embarrassment may result. Even more threatening to personal privacy, is unauthorized use of such interrogators to find out more personal information about a person such as what medications a person is carrying, taste in products not readily visible, and the like.

[0006] A second concern in addition to the privacy concern, is what shall be referred to hereinafter as 'radiation pollution'. It is clear that in time the proliferation of tags will cause numerous responses from undesirable tags: tags other than the tags the interrogator directed its signal to. For example, if an interrogator is installed at the entrance to a store, many old tags, i.e. tags of previously purchased items, may be present in the interrogator field of operation. The signal from such old tags will cause a significant noise problem that may interfere with the operation of the 'desired' tag. Additionally, the energy absorbed by old tags may deplete the available energy and preventing the activation of the desirable tag.

[0007] US 6,480,110 to Lee et al teaches tuning an antenna of an RFID tag by melting, or blowing open, fusible links. By doing so, the electrical length of an inductor is modified to cause it to resonate at a desired frequency.

[0008] There is however a need for capacity to deactivate a tag after it performed its intended purpose. The present invention is directed to providing a solution to this problem.

Brief Description

[0009] In its most basic embodiment, the invention comprises a data transmitting tag having a deactivation arrangement, in hardware or in software, wherein the deactivation arrangement is operable responsive to a deactivation signal.

[0010] Two primary solutions are envisioned for deactivating the tag. The first involves sending a signal that will cause the tag to stop transmitting data or alter the data it is transmitting. The second revolves about disabling a portion or all of the tag circuitry.

[0011] The first solution contemplated above may be achieved by sending a signal to be received by the tag, that will cause it to permanently stop sending out data stored therein. Such solution may be achieved for example by setting a flag within the memory of the tag that will prevent the tag from responding to future interrogations. Thus an aspect of the invention comprises a tag having a controller embedded therein, said controller being operative, responsively to a command, to set a condition that will disable future responses to interrogations. In a preferable embodiment of this aspect of the invention, the controller is a programmable controller and the condition is set as a software flag being tested in future interrogation cycles. Responsive to the flag, the tag may send an indication that the data content has been blocked. Yet even more preferably, the tag will not respond at all to future interrogations. Another method is the erasure of data from the tag responsive to the deactivating signal.

[0012] While this solution solves the problems identified above it is not the most preferred solution. A tag having only its data transmitting capacity disabled still consumes energy when being exposed to an interrogation signal. If only a portion of the data transmitting capacity is disabled, than other

signals are still being transmitted, and the problem of noise pollution is merely reduced. It is therefore more desirable to disable the circuitry of the tag, or a portion of that circuitry, so as to minimize or eliminate power consumption by the tag, and even more preferably, to disable resonance by the tag circuitry at the interrogation frequency.

[0013] Thus in a preferred embodiment of the invention there is provided a data transmitting tag comprising a deactivation circuitry for deactivating the tag or a portion thereof, said circuitry operable responsively to deactivation command received by the tag. Preferably, the circuitry comprising a fusible link and a controllable short. The controllable short being connected to cause, when operational, sufficient current in the fusible link that will cause the link to become an open circuit. The fusible link being operative to disable the tag or a portion thereof. In a more preferred embodiment the fusible link is connected to the power supply portion of a tag. In the most preferable embodiment, the fusible link is located within the resonant antenna circuit of the tag. In yet another embodiment, the circuitry is operable to permanently modify the tag operating parameters so as to modify the resonant frequency of the tag resonant circuit. Those skilled in the art will recognize that several methods for doing so are well known, such as changing capacitance or inductance in the resonant circuit, causing permanent change in operating parameters of a circuit component, e. g. raising resistance of a resistor, destroying a semiconductive junction, and the like. Disablement methods are known that electrically activate a chemical material to disrupt circuitry operation, and the invention extends thereto.

[0014] It should be noted that this system is operable on passive as well as active types of tags.

[0015] In another aspect of the invention there is provided a method for deactivating a data transmitting tag comprising the steps of transmitting a deactivating signal to a tag; and activating within the tag, a deactivation arrangement responsive to reception of said deactivation signal, wherein

said deactivation arrangement being constructed to prevent the tag from sending data in response to future interrogations. The deactivation arrangement may be implemented in software, by setting a flag to prevent future responses or provide only partial responses, or by erasing the data in the tag. However, in a preferable embodiment, the deactivation arrangement is done by hardware. Such deactivation circuit may be implemented for example by disablement of a selected component of the tag, preferably directly connected to the tag power supply circuit, and even more preferably to the tag resonant circuitry.

[0016] Yet another aspect of the invention is to provide a tag that may be read after disablement as described herein, by directly coupling such tag or a portion thereof, to a specialized reader.

Brief description of the drawings

[0017] Fig. 1 depicts circuitry to affect a preferred embodiment of a tag operative in accordance with the invention.

[0018] Fig. 2 depicts circuitry to affect the most preferred embodiment of tag operative in accordance with the invention.

[0019] Fig. 3 depicts flow diagram in accordance to several aspects of the invention.

Detailed Description

[0020] Presently, most RFID tag variants are coupled inductively to the interrogator. However capacitive coupling operates in a similar fashion, and the invention extends to such coupling. Similarly light operated coupling is yet another known method. In the case of passive tags, a single coupling may be utilized to power or the tag and communicate therewith. Alternatively, two separate coupling methods may be employed, one for powering the tag e.g. inductive, capacitive, light activation, and the like, and a separate coupling for communication with the tag. Generally, every coupling such as radio frequency radiating, is appropriate for use in the invention.

[0021] To assist in understanding the invention, the following specifications are directed at passive tags that receive their energy from an RF radiated interrogation signal. Such tag may be divided into three major component areas: A resonant circuit, a power supply and a logic portion.

[0022] The resonant circuit comprises an antenna and some sort of an inductive/capacitive circuit adapted to resonate at a known frequency range. Oftentimes the antenna is an integral part of the resonant circuit, and sometimes parasitic capacity is utilized for tuning the circuit to the desired frequency. While not strictly a portion of the resonant circuit, for the purpose of these specifications, other transmitting and receiving components that allow the tag to receive or transmit data are considered herein as a portion of the resonant circuit.

[0023] The power supply utilizes energy collected by the resonant circuit to power the rest of the tag. Such power supply commonly operates by rectifying the energy received by the resonant circuit. As described above the power supply may be separate from the resonant circuit, such as for example by utilizing light sensitive power cells, while communications occurs via a separate path.

[0024] The logic portion is the heart of the RFID tag. It typically comprises memory of some sort, and a controller adapted to perform operations such as responding to interrogation signals, deal with communication protocols, run an application, transmit data, receive data, store data, and the like.

[0025] Several software embodiments of software based tag deactivation will be apparent to those skilled in the art once the need for such deactivation is made clear by these specifications. In a first software based embodiment of the invention, the tag is programmed to stop responding to future interrogations. This may be achieved by setting a flag in the memory 350 and in response to future interrogations check if the flag is set 360 and transmit data 370 only when it is not set. Optionally, the tag data may be erased 340 responsive to the deactivating signal.

[0026] A more preferred embodiment of the invention is depicted in Fig. 1. In regular operation, the tag receives energy from antenna A1, which is fed to resonant circuit comprising of capacitor C1 and an inductor which is a portion of T1. Energy captured from the secondary winding of T1 is rectified by diode D1 and filtered by capacitor C2. The energy collected is used to power the tag. It should be noted tat this power supply arrangement is but one simplified arrangement of many known methods of providing power to the tag. This method was selected merely for simplicity of explanation. It is recognized however that in practical use many tags utilize a far simpler power supply arrangement in order to reduce cost, increase efficiency, and the like. While many arrangements are known for collecting energy and utilizing it to power the tag, the invention extends to all such arrangements, as well as to active tags which carry their own power supply.

[0027] Logic L1 is provided to activate Q1 which acts as controllable short. Responsive to a deactivation signal received from the transmitting antenna, the logic causes Q1 to conduct in such a way as to cause the fusible link F1 to permanently change state to an open circuit (commonly known as 'blowing' the fuse). Thus the tag is permanently deactivated.

[0028] The role of Q1 may be achieved by many devices such as, but not limited to, triac, SCR, UJT, micro relay, or any other component characterized by causing high current to blow the fusible link F1 when the component or a combination of components is activated.

[0029] It will also be clear to those skilled in the art that fusible link F1 is merely a convenience. It may indeed be implemented a fuse, but may also be implemented as an active or passive component that becomes a path of high resistance preventing normal tag operation, or as a path of low resistance, preventing tag operation by short circuiting of one or more critical tag components. The fusible link may even be implemented directly within the shorting element itself. Thus for example Q1 may become a permanent short that prevents proper operation of the tag even without a

fusible link F1, as it becomes the deactivating device. An example of such arrangement may be made by making a transistor having a base layer that will be deactivated once sufficient current flows through Q1. Additional disablement methods are known, such as electrically activating a chemical that will disable the tag.

[0030] While this implementation has the advantage of disabling the tag from operation, it still allows the tag to collect energy from the transmitting antenna. A better embodiment is provided by the example depicted in Fig. 2. In it, the deactivation occurs by disconnecting a portion of the resonant circuit, or otherwise detuning it. By doing so, the circuit will not draw any significant energy from the activating interrogator.

[0031] While it is possible to detune or otherwise deactivate the resonant circuit by short-circuiting it, it is preferable to create an open circuit, such as the one that will occur if Q1 is activated by the logic L1 to cause fusible link F1 to open.

[0032] Fig. 3 depicts a simplified flow diagram where responsive to receiving a deactivation signal 310 the deactivation arrangement is operated 320. The specific manner in which deactivation occurs is dependent on the manner in which the tag is deactivated and is a matter of technical choice such as burning a fuse 330 erasing the data 340 or by software as described above.

[0033] When the information in the tag is not needed further, (e.g. after the item the device is coupled to is sold) a deactivation signal is sent to the tag, and the tag becomes disabled. In order to prevent unintended (or malicious) deactivation, it is preferable that a deactivation signal be an encoded signal. Such encoding may be at least partially derived from information within the tag, or a deactivation may be kept as the prerogative of authorized interrogators, as required. Thus the deactivation event itself may be reported to an interested party, such as the report of a sale to a manufacturer.

[0034] It is sometimes desirable to have access to the data after the tag has been disabled. Such a case is when, for example, the customer attempts to return the tag to the store. If the arrangement in Fig. 2 is utilized, it is possible to connect power to points of contact Pa and Pb, and thus read the tag. Because the resonant circuit is still disabled, the tag needs to be removed and read by placing it into a specialized reader. However doing so will be normally done with the client consent. Clearly other methods of reading the a tag data are available, such as powering the tag from different points, removing a portion of the tag for direct reading, software reversal in case of software disablement, and the like. However as the capacity to read the data remotely is removed, the customer has greater control of such operations.

[0035] It will be clear to those skilled in the art that the logical divisions provided above are but one example of how to make the invention, and that one skilled in the art would be able to divide the provided functionality in many ways and circuit designs, given the flexible nature of electronics, once the need for the invention is made clear as described above. However the invention is clearly directed at covering such modifications and equivalents as will be clear to those skilled persons, and not limited to the logical block arrangement, or other aspects of the description and drawings provided by way of none limiting example only.

What is claimed is:

1. A data transmitting tag capable of containing data and transmitting said data upon inquiry signal, said tag comprising a hardware disablement arrangement, operable responsive to a deactivation signal, said deactivation arrangement being operable to disable a portion of electrical circuitry of said tag to prevent transmission of the data or a portion thereof.
2. A data transmitting tag as claimed in claim 1 wherein said deactivation arrangement is constructed to cause alteration or destruction of at least a portion of the circuitry of said tag.
3. A data transmitting tag as claimed in claims 1 or 2, wherein said hardware is constructed to alter at least the data stored in the tag, or erase at least a portion of the data of said tag, or a combination thereof.
4. A data transmitting tag as claimed in any preceding claim wherein said deactivation arrangement is constructed to alter or destroy a portion of the tag circuit responsible for transmission of data.
5. A data transmitting tag as claimed in any preceding claim wherein said portion of the tag circuitry is an antenna.
6. A data transmitting tag as claimed in any preceding claim wherein said deactivation arrangement is constructed to alter or destroy a portion of the tag circuit responsible for reception of operating energy.
7. A data transmitting tag as claimed in any preceding claim wherein said portion of the tag circuitry is an antenna.
8. A data transmitting tag as claimed in any preceding claim wherein said tag is further adapted to allow transmission of the data stored therein in response to connection to reactivation inquiry device.
9. A data transmitting tag as claimed in any preceding claim adapted for transmitting blank data in response to said inquiry signal after receiving said deactivation signal.

10. A data transmitting tag as claimed in any preceding claim wherein said tag further comprises a transmitting circuitry and wherein said deactivation signal is constructed to, in response to a disablement signal, alter or destroy at least a portion of said transmitting circuitry.

11. A data transmitting tag as claimed in claim 10, wherein said portion of the transmitting circuitry is an antenna.

12. A data transmitting tag as claimed in any preceding claim wherein said tag further comprises a controller and wherein said deactivation signal is constructed to, in response to a disablement signal, alter or destroy at least a portion of said controller.

13. A data transmitting tag as claimed in any preceding claim wherein said tag further comprises a receiving circuitry and wherein said deactivation signal is constructed to, in response to a disablement signal, alter or destroy at least a portion of said receiving circuitry.

14. A data transmitting tag as claimed in claim 13, wherein said receiving circuitry further comprises energy receiving circuitry for energizing said tag and wherein said disablement arrangement is constructed to disable or alter the characteristics of said antenna.

15. A data transmitting tag as claimed in any preceding claim, wherein the deactivation arrangement comprises a fusible link and a controllable short, the controllable short being connected to cause, when operational, sufficient current in the fusible link that will cause the link to become an open circuit, and the fusible link is being operative to disable the tag or a portion thereof.

16. A data transmitting tag as claimed in any preceding claim, further comprising a resonant circuit, and wherein said deactivation arrangement is constructed to modify or destroy at least a portion of said resonant circuit.

17. A data transmitting tag capable of containing data and transmitting said data upon inquiry signal, said tag comprising a hardware disablement arrangement, operable responsive to a deactivation signal, said deactivation arrangement being operable to disable a portion of electrical circuitry of said tag to prevent transmission of the data or a portion thereof.

18. A data transmitting tag as claimed in claim 14, wherein said disablement signal is encoded.

19. A data transmitting tag capable of containing data and transmitting said data upon inquiry signal, said tag comprising a hardware disablement arrangement, operable responsive to an encoded deactivation signal, said deactivation arrangement being operable to prevent transmission of the data or a portion thereof in response to future inquiry signals.

20. A data transmitting tag as claimed in claim 19, wherein said deactivation arrangement comprises software.

21. A data transmitting tag as claimed in claim 20, wherein said software is operable to alter and/or erase said data or a portion thereof.

22. A data transmitting tag as claimed in any of claims 19-21, further comprising a reactivation software constructed to allow transmission of said data or a portion thereof in response to an encoded reactivation signal.

23. A data transmitting tag as claimed in any of claims 19-22 wherein said tag is adapted to transmit an indication that the tag has been deactivated.

24. A method for deactivating a data transmitting tag comprising the steps of:

transmitting a deactivating signal to a tag;

activating within the tag, a deactivation arrangement responsive to reception of said deactivation signal;

altering the circuitry of the tag or a portion thereof by said deactivation arrangement, so as to prevent the tag from transmitting the or a portion thereof in response to future inquiry signals.

25. A method for deactivating a data transmitting tag as claimed in claim 24, wherein said deactivation signal is encoded.

26. A method for deactivating a data transmitting tag as claimed in claims 24 or 25, wherein said step of altering is carried out to modify the characteristics of a resonant circuit within the tag, and/or an antenna.

27. A method for deactivating a data transmitting tag comprising the steps of:

transmitting an encoded deactivating signal to a tag;

activating within the tag, a deactivation arrangement responsive to reception of said deactivation signal, so as to prevent the tag from transmitting the or a portion thereof in response to future inquiry signals.

28. A method for deactivating a data transmitting tag as claimed in claim 27, wherein said deactivation arrangement comprises software.

29. A method for deactivating a data transmitting tag as claimed in claim 27, wherein said software is operable to alter and/or erase said data or a portion thereof.

30. A method for deactivating a data transmitting tag as claimed in any of claims 27-29, further comprising the step of transmitting an encoded reactivation signal, to allow transmission of said data or a portion thereof in response to said reactivation signal.

31. A data transmitting tag as claimed in any of claims 27-29, further comprising the steps of:

a. interrogating said tag for data stored therein;

b. encoding said deactivation signal in accordance with the data received in said step of interrogating.

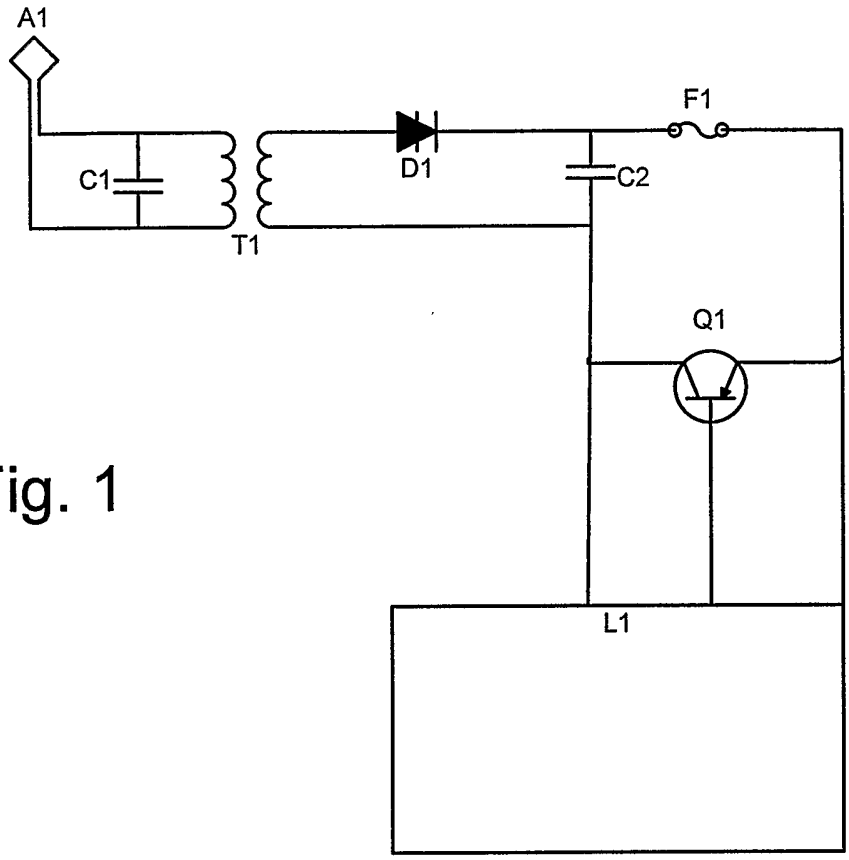


Fig. 1

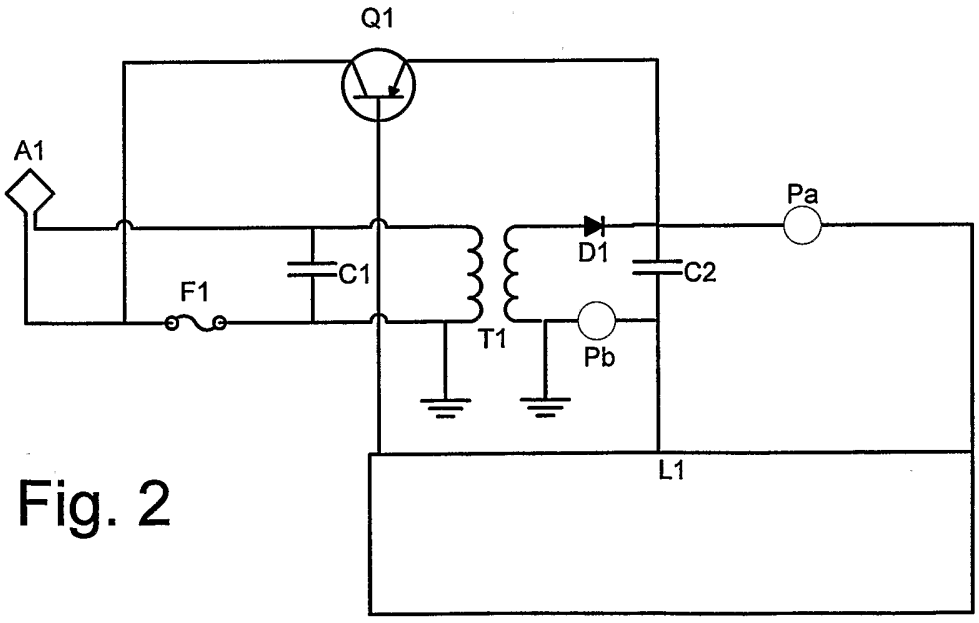


Fig. 2

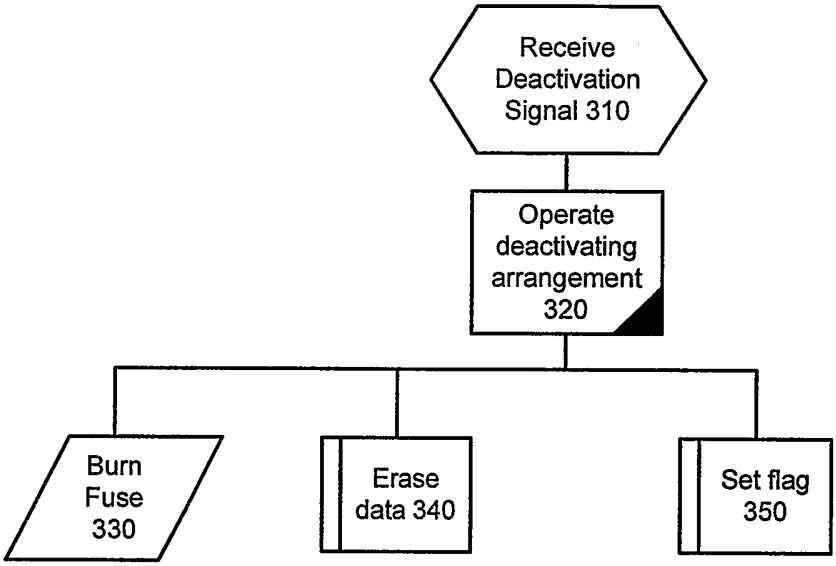
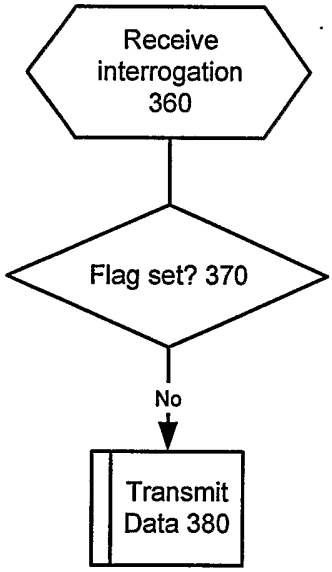

Receive Deactivation Signal 310
Operate deactivating arrangement 320
Burn Fuse 330
Erase data 340
Set flag 350

Fig. 3


Receive interrogation 360
Flag set? 370
No
Transmit Data 380

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/38609

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 17/00
US CL : 700/238; 340/572.5

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)
U.S. : 700/238; 340/572.5

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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6,480,110 B2(LEE et al.) 12 November 2002 (12.11.2002), Whole Document.	1, 24 and 27
Y	US 5,963,134 A (BOWERS et al.) 5 October 1999 (05. 10.1999), Whole document.	1-31
Y	US 6,025,780 A (BROWERS et al.) 15 February 2000 (15.02.2000), Whole Document.	1-31

☐ 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 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
17 March 2004 (17.03.2004)

Date of mailing of the international search report
26 MAR 2004

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703)305-3230

Authorized officer
Michelle K. Eason
for
Leo Picard

Telephone No. (703) 308-0538

Form PCT/ISA/210 (second sheet) (July 1998)