US007872582B1

(12) **United States Patent**
Diorio

(10) **Patent No.: US 7,872,582 B1**
(45) **Date of Patent: *Jan. 18, 2011**

(54) **RFID TAG CHIPS AND TAGS WITH ALTERNATIVE MEMORY LOCK BITS AND METHODS**

(75) Inventor: **Christopher J. Diorio**, Shoreline, WA (US)

(73) Assignee: **Impinj, Inc.**, Seattle, WA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 344 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **11/872,774**

(22) Filed: **Oct. 16, 2007**

Related U.S. Application Data

(60) Provisional application No. 60/853,994, filed on Oct. 24, 2006.

(51) **Int. Cl.**

G08B 13/14	(2006.01)
G08B 13/26	(2006.01)
G06F 13/00	(2006.01)
G06F 13/28	(2006.01)
G11C 5/14	(2006.01)

(52) **U.S. Cl.** **340/572.1**; 711/154; 711/156; 340/825.34; 340/825.54; 340/572.9; 340/5.61; 340/10.51; 340/10.1; 340/5.74; 340/539.11; 340/5.25; 365/195; 365/228

(58) **Field of Classification Search** ... 340/572.1–572.9, 340/568.1, 540, 500, 825, 5.1, 5.2, 5.8, 5.81–5.86; 365/195, 189.07, 189.011; 711/154, 156
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,506,329	A *	3/1985	Duwel et al.	705/410
5,175,837	A *	12/1992	Arnold et al.	711/152
5,394,367	A *	2/1995	Downs et al.	365/195
5,467,081	A *	11/1995	Drews et al.	340/5.22
5,513,136	A *	4/1996	Fandrich et al.	365/185.04
5,809,553	A *	9/1998	Choi et al.	711/170
5,874,896	A	2/1999	Lowe et al.	
6,031,757	A *	2/2000	Chuang et al.	365/185.04
7,007,145	B2 *	2/2006	Schrodinger et al.	711/164
7,108,183	B1	9/2006	Cox, Jr.	
7,167,090	B1	1/2007	Mandal et al.	
7,321,300	B2 *	1/2008	Friedrich et al.	340/539.11
2004/0246103	A1	12/2004	Zukowski	
2005/0073197	A1	4/2005	Matsubara et al.	

(Continued)

OTHER PUBLICATIONS

EPCglobal, Inc "Specification of RFID Air Interface-EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz-960 MHz, Version 1.1.0." (*a.k.a. "The Gen 2 Spec"*) *EPCglobal Inc.* Dec. 17, 2005.

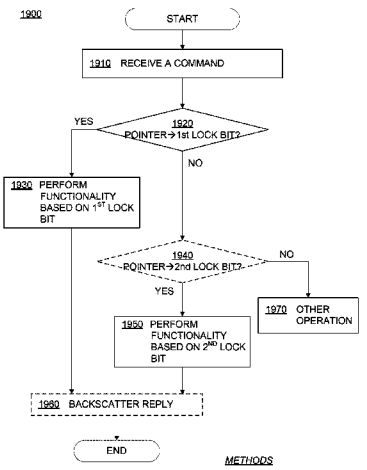
(Continued)

Primary Examiner—Brian A Zimmerman
Assistant Examiner—An T Nguyen
(74) *Attorney, Agent, or Firm*—Turk IP Law, LLC

(57) **ABSTRACT**

RFID tag circuits, tags, and methods are provided for using alternative memory lock bits. A pointer in tag memory is configured to point to one or the other of the alternative lock bits associated with a section of the memory for performing a function in response to a reader command. Upon receiving the reader command, the tag first checks the pointer and performs the function based on which lock bit(s) is selected.

19 Claims, 18 Drawing Sheets



U.S. PATENT DOCUMENTS

2005/0270141	A1*	12/2005	Dalglish	340/10.4
2007/0008070	A1*	1/2007	Friedrich	340/10.1
2007/0176756	A1*	8/2007	Friedrich	340/10.51
2007/0199988	A1	8/2007	Labgold et al.	
2007/0273481	A1*	11/2007	Soleimani	340/10.1
2007/0276985	A1*	11/2007	Schuessler	711/100
2008/0001724	A1*	1/2008	Soleimani et al.	340/10.51
2008/0001725	A1*	1/2008	White et al.	340/10.51
2008/0012685	A1*	1/2008	Friedrich et al.	340/5.25
2008/0034183	A1*	2/2008	Drago et al.	711/219
2008/0129506	A1*	6/2008	Schuessler	340/572.1

OTHER PUBLICATIONS

EPCglobal, Inc "Specification of RFID Air Interface-EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz-960 MHz, Version 1.0.8." (*a.k.a. "The Gen 2 Spec"*) *EPCglobal Inc*. Dec. 14, 2004.

"Specification for RFID Air Interface: EPCTM Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocols for Communications at 860 MHz—960 MHz Version 1.2.0. 2004-2008", *EPCglobal Inc*. Oct. 23, 2008, 1-108.

Specification for RFID Air Interface: EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocols for Communications at 860 MHz—960 MHz Version 1.2.0. 2004-2008 EPCglobal Inc. Oct. 23, 2008: 1-108.

"Declaration of Stacy L. Jones authenticating attached website materials", www.autoid.org/SC31/sc_31_wg4_sg3.htm Sep. 1, 2006.

Non-Final Office Action U.S. Appl. No. 11/877,054 mailed Oct. 2, 2009.

Non-Final Office Action U.S. Appl. No. 11/877,054 mailed Mar. 9, 2010.

* cited by examiner

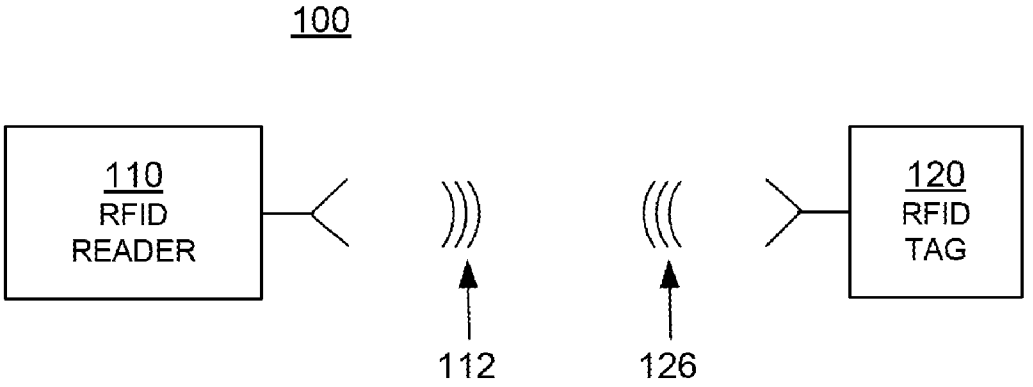

100
110
RFID
READER
120
RFID
TAG
112
126
RFID SYSTEM

FIG. 1

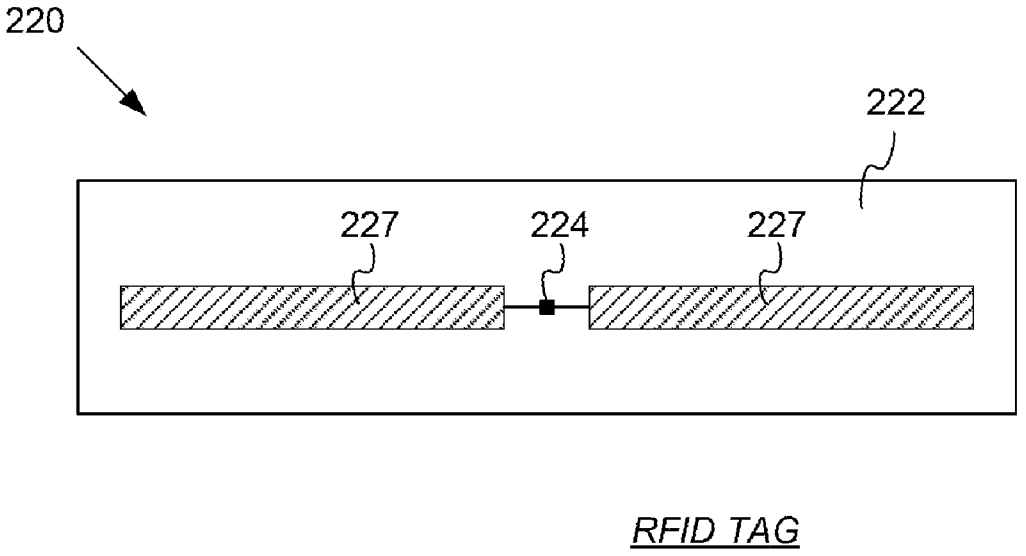
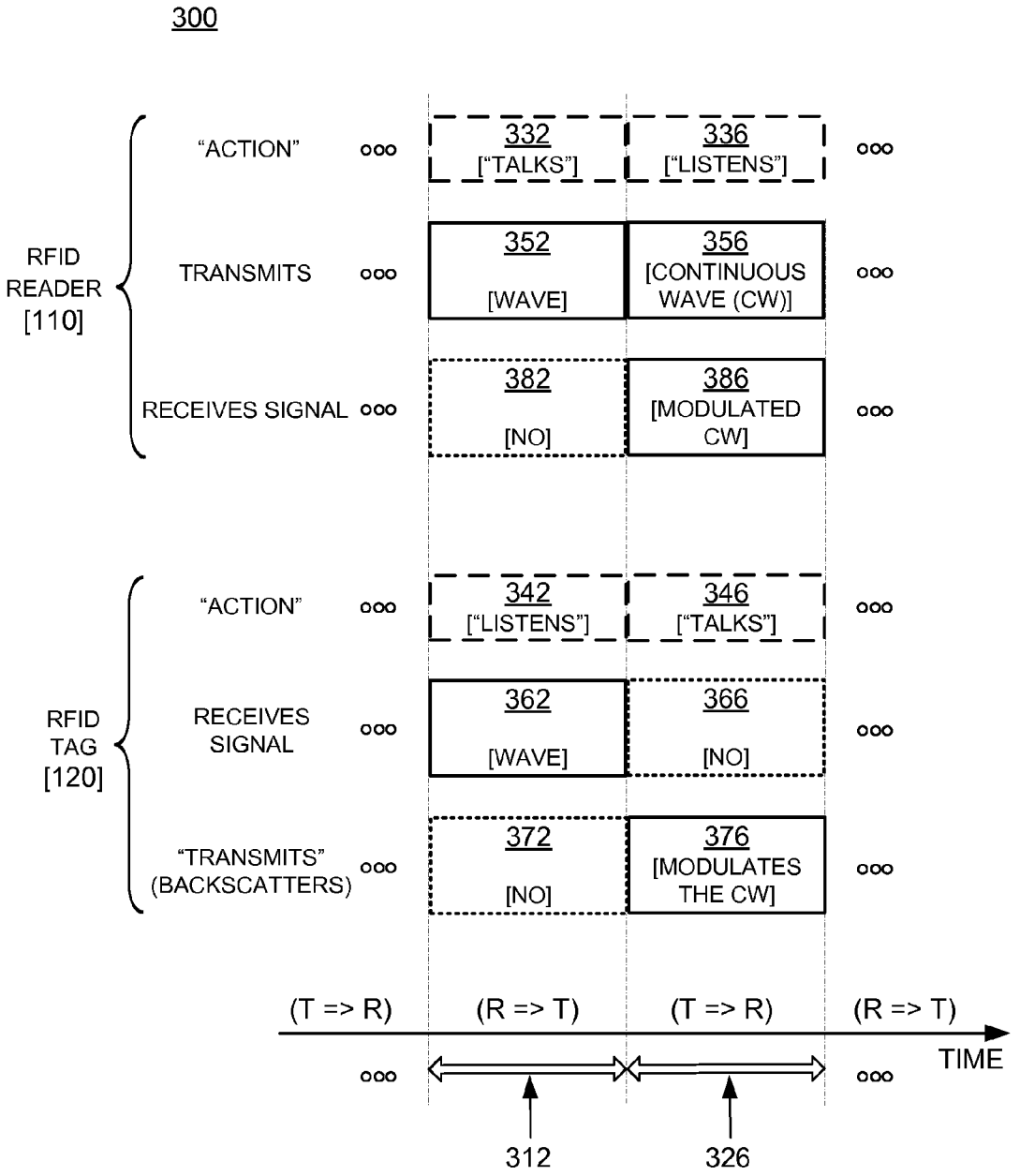

220
222
227
224
227
RFID TAG

FIG. 2



RFID SYSTEM COMMUNICATION

FIG. 3

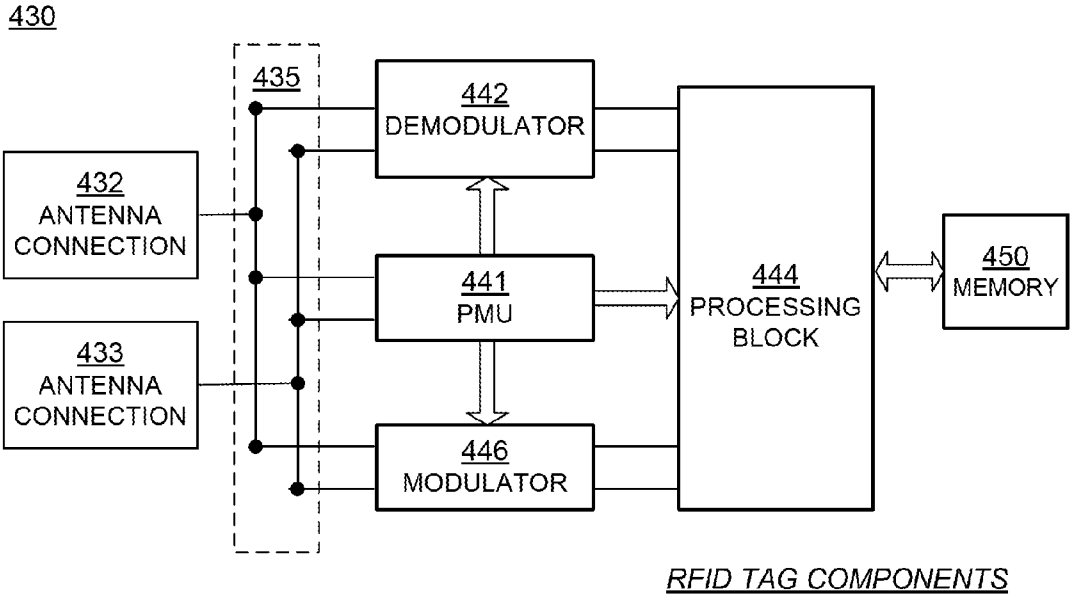


FIG. 4

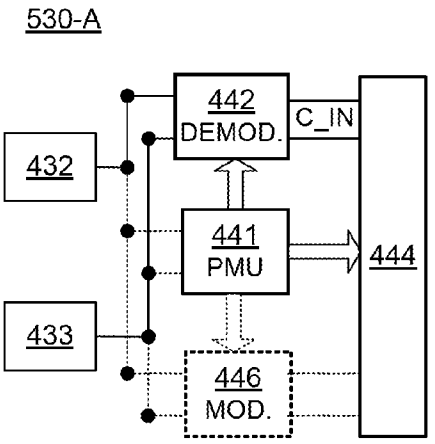


FIG. 5A

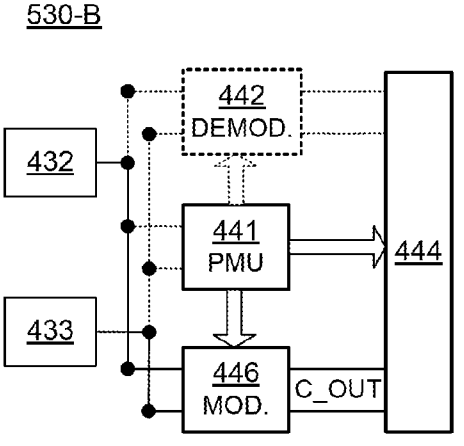


FIG. 5B

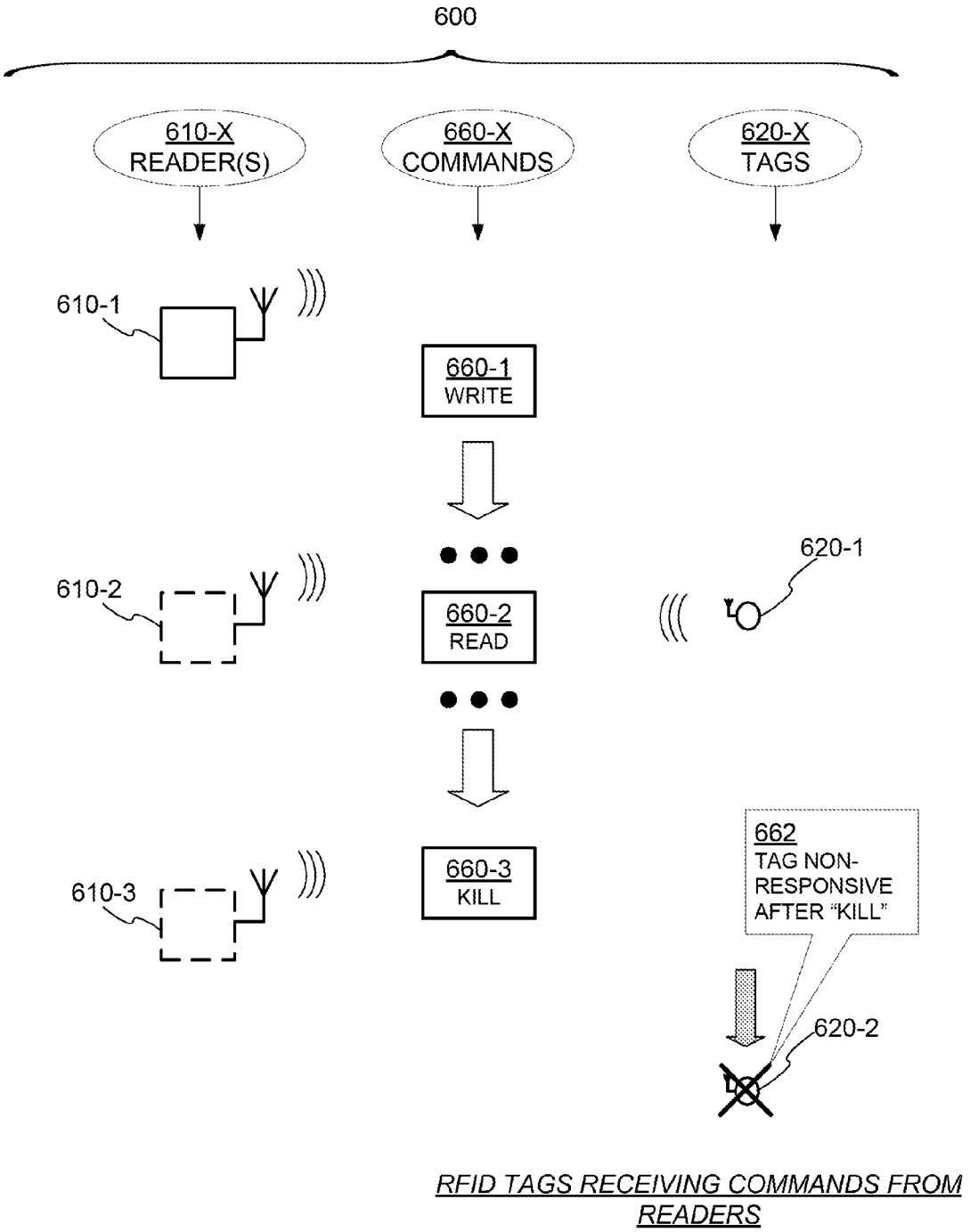
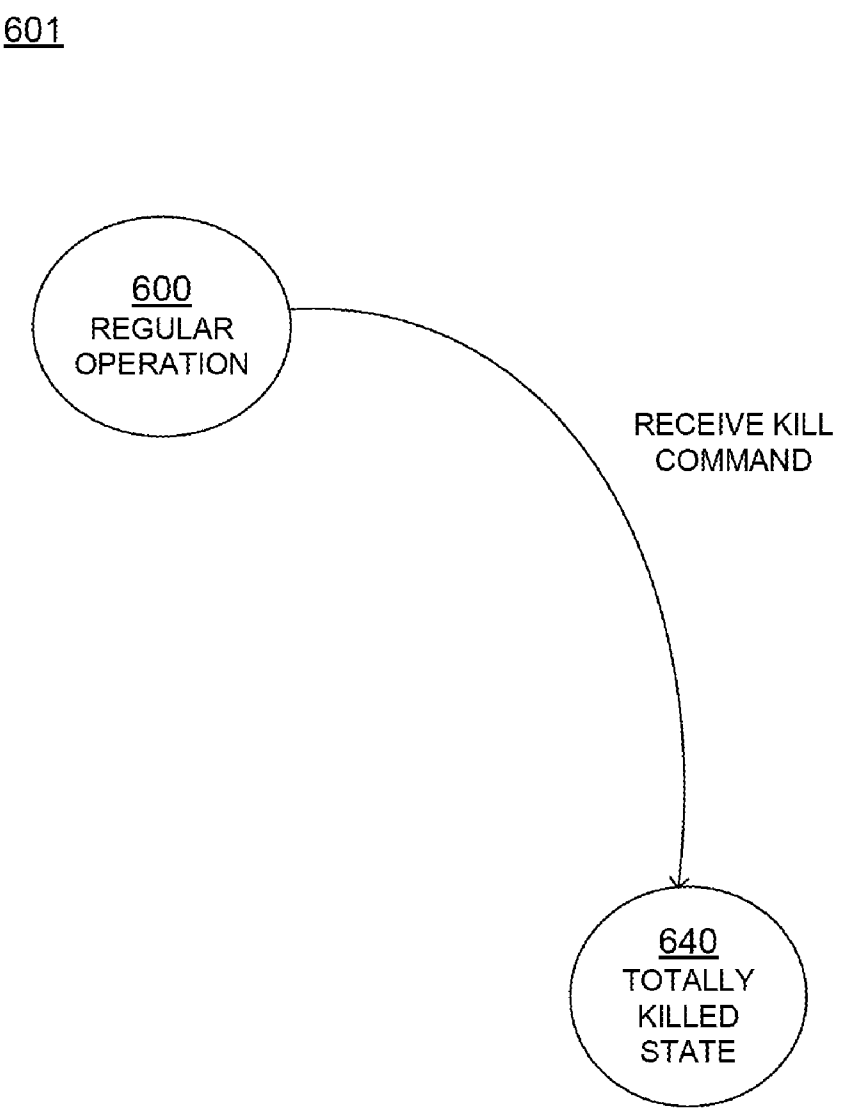


FIG. 6A (PRIOR ART)



TAG STATE DIAGRAM

FIG. 6B (PRIOR ART)

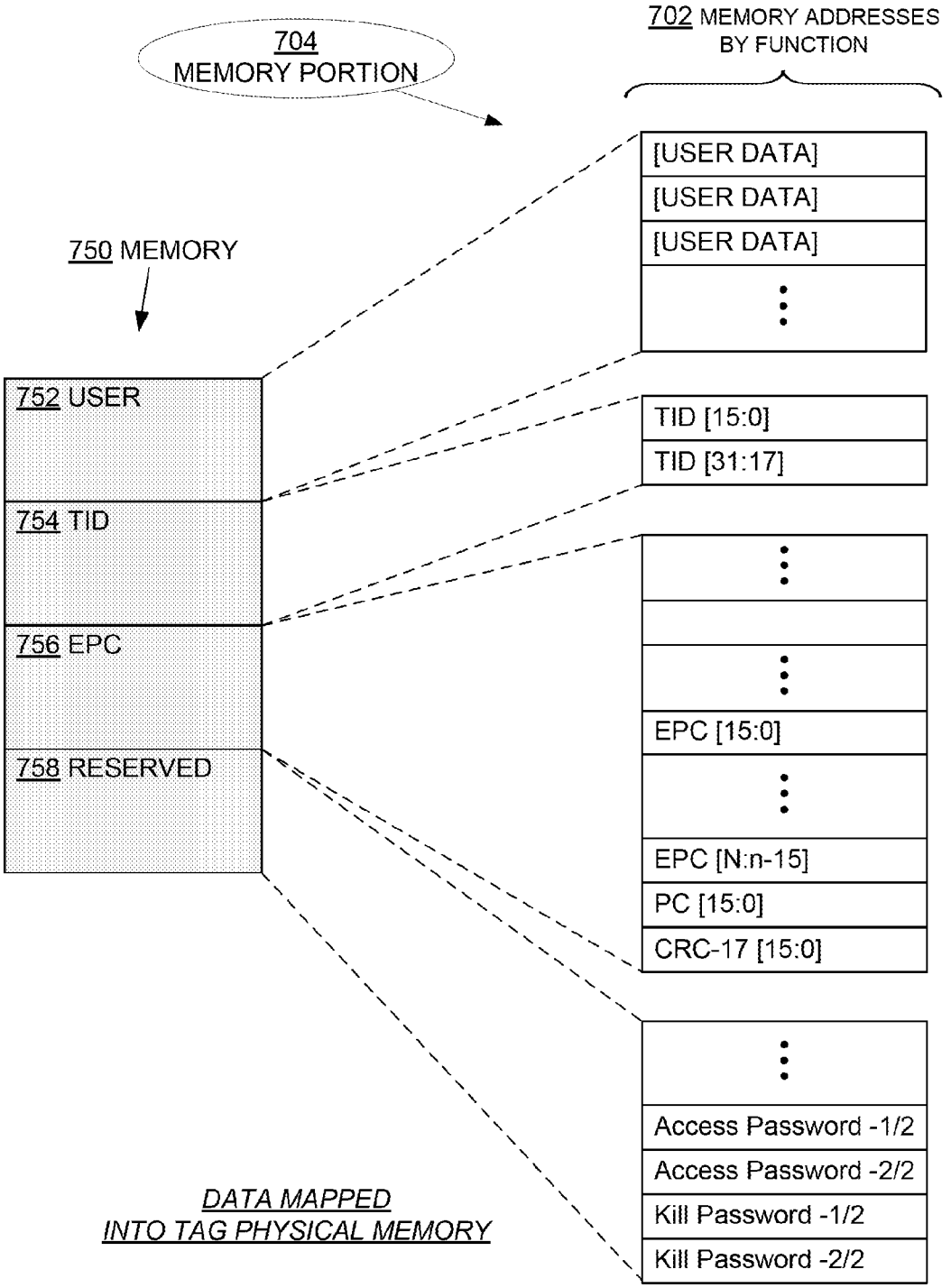
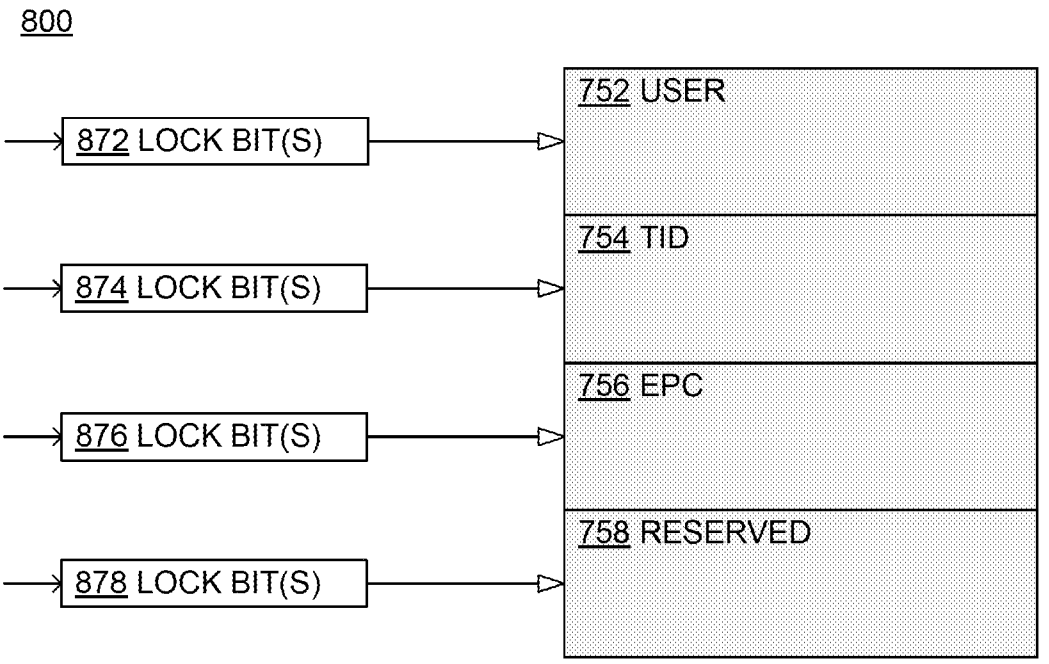


FIG. 7 (PRIOR ART)



MEMORY WITH DEDICATED LOCK BITS

FIG. 8 (PRIOR ART)

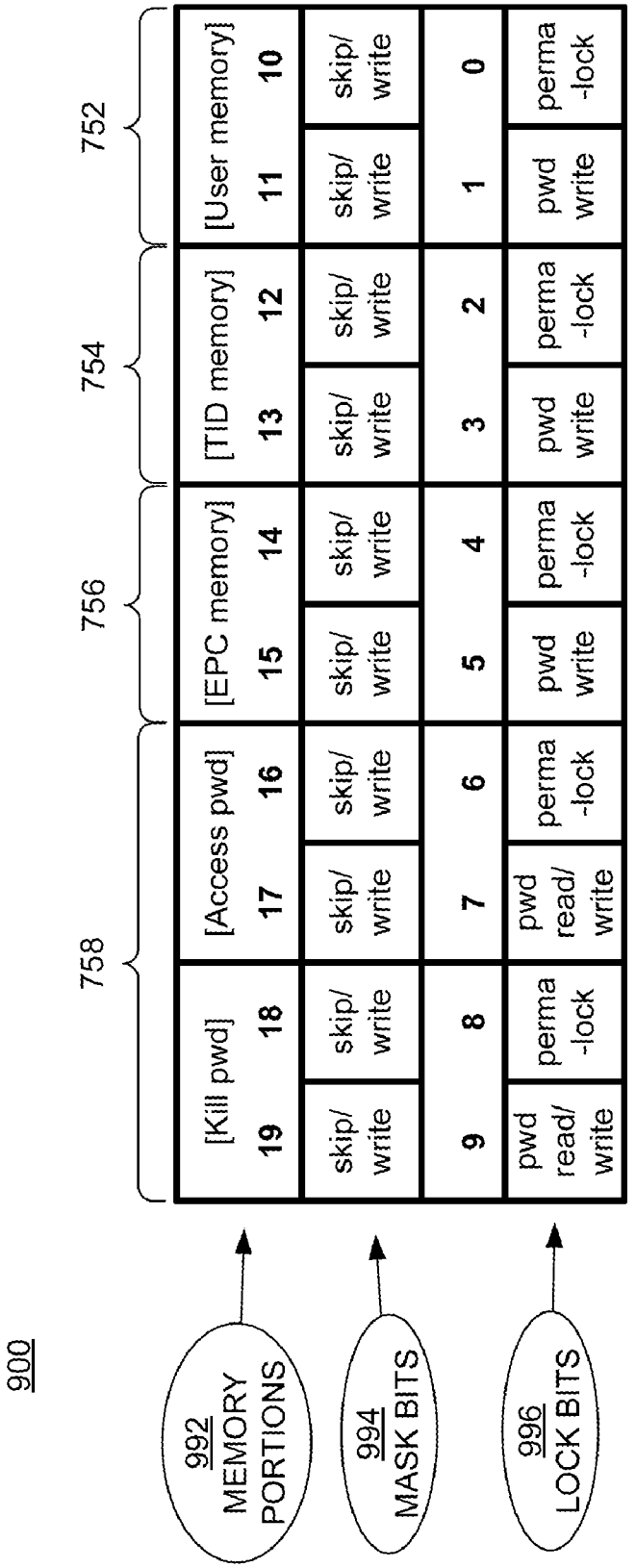


FIG. 9 (PRIOR ART)

EXAMPLE PAYLOAD OF A "LOCK" COMMAND

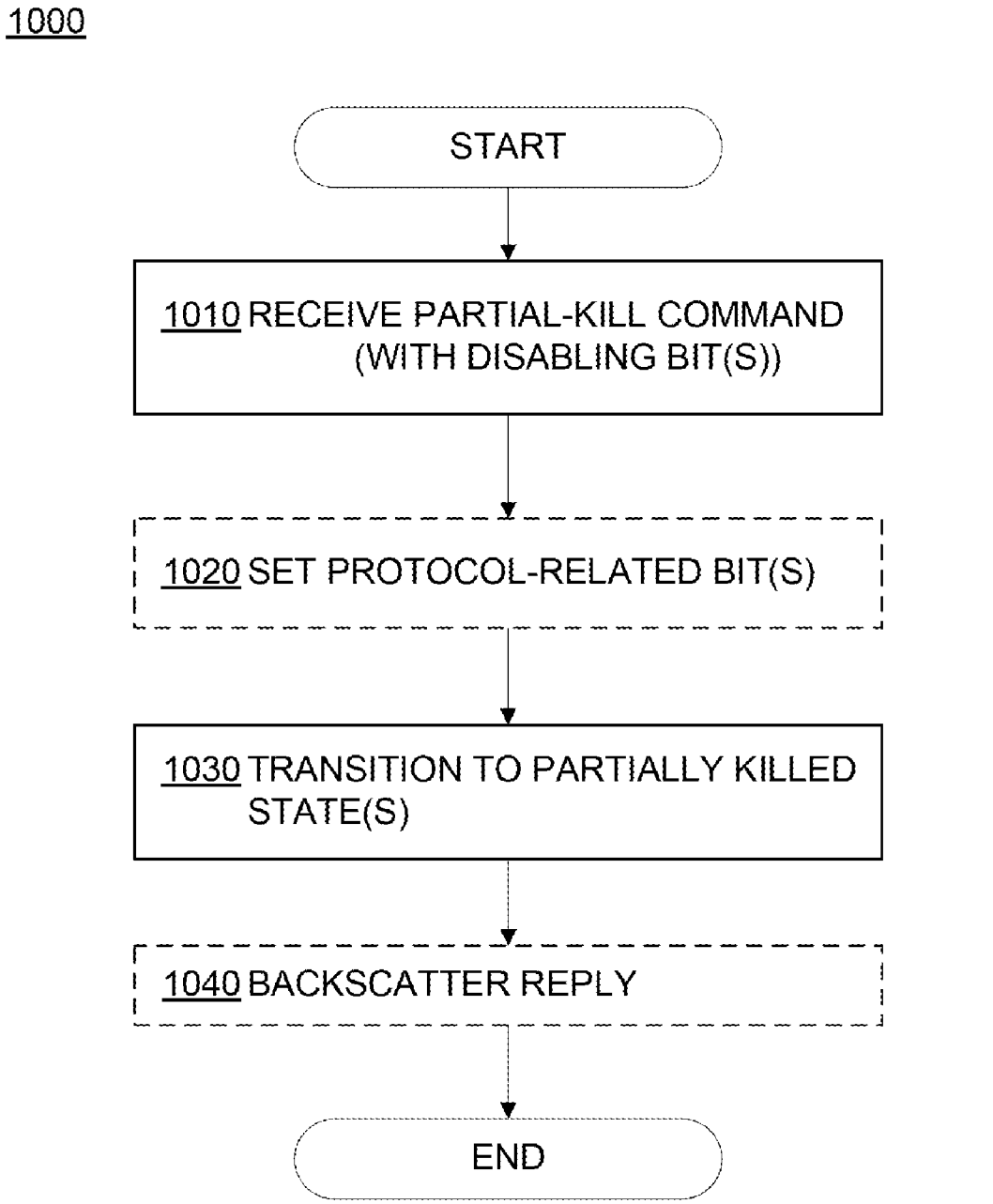
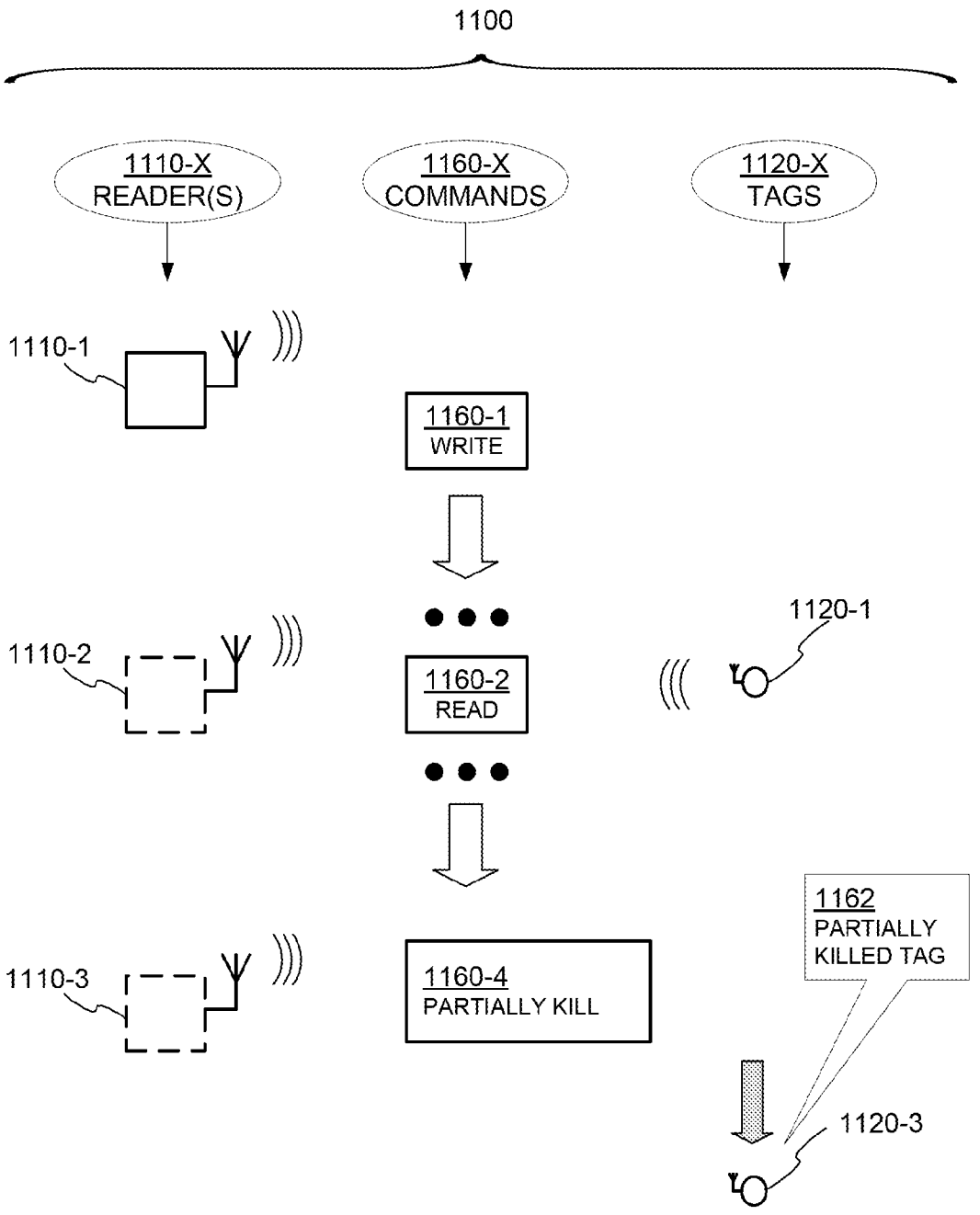

1000
START
1010 RECEIVE PARTIAL-KILL COMMAND (WITH DISABLING BIT(S))
1020 SET PROTOCOL-RELATED BIT(S)
1030 TRANSITION TO PARTIALLY KILLED STATE(S)
1040 BACKSCATTER REPLY
END
METHODS

FIG. 10



RFID TAGS BEING PARTIALLY KILLED

FIG. 11

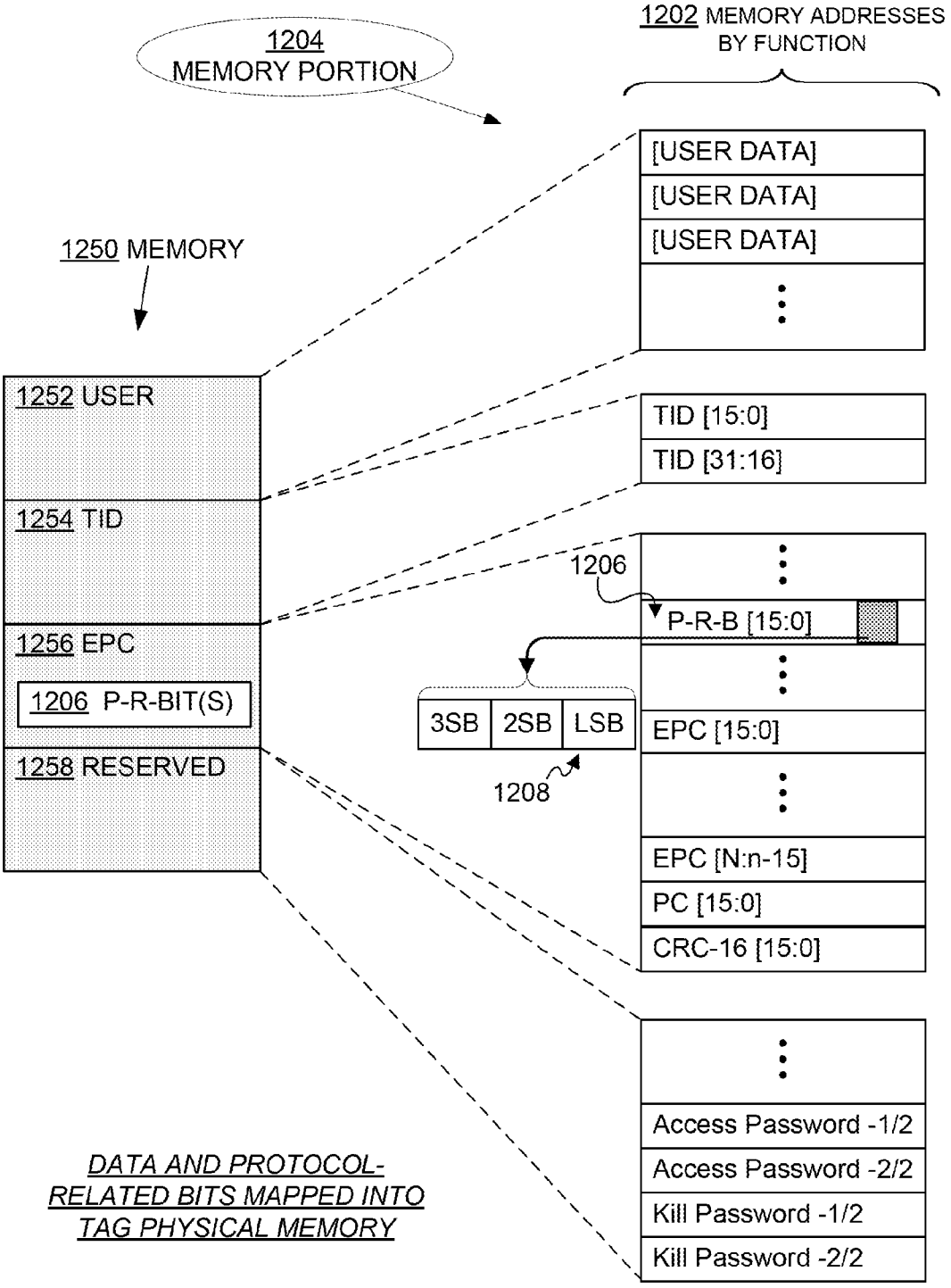
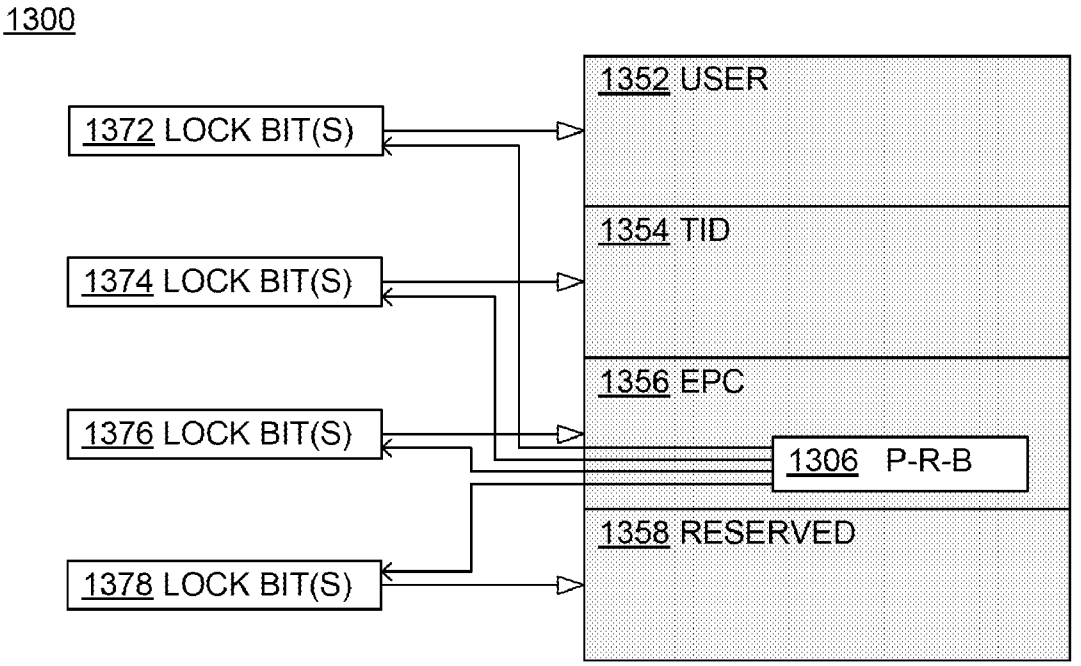
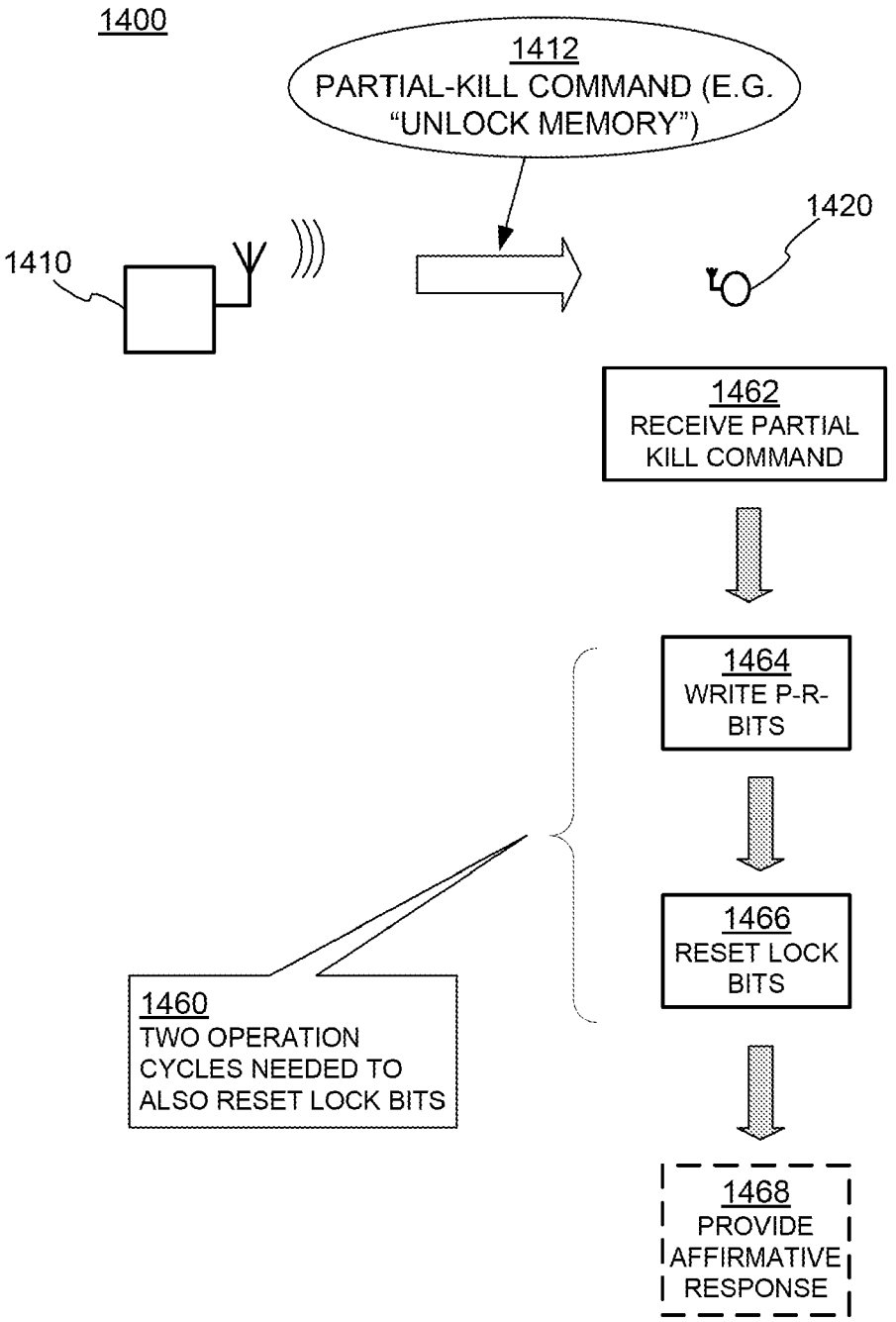

1204
MEMORY PORTION
1202 MEMORY ADDRESSES
BY FUNCTION
1250 MEMORY
1252 USER
1254 TID
1256 EPC
1206 P-R-BIT(S)
1258 RESERVED
[USER DATA]
[USER DATA]
[USER DATA]
TID [15:0]
TID [31:16]
1206
P-R-B [15:0]
3SB
2SB
LSB
1208
EPC [15:0]
EPC [N:n-15]
PC [15:0]
CRC-16 [15:0]
Access Password -1/2
Access Password -2/2
Kill Password -1/2
Kill Password -2/2
DATA AND PROTOCOL-
RELATED BITS MAPPED INTO
TAG PHYSICAL MEMORY

FIG. 12



MEMORY WITH DEDICATED MEMORY LOCK BITS

FIG. 13



RFID TAGS RESETTING MEMORY LOCK BITS UPON RECEIVING PARTIAL KILL COMMAND

FIG. 14

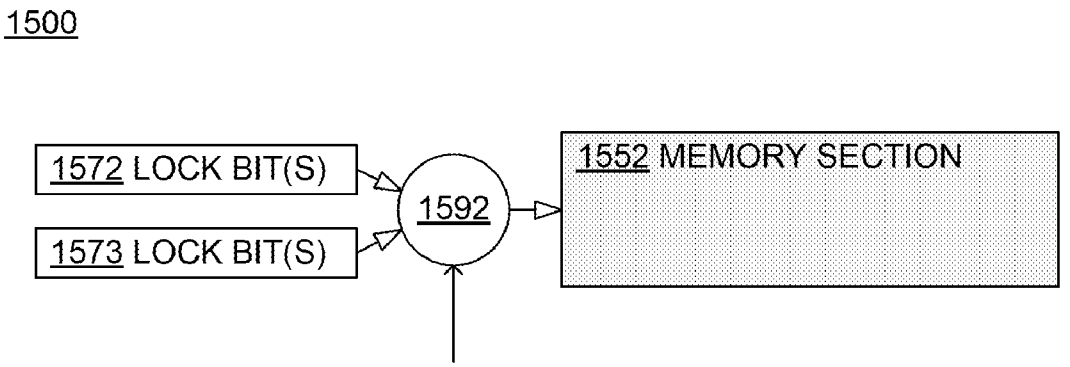

1500
1572 LOCK BIT(S)
1573 LOCK BIT(S)
1592
1552 MEMORY SECTION
MEMORY WITH ALTERNATIVE LOCK BITS

FIG. 15

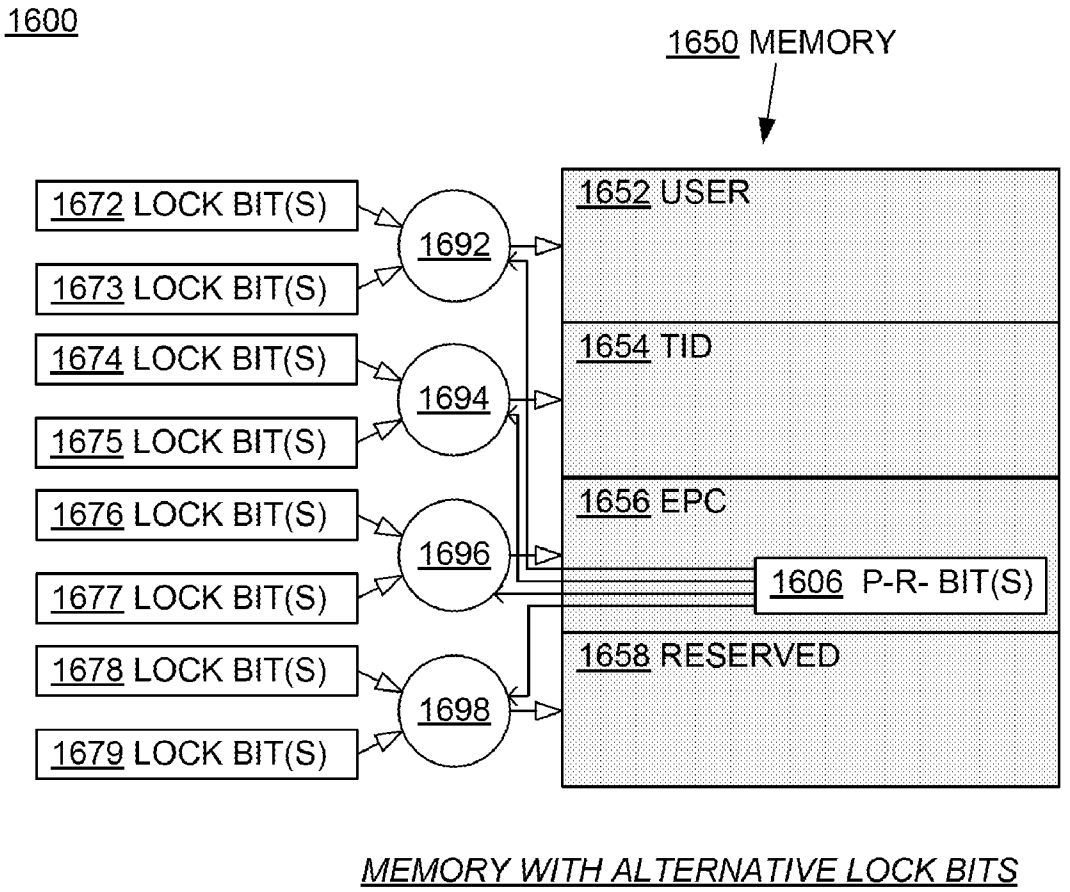
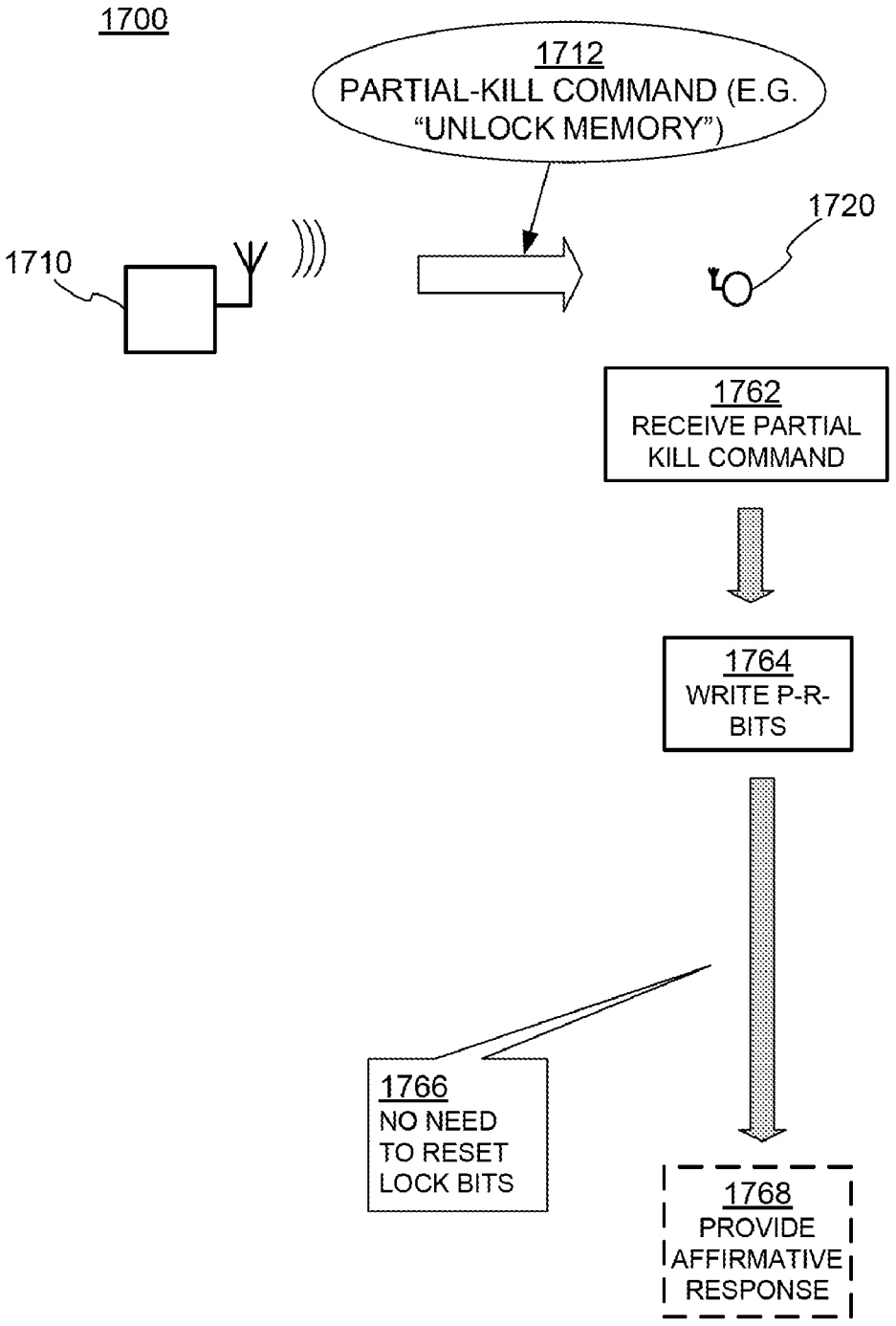

1600
1650 MEMORY
1672 LOCK BIT(S)
1673 LOCK BIT(S)
1674 LOCK BIT(S)
1675 LOCK BIT(S)
1676 LOCK BIT(S)
1677 LOCK BIT(S)
1678 LOCK BIT(S)
1679 LOCK BIT(S)
1692
1694
1696
1698
1652 USER
1654 TID
1656 EPC
1606 P-R- BIT(S)
1658 RESERVED
MEMORY WITH ALTERNATIVE LOCK BITS

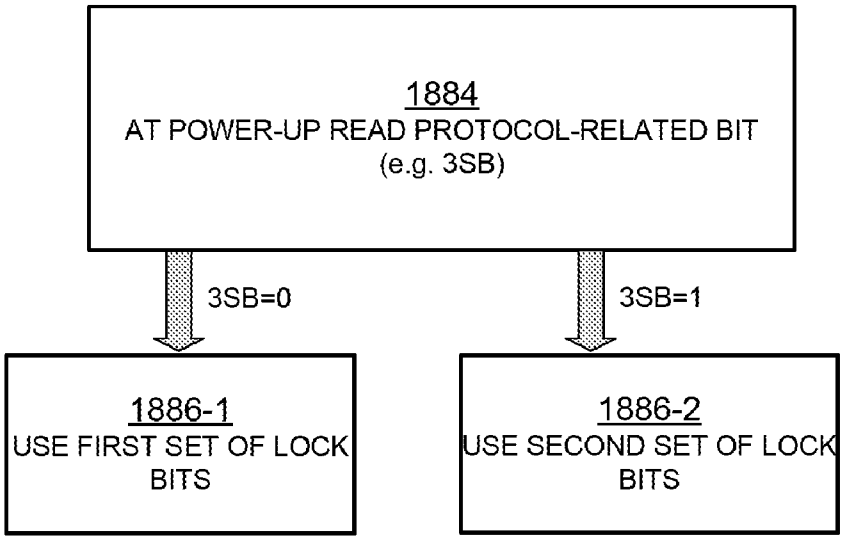
FIG. 16



RFID TAGS RESETTING MEMORY LOCK BITS UPON RECEIVING PARTIAL KILL COMMAND

FIG. 17

1800



RFID TAGS CHOOSING DIFFERENT SETS OF LOCK BITS AT POWER-UP

FIG. 18

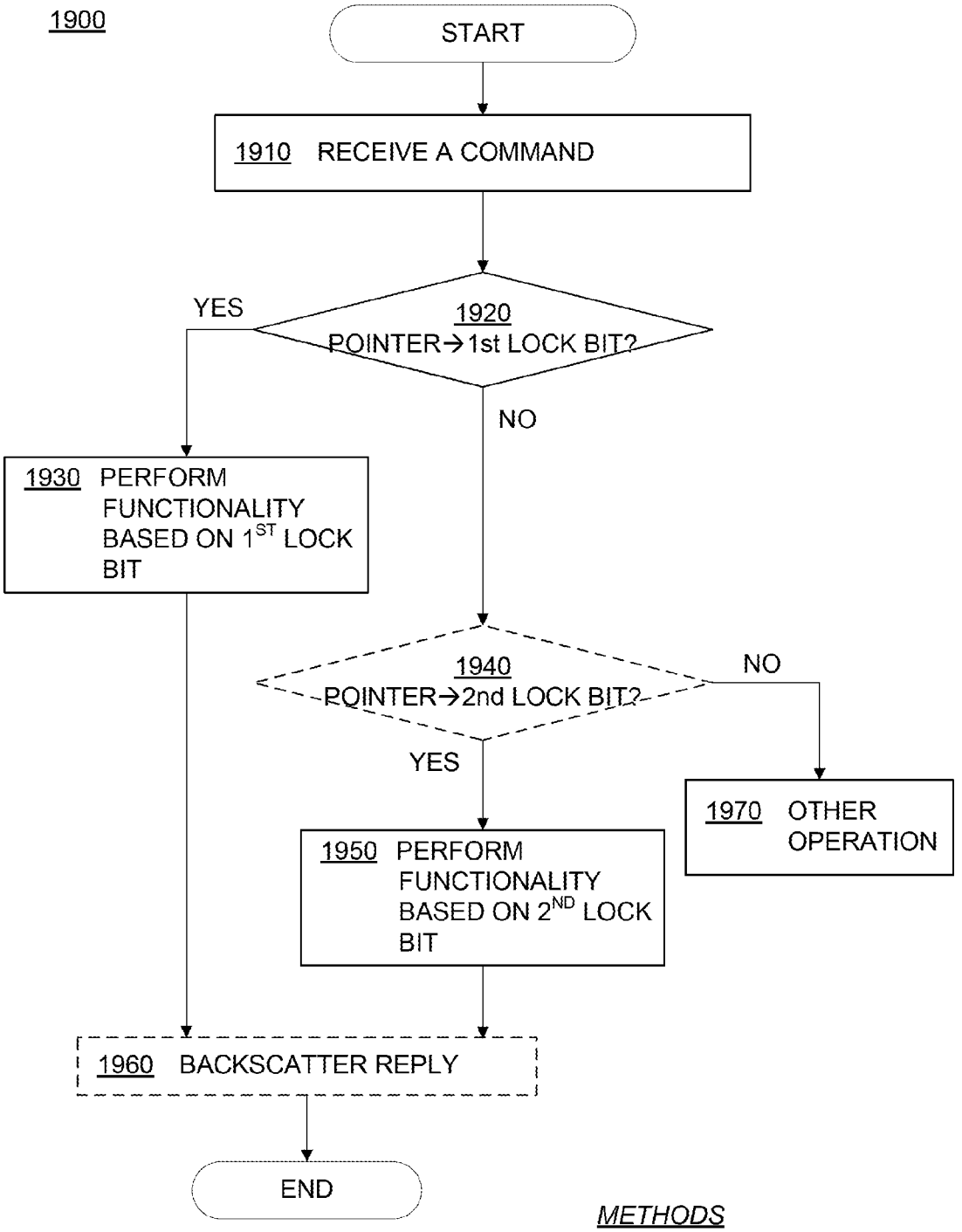

1900
START
1910 RECEIVE A COMMAND
YES
1920
POINTER→1st LOCK BIT?
NO
1930 PERFORM FUNCTIONALITY BASED ON 1ST LOCK BIT
1940
POINTER→2nd LOCK BIT?
NO
YES
1970 OTHER OPERATION
1950 PERFORM FUNCTIONALITY BASED ON 2ND LOCK BIT
1960 BACKSCATTER REPLY
END
METHODS

FIG. 19

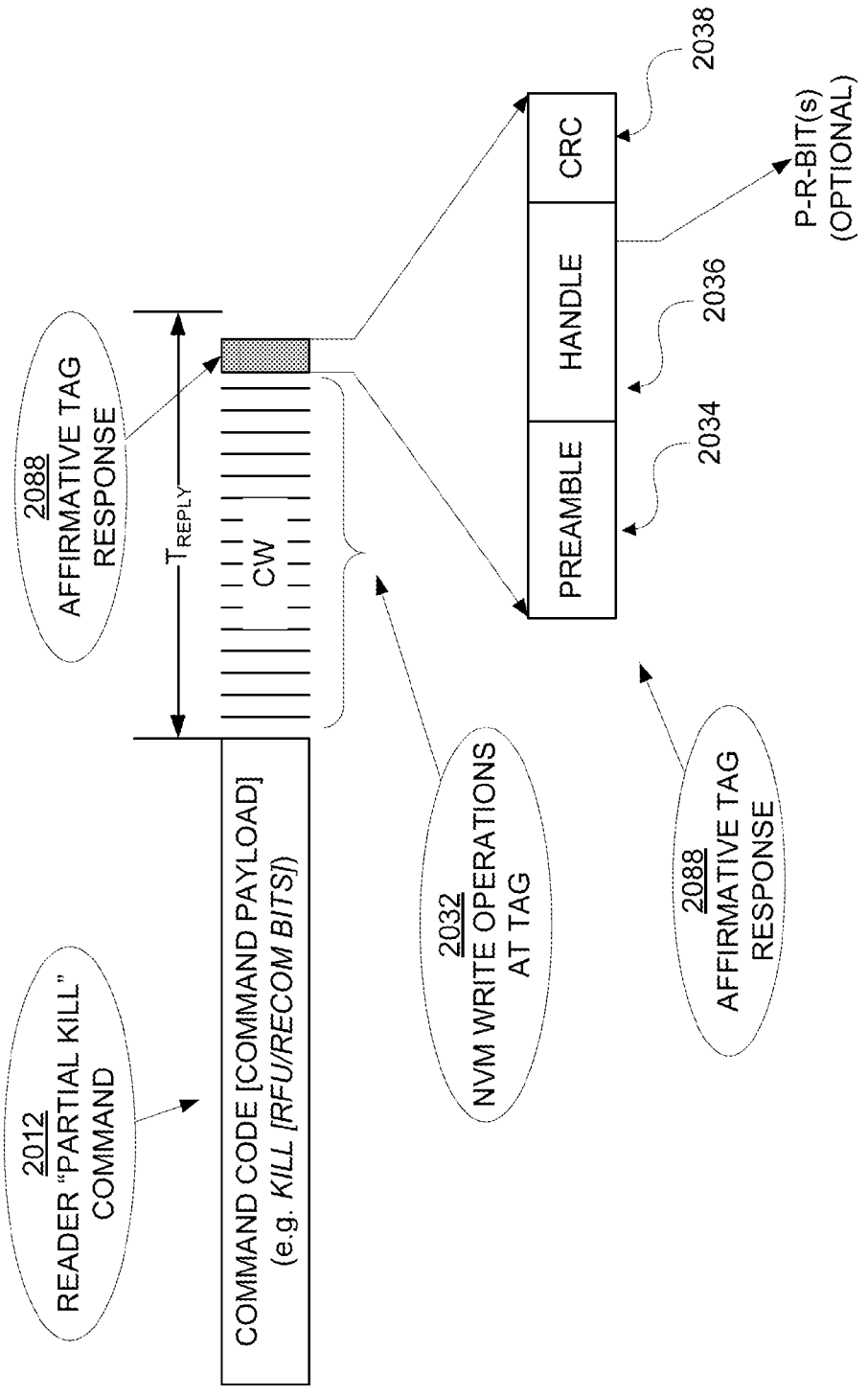


FIG. 20

NVM WRITE OPERATIONS IN RESPONSE TO DISABLING BITS (e.g. RFU/RECOM) IN READER COMMAND AND TAG RESPONSE

RFID TAG CHIPS AND TAGS WITH ALTERNATIVE MEMORY LOCK BITS AND METHODS

RELATED APPLICATIONS

This utility patent application claims the benefit of U.S. Provisional Application Ser. No. 60/853,994 filed on Oct. 24, 2006, which is hereby claimed under 35 U.S.C. §119(e). The provisional application is incorporated herein by reference.

This utility patent application have a portion of its specification in common with U.S. patent application Ser. No. 11/852,439 (IMPJ-0245) filed on Sep. 10, 2007. The benefit of the earlier filing date of the parent applications is hereby claimed under 35 U.S.C. §120.

This utility patent application may have a portion of its specification in common with U.S. patent application Ser. No. 11/877,054 filed on Oct. 23, 2007, titled "RFID TAG CHIPS AND TAGS ARRANGING PROTOCOL-RELATED BIT AND LOCK BIT IN SINGLE NVM MEMORY WORD AND METHODS."

BACKGROUND

Radio Frequency IDentification (RFID) systems typically include RFID tags and RFID readers (the latter are also known as RFID reader/writers or RFID interrogators). RFID systems can be used in many ways for locating and identifying objects to which the tags are attached. RFID systems are particularly useful in product-related and service-related industries for tracking large numbers of objects being processed, inventoried, or handled. In such cases, an RFID tag is usually attached to an individual item, or to its package.

In principle, RFID techniques entail using an RFID reader to interrogate one or more RFID tags. The reader transmitting a Radio Frequency (RF) wave performs the interrogation. A tag that senses the interrogating RF wave responds by transmitting back another RF wave. The tag generates the transmitted back RF wave either originally, or by reflecting back a portion of the interrogating RF wave in a process known as backscatter. Backscatter may take place in a number of ways.

The reflected-back RF wave may further encode data stored internally in the tag, such as a number. The response is demodulated and decoded by the reader, which thereby identifies, counts, or otherwise interacts with the associated item. The decoded data can denote a serial number, a price, a date, a destination, other attribute(s), any combination of attributes, and so on.

An RFID tag typically includes an antenna system, a power management section, a radio section, and frequently a logical section, a memory, or both. In earlier RFID tags, the power management section included an energy storage device, such as a battery. RFID tags with an energy storage device are known as active or semi-active tags. Advances in semiconductor technology have miniaturized the electronics so much that an RFID tag can be powered solely by the RF signal it receives. Such RFID tags do not include an energy storage device, and are called passive tags.

A tag may have multiple functionalities, some of which are associated with the information stored in different portions of its memory. It may be possible to disable some of those functionalities using a "Kill" command. For example, the user memory portion of the tag memory may be disabled at a Point-Of-Sale (POS) terminal. Kill operations are usually permanent and irreversible, even though it may be desirable to revive the disabled functionality or functionalities at a later

date. Lock bits may also be used in blocking (or killing) portions of the tag memory for certain functionalities permanently or temporarily.

SUMMARY

This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter.

Embodiments are directed to RFID tag circuits, tags, and methods for using alternative lock bits in determining how a functionality associated with a section of tag memory is to be performed in response to a reader command. A pointer may be employed to indicate which set of the lock bits are to be used. The functionality of the memory section may then be performed based on the indicated lock bits.

This and other features and advantages of the invention will be better understood in view of the Detailed Description and the Drawings, in which:

BRIEF DESCRIPTION OF THE DRAWINGS

Non-limiting and non-exhaustive embodiments are described with reference to the following drawings.

FIG. **1** illustrates a typical RFID system with an RFID reader and an RFID tag;

FIG. **2** is a diagram of an RFID tag such as the RFID tag shown in FIG. **1**;

FIG. **3** is a conceptual diagram for explaining a half-duplex mode of communication between the components of the RFID system of FIG. **1**;

FIG. **4** is a block diagram illustrating one embodiment of an electrical circuit that may be employed in an RFID tag such as the RFID tag of FIG. **1**;

FIGS. **5**A and **5**B illustrate two versions of the electrical circuit of FIG. **4** emphasizing signal flow in receive and transmit operational modes of the RFID tag, respectively;

FIG. **6**A is a conceptual diagram illustrating different commands transmitted by one or more readers including a "Kill" command rendering a tag unusable;

FIG. **6**B is an example tag state diagram illustrating transition of a tag from an operational state to a totally killed state upon receiving a "Kill" command;

FIG. **7** is a diagram illustrating how a tag's physical memory such as the memory shown in FIG. **4** can be partitioned and organized for data to be mapped onto it, also in compliance with the Gen2 Specification;

FIG. **8** is a diagram illustrating how lock bits can be used to control access of the partitioned and organized memory of FIG. **7**, also in compliance with the Gen2 Specification;

FIG. **9** illustrates an example payload of a "Lock" command that can be applied to control the memory lock bits of the memory of FIG. **8**, also in compliance with the Gen2 Specification;

FIG. **10** is a flowchart of an RFID tag becoming partially killed;

FIG. **11** is a conceptual diagram illustrating different commands transmitted by one or more readers and a "Partial Kill" command causing a tag to become partially killed as per FIG. **10**;

FIG. **12** is a diagram illustrating how a tag's physical memory such as the memory shown in FIG. **7** can be partitioned and organized for data to be mapped into it, including the protocol-related bits;

FIG. **13** is a diagram illustrating how lock bits can be used to control access of a memory that is partitioned and organized as the memory of FIG. **12**, and in which further the lock bits are controlled by protocol-related bits that are mapped within the controlled memory;

FIG. **14** is a conceptual diagram illustrating how an RFID tag with a memory partitioned and organized as in the memory of FIG. **12** could reset its memory lock bits upon receiving a "Partial Kill" command, and also for describing a problem;

FIG. **15** is a block diagram illustrating a memory section whose access is controlled by one or more alternative lock bits according to embodiments;

FIG. **16** is a block diagram illustrating a memory that is partitioned into sections and organized as the memory of FIG. **12**, and where further access to each of these sections is controlled by one or more alternative lock bits according to embodiments;

FIG. **17** is a conceptual diagram illustrating how an RFID tag with a memory partitioned and organized as in the memory of FIG. **12** could automatically reset its memory lock bits upon receiving a partial-kill command, because there are alternative memory lock bits as per the embodiment of FIG. **16**;

FIG. **18** is a conceptual diagram illustrating how an RFID tag could chose among memory lock bits at power-up, as may have been determined by resetting them upon receiving the partial-kill command of FIG. **14**;

FIG. **19** is a flowchart for illustrating a method of an RFID tag responding to a command by using a set of lock bits chosen as illustrated with reference to FIG. **16** as per embodiments of the invention;

FIG. **20** is a diagram illustrating a reader command and corresponding tag response with a payload that includes protocol-control bits for disabling, according to embodiments.

DETAILED DESCRIPTION

Various embodiments will be described in detail with reference to the drawings, where like reference numerals represent like parts and assemblies throughout the several views. Reference to various embodiments does not limit the scope of the invention, which is limited only by the scope of the claims attached hereto. Additionally, any examples set forth in this specification are not intended to be limiting and merely set forth some of the many possible embodiments for the claimed subject matter.

Throughout the specification and claims, the following terms take at least the meanings explicitly associated herein, unless the context clearly dictates otherwise. The meanings identified below are not intended to limit the terms, but merely provide illustrative examples for the terms. The meaning of "a," "an," and "the" includes plural reference, the meaning of "in" includes "in" and "on." The term "connected" means a direct electrical connection between the items connected, without any intermediate devices. The term "coupled" means either a direct electrical connection between the items connected or an indirect connection through one or more passive or active intermediary devices. The term "circuit" means either a single component or a multiplicity of components, either active and/or passive, that are coupled together to provide a desired function. The term "signal" means at least one current, voltage, charge, temperature, data, or other measurable quantity. The terms "RFID reader" and "RFID tag" are used interchangeably with the terms "reader" and "tag", respectively, throughout the text and claims.

All of the circuits described in this document may be implemented as circuits in the traditional sense, such as with integrated circuits etc. All or some of them can also be implemented equivalently by other ways known in the art, such as by using one or more processors, Digital Signal Processing (DSP), a Field-Programmable Gate Array (FPGA), etc.

FIG. **1** is a diagram of an example RFID system including an RFID reader communicating with an RFID tag in its field of view. An RFID reader **110** transmits an interrogating Radio Frequency (RF) wave **112**. RFID tag **120** in the vicinity of RFID reader **110** may sense interrogating RF wave **112**, and generate wave **126** in response. RFID reader **110** senses and interprets wave **126**.

Reader **110** and tag **120** exchange data via wave **112** and wave **126**. In a session of such an exchange, each encodes, modulates, and transmits data to the other, and each receives, demodulates, and decodes data from the other. The data is modulated onto, and decoded from, RF waveforms.

Encoding the data in waveforms can be performed in a number of different ways. For example, protocols are devised to communicate in terms of symbols, also called RFID symbols. A symbol for communicating can be a delimiter, a calibration symbol, and so on. Further symbols can be implemented for ultimately exchanging binary data, such as "0" and "1", if that is desired. In turn, when the waveforms are processed internally by reader **110** and tag **120**, they can be equivalently considered and treated as numbers having corresponding values, and so on.

Tag **120** can be a passive tag or an active or semi-active tag, i.e. having its own power source. Where tag **120** is a passive tag, it is powered from wave **112**.

FIG. **2** is a diagram of an RFID tag **220**, which can be the same as tag **120** of FIG. **1**. Tag **220** is implemented as a passive tag, meaning it does not have its own power source. Much of what is described in this document, however, applies also to active tags.

Tag **220** is formed on a substantially planar inlay **222**, which can be made in many ways known in the art. Tag **220** includes an electrical circuit, which is preferably implemented in an integrated circuit (IC) **224**. IC **224** is arranged on inlay **222**.

Tag **220** also includes an antenna for exchanging wireless signals with its environment. The antenna is usually flat and attached to inlay **222**. IC **224** is electrically coupled to the antenna via suitable antenna ports (not shown in FIG. **2**).

The antenna may be made in a number of ways, as is well known in the art. In the example of FIG. **2**, the antenna is made from two distinct antenna segments **227**, which are shown here forming a dipole. Many other embodiments are possible, using any number of antenna segments.

In some embodiments, an antenna can be made with even a single segment. Different points of the segment can be coupled to one or more of the antenna ports of IC **224**. For example, the antenna can form a single loop, with its ends coupled to the ports. When the single segment has more complex shapes it should be remembered that, at the frequencies of RFID wireless communication, even a single segment could behave like multiple segments.

In operation, a signal is received by the antenna, and communicated to IC **224**. IC **224** both harvests power, and responds if appropriate, based on the incoming signal and its internal state. In order to respond by replying, IC **224** modulates the reflectance of the antenna, which generates the backscatter from a wave transmitted by the reader. Coupling together and uncoupling the antenna ports of IC **224** can modulate the reflectance, as can a variety of other means.

In the embodiment of FIG. **2**, antenna segments **227** are separate from IC **224**. In other embodiments, antenna segments may alternately be formed on IC **224**, and so on.

The components of the RFID system of FIG. **1** may communicate with each other in any number of modes. One such mode is called full duplex. Another such mode is called half-duplex, and is described below.

FIG. **3** is a conceptual diagram **300** for explaining the half-duplex mode of communication between the components of the RFID system of FIG. **1**, especially when tag **120** is implemented as passive tag **220** of FIG. **2**. The explanation is made with reference to a TIME axis, and also to a human metaphor of "talking" and "listening". The actual technical implementations for "talking" and "listening" are now described.

RFID reader **110** and RFID tag **120** talk and listen to each other by taking turns. As seen on axis TIME, when reader **110** talks to tag **120** the communication session is designated as "R→T", and when tag **120** talks to reader **110** the communication session is designated as "T→R". Along the TIME axis, a sample R→T communication session occurs during a time interval **312**, and a following sample T→R communication session occurs during a time interval **326**. Of course interval **312** is typically of a different duration than interval **326**—here the durations are shown approximately equal only for purposes of illustration.

According to blocks **332** and **336**, RFID reader **110** talks during interval **312**, and listens during interval **326**. According to blocks **342** and **346**, RFID tag **120** listens while reader **110** talks (during interval **312**), and talks while reader **110** listens (during interval **326**).

In terms of actual technical behavior, during interval **312**, reader **110** talks to tag **120** as follows. According to block **352**, reader **110** transmits wave **112**, which was first described in FIG. **1**. At the same time, according to block **362**, tag **120** receives wave **112** and processes it, to extract data and so on. Meanwhile, according to block **372**, tag **120** does not backscatter with its antenna, and according to block **382**, reader **110** has no wave to receive from tag **120**.

During interval **326**, tag **120** talks to reader **110** as follows. According to block **356**, reader **110** transmits a Continuous Wave (CW), which can be thought of as a carrier signal that ideally encodes no information. As discussed before, this carrier signal serves both to be harvested by tag **120** for its own internal power needs, and also as a wave that tag **120** can backscatter. Indeed, during interval **326**, according to block **366**, tag **120** does not receive a signal for processing. Instead, according to block **376**, tag **120** modulates the CW emitted according to block **356**, so as to generate backscatter wave **126**. Concurrently, according to block **386**, reader **110** receives backscatter wave **126** and processes it.

FIG. **4** is a block diagram of an electrical circuit **430**. Circuit **430** may be formed in an IC of an RFID tag, such as IC **224** of FIG. **2**. Circuit **430** has a number of main components that are described in this document. Circuit **430** may have a number of additional components from what is shown and described, or different components, depending on the exact implementation.

Circuit **430** includes at least two antenna connections **432**, **433**, which are suitable for coupling to one or more antenna segments (not shown in FIG. **4**). Antenna connections **432**, **433** may be made in any suitable way, such as pads and so on. In a number of embodiments more than two antenna connections are used, especially in embodiments where more antenna segments are used.

Circuit **430** includes a section **435**. Section **435** may be implemented as shown, for example as a group of nodes for proper routing of signals. In some embodiments, section **435** may be implemented otherwise, for example to include a receive/transmit switch that can route a signal, and so on.

Circuit **430** also includes a Power Management Unit (PMU) **441**. PMU **441** may be implemented in any way known in the art, for harvesting raw RF power received via antenna connections **432**, **433**. In some embodiments, PMU **441** includes at least one rectifier, and so on.

In operation, an RF wave received via antenna connections **432**, **433** is received by PMU **441**, which in turn generates power for components of circuit **430**. This is true for either or both R→T and T→R sessions, whether or not the received RF wave is modulated.

Circuit **430** additionally includes a demodulator **442**. Demodulator **442** demodulates an RF signal received via antenna connections **432**, **433**. Demodulator **442** may be implemented in any way known in the art, for example including an attenuator stage, amplifier stage, and so on.

Circuit **430** further includes a processing block **444**. Processing block **444** receives the demodulated signal from demodulator **442**, and may perform operations. In addition, it may generate an output signal for transmission.

Processing block **444** may be implemented in any way known in the art. For example, processing block **444** may include a number of components, such as a processor, a memory, a decoder, an encoder, and so on.

Circuit **430** additionally includes a modulator **446**. Modulator **446** modulates an output signal generated by processing block **444**. The modulated signal is transmitted by driving antenna connections **432**, **433**, and therefore driving the load presented by the coupled antenna segment or segments. Modulator **446** may be implemented in any way known in the art, for example including a driver stage, amplifier stage, and so on.

In one embodiment, demodulator **442** and modulator **446** may be combined in a single transceiver circuit. In another embodiment, modulator **446** may include a backscatter transmitter or an active transmitter. In yet other embodiments, demodulator **442** and modulator **446** are part of processing block **444**.

Circuit **430** additionally includes a memory **450**, which stores information. Memory **450** is preferably implemented as a Nonvolatile Memory (NVM), which means that its stored information is retained even when circuit **430** does not have power, as is frequently the case for a passive RFID tag.

It will be recognized at this juncture that the shown components of circuit **430** can be those of a circuit of an RFID tag according to the invention, with or without needing PMU **441**. Indeed, an RFID tag can be powered differently, such as from a wall outlet, a battery, and so on. Additionally, when circuit **430** is configured as a reader, processing block **444** may have additional Inputs/Outputs (I/O) to a terminal, network, or other such devices or connections.

In terms of processing a signal, circuit **430** operates differently during an R→T session and a T→R session. The different operations are described below, in this case with circuit **430** representing an RFID tag.

FIG. **5**A shows version **530**-A of components of circuit **430** of FIG. **4**, further modified to emphasize a signal operation during an R→T session (receive mode of operation) during time interval **312** of FIG. **3**. An RF wave is received from antenna connections **432**, **433**; a signal is demodulated from demodulator **442**, and then input to processing block **444** as C_IN. In one embodiment according to the present invention, C_IN may include a received stream of symbols.

Version **530**-A shows as relatively obscured those components that do not play a part in processing a signal during an

R→T session. Indeed, PMU **441** may be active, but only in converting raw RF power. And modulator **446** generally does not transmit during an R→T session. Modulator **446** typically does not interact with the received RF wave significantly, either because switching action in section **435** of FIG. **4** decouples the modulator **446** from the RF wave, or by designing modulator **446** to have a suitable impedance, and so on.

While modulator **446** is typically inactive during an R→T session, it need not always be the case. For example, during an R→T session, modulator **446** could be active in other ways. For example, it could be adjusting its own parameters for operation in a future session.

FIG. **5**B shows version **530**-B of components of circuit **430** of FIG. **4**, further modified to emphasize a signal operation during a T→R session during time interval **326** of FIG. **3**. A signal is output from processing block **444** as C_OUT. In one embodiment according to the present invention, C_OUT may include a transmission stream of symbols. C_OUT is then modulated by modulator **446**, and output as an RF wave via antenna connections **432**, **433**.

Version **530**-B shows as relatively obscured those components that do not play a part in processing a signal during a T→R session. Indeed, PMU **441** may be active, but only in converting raw RF power. And demodulator **442** generally does not receive during a T→R session. Demodulator **442** typically does not interact with the transmitted RF wave, either because switching action in section **435** decouples the demodulator **442** from the RF wave, or by designing demodulator **442** to have a suitable impedance, and so on.

While demodulator **442** is typically inactive during a T→R session, it need not be always the case. For example, during a T→R session, demodulator **442** could be active in other ways. For example, it could be adjusting its own parameters for operation in a future session.

FIG. **6**A is a conceptual diagram illustrating a few of the possible commands that can be received by a tag, e.g. as transmitted by one or more readers. One such command is a "Kill" command, which renders a tag permanently non-responsive to any further commands by a reader.

As shown in diagram **600**, a reader **610-1** may transmit a "Write" command (**660-1**) to tag **620-1** causing the tag to store information in its memory. Tag **620-1** may be written multiple times, including after intervening commands such as a "Read".

At a later time point, reader **610-1** or another reader (**610-2**) may transmit a "Read" command (**660-2**) to read tag **620-1**. Tag **620-1** may be read multiple times.

At one point during the operations, reader **610-1** or yet another reader (**610-3**) may transmit a "Kill" command to tag **620-1**. Upon receiving the "Kill" command, tag **660-1** performs a series of operations that typically renders tag **660-1** nonresponsive to further commands, according to comment **662**. Often such a tag is then called a killed tag.

FIG. **6**B is an example tag state diagram illustrating the transition of a tag from an operational state to a killed state upon receiving a "Kill" command.

As shown in tag state diagram **601**, a tag in a regular operational state **600**, upon receiving a "Kill" command, transitions to totally killed state **640** in which the tag becomes no longer responsive to subsequent commands. In the prior art, state **640** was known as killed stated; the adverb "totally" is added in this disclosure to differentiate from embodiments of the invention.

FIG. **7** is a diagram illustrating how a tag physical memory such as the memory shown in FIG. **4** can be partitioned and organized for data to be mapped into it, also in compliance with the Gen2 Specification. In FIG. **7** a single memory is shown, but it will be understood that two memories devices can be used for the different functions of the tag, and so on.

Tag memory **750** is partitioned into different portions. The data stored in memory **750** may include identification information associated with the tag, information associated with an item the tag is attached to, communication parameters such as a password, externally delivered data, and the like. Data may be stored in portions of the memory such as memory portion **704** during a production stage, or during an operation by processing block **444** of FIG. **4**. Processing block **444** may access memory **750** to store or retrieve one or more of a received command, password, production data, and externally delivered data. Processing block **444** may also access memory **750** to change its contents based on a command received from a reader.

As mentioned above, tag memory **750** may be partitioned into user-specific portion **752**, tag-identification (TID) portion **754**, object-identification portion (EPC) **756**, and reserved portion **758**. In other embodiments, memory **750** may be partitioned in other ways with fewer or more portions, or not partitioned at all.

User-specific portion **752** may be employed to store user-specified information such as a date code, a store location, and sensor data if the tag is associated with a sensor whose data is mapped to user memory. Mapping of sensor data is discussed in commonly owned U.S. patent application Ser. No. 11/217,616, published on 2006 Aug. 24 as document 2006/0187031A1.

Information stored in user memory **752** may be used in tag operations. Tag-identification portion (TID) **754** may be employed to store information associated with a tag identifier, and may store other data as well.

Object identification portion (EPC) memory **756** can be arranged to store, as convenient, a protocol control (PC) parameter, an EPC code, and/or a CRC16 (cyclic redundancy check) as shown in memory addresses **752**. Reserved memory portion **758** may be used to store system parameters such as passwords.

FIG. **8** is a diagram illustrating how lock bits can be used to control access of the partitioned and organized memory of FIG. **7**, also in compliance with the Gen2 Specification.

A reader may control access to particular portions of a tag's memory by transmitting commands that can temporarily or permanently block access to those portions such that the contents of the memory portion cannot be changed (or even read) by subsequent commands.

For example, a retail sales organization may desire to permanently lock some information stored in their tags, such as recycling information stored in User memory portion **752**, so that the product to which the tag is attached can be recycled at the end of the product's life. On the other hand certain memory portions may be temporarily blocked such that they can be made accessible again later if necessary (e.g. to be able to process returned goods).

A reader may accomplish the above described memory blocking operations by transmitting a command such as a "Lock" command that includes a payload with mask and action bits as described above. The action bits, also called the lock bits, may be used to "lock" specific memory portions.

The locking of memory portions such as user memory portion **752**, TID portion **754**, EPC portion **756**, and reserved memory portion **758** may be accomplished by assigning specific lock bits such as lock bits **872**, **874**, **876**, and **878** to the respective memory portions. When the tag receives a "Lock" command with one or more of the lock bits set to a predetermined value (e.g. "1"), it locks the corresponding memory portion.

RFID tags according to embodiments are not limited to lock bits being assigned to individual memory portions in a one-on-one manner. Rather, a combination of lock bits may also specify a particular memory portion.

FIG. **9** illustrates an example payload of a "Lock" command that can be applied to control the memory lock bits of the memory of FIG. **8**, also in compliance with the Gen2 Specification.

A reader according to Gen2 Specification may set 10 lock bits in the tag by issuing a "Lock" command, which includes a 20-bit payload. 10 bits of the payload are mask bits, the other 10 are the lock bits. Diagram **900** illustrates the mask bits (**994**) and lock bits (**996**) of a "Lock" command's payload and their associated action fields (e.g. which memory portions **992** the lock bits act on).

According to the Gen2 Specification, a mask bit being set to "0" causes the tag to retain its current lock bit (skip). If a mask bit is set to "1", the tag may overwrite the current lock bit (write) with the value included in the "Lock" command's payload.

As shown in FIG. **9**, two lock bits are assigned to user memory portion **752**. If the first lock bit (bit 0) is set to a "1" then the user memory portion **752** is permanently locked. If bit **0** is set to a "0" then user memory portion **752** is not permanently locked. User memory portion **752** may be locked or permanently locked in one of a writeable or unwriteable state, the state being determined by the second lock bit (bit **1**). If bit **1** is set to a "0" then user memory portion **752** is writeable; if bit **1** is set to a '1" then it is not writeable.

The TID portion **754** and the EPC portion **756** are configured to be locked (or unlocked) in a similar manner by using lock bits **2**, **3** and **4**, **5**, respectively, and their corresponding mask bits.

Diagram **900** also shows lock bit pairs (bits **6**, **7** and **8**, **9**) and their corresponding mask bits being used to lock or leave accessible the "Kill" and "Access" passwords stored in the reserved memory portion **758** of the tag memory.

In some embodiments of the invention the first memory function is disabled permanently. In others, it is reversible. It is often preferred that the disabling become permanent, so that better privacy can be implemented, where, for example, RFID tags are used for consumer goods. In preferred embodiments, the disabling by using alternative lock bits is made permanent by making it so that the first protocol-related bit cannot be reset once it has been set.

Any suitable memory function can be disabled, in different ways. A number of such possible memory functions are described.

A memory function to be disabled may include prevention of a later ability to lock the memory portion. For example, if this memory function is disabled, the tag or chip will no longer support permalocking subportions (also known as blocks) of the memory portion. Block permalocking is defined in the Gen 2 Specification, and the portion can be the user memory.

The memory function to be disabled may also include reading a memory portion. For example, if this memory function is disabled, that portion of the memory can no longer be read. It could be the user memory, or another portion.

The memory function to be disabled may further include a locking function of a memory portion. For example, if this memory function is disabled, that portion of the memory becomes unlocked, and can be changed. This could be applied to all banks of memory that are ordinarily un-lockable. This procedure may further be reversible in some embodiments.

The memory function to be disabled may yet further include writing to a memory portion. For example, if this memory function is disabled, that portion of the memory becomes un-writable.

Of course, the function may also include combinations of the above individual functions. For example, a memory might be prevented from being read, and from being written to, and so on.

When a first memory function becomes disabled, the tag no longer responds the same way. For example, if it were to receive again the initial command that previously caused it to employ the first memory function, after disabling it will not employ again the first memory function.

The tag will know to not employ the first memory function because it can determine internally that it has been disabled. For example, determining can take place by determining that the protocol-related bit has been set.

In such an instance, a tag may respond in any number of ways, or not at all. In some embodiments, it backscatters a negative reply on occasion of not employing the first memory function.

Moreover, when the first memory function becomes disabled, the tag might again receive the first partial-kill command, which at this point would be redundant. The redundant command might be ignored, or responded to in any fashion. In some embodiments, it might backscatter another reply to indicate that the first memory function has been disabled. The other reply can indicate, or not, whether the first memory function had previously become disabled, or is just becoming disabled. The other reply can be generated from the set first protocol-related bit, if these are used.

The invention also includes methods. Some are methods of operation of an RFID tag or an RFID tag circuit. Others are methods for controlling an RFID tag or RFID tag circuit. These methods can be implemented in any number of ways, including using the structures described in this document. One such way is by machine operations, by devices of the type described in this document.

Methods are now described more particularly according to embodiments.

FIG. **10** is a flowchart **1000** of an RFID tag becoming partially killed. The tag or chip starts by having a memory, and a memory function associated with at least a portion of the memory. In other words, it can employ the memory function in response to receiving an initial memory command.

In addition, the tag or chip is able to backscatter a particular operating reply in response to an operating request. Such an operating request can be, for example, a request for a random number, which is called Req_RN in the Gen2 Specification. The appropriate reply is a random number backscattered from the tag.

According to operation **1010**, the tag receives from a reader a first command. The first command can be any command suitable for being designed as a partial-kill command. In some embodiments it is a standalone partial-kill custom command, without a payload. In other embodiments, the first command includes a command code and a command payload that has one or more disabling bits. These disabling bits indicate that the first command is a partial-kill command. The command code can be any command suitable for creating a partial-kill command, such as that of a "Kill" command, a protocol command, a proprietary command, a custom command, etc.

According to an optional next operation **1020**, the tag sets one or more corresponding protocol-related bits in response to the received first command. Where disabling bits have been implemented, the one or more corresponding protocol-re-

lated bits can be set according to the received disabling bits. In fact, the protocol-related bits can be the same as the disabling bits, although that is not necessary.

The protocol-related bit(s) can be set anywhere. It is preferred that they be set in the memory, as will be described below.

According to a next operation **1030**, the tag transitions to a partially killed state, in response to receiving the first command of operation **1010**. In other words, the tag transitions to a state where one or more (but not all) of its memory functions are disabled. The partial-kill command means, therefore, that the tag is not to be totally killed in the traditional sense, but only to be partially killed. Therefore, the tag does not lose all ability to backscatter any reply, but still retains at least some functionality. For example, the tag or chip may still be above to backscatter an appropriate operating reply to an operating request, such as for a random number as described above. However, the tag becoming partially killed means that there can be some operating requests for which the appropriate operating reply will no longer be backscattered, due to the disabling.

Where the first command includes one or more disabling bits, disabling can be performed according to the disabling bits. In fact, the disabling bits can dictate which one(s) of the memory functionalities are to be disabled.

Where protocol-related bits are set in response to the received first command, these protocol-related bits can further be set responsive to the disabling bits.

A protocol-related bit may be set, or not, by performing a logic OR operation between a value of a currently stored protocol-related bit, and a value of a corresponding received disabling bit. So, the protocol-related bit can start with a value of 0, which can be defined as not set. As long as the disabling bits are 0, it remains with the value of 0. Once a disabling bit with a value of 1 is received, the protocol-related bit becomes 1 by the logic OR operation, which means that the protocol-related bit becomes set. Subsequent disabling bits will not change it, which can make for an irreversible operation.

In a number of embodiments, the memory function is disabled by adjusting a first lock bit. For example, the lock bit is adjusted responsive to setting the associated protocol-related bit.

According to a next optional operation **1040**, the tag backscatters a reply. The reply has been generated also from the first protocol-related bit, to indicate that the first memory function has been disabled.

The reply can be implemented in any number of ways. For example, the reply can be backscattered in response to receiving the first command. This way the tag can confirm to the reader that it performed the commanded operation, as a "DONE" response.

For another example, the reply can be backscattered in response to a subsequent command by a reader. This way the tag can inform a different reader that it has been partially killed.

The disabling can be indicated in any number of ways. For example, the reply can indicate a value of the set first protocol-related bit, directly or not, or the original disabling bit, etc.

It will be understood that the operations included in process **1000** are for illustration purposes only. The invention may be further practiced by similar processes with fewer or with additional steps, as well as in a different order of operations, using the principles described herein.

FIG. **11** is a conceptual diagram illustrating different commands transmitted by one or more readers and a "Partial Kill" command causing a tag to become partially killed, as per FIG. **10**.

Similar to the operations described in FIG. **6**A, a reader **1110-1** may cause tag **1120-1** to store information in its memory by transmitting "Write" command **1160-1**. The same reader or another reader (**1110-2**) may read the tag by transmitting "Read" command **1160-2**.

At some point in the tag's life cycle, a reader (e.g. **1110-3**) may transmit a partial-kill command **1160-4** to tag **1120-1**. This causes the tag to disable one or more of its functionalities (partially disabled tag **1120-3**, according to comment **1162**).

For understanding the use and relations between the protocol-related bits, lock bits, and memory functions better, it is advantageous to describe at this point how a tag physical memory can be according to embodiments. Thus, a survey of the tag memory is given below.

FIG. **12** is a diagram illustrating how a tag physical memory such as the memory shown in FIG. **7** can be partitioned and organized for data to be mapped into it, including the protocol-related bits.

User memory portion **1252**, TID memory portion **1254**, and reserved memory portion **1258** of tag memory **1250** are configured to operate similarly to the tag memory **750** of FIG. **7** with data stored as discussed above.

Differently from FIG. **7**, a tag memory **1250** according to some embodiments may include an EPC portion **1256** with a location **1206** for the protocol-related bits (P-R-B). While a single location is shown, such P-R-Bits may be stored as one word or as multiple words. In some embodiments, the P-R-Bits are stored as one word whose size is 16 bits.

In preferred embodiments, the disabling bits will be in a payload of a reader command, in the position specified by the Gen 2 Specification for the extended protocol control XPC bits. Such is shown, for example, with a brief reference to FIG. **20**, where disabling bits are known as RFU/RECOM bits. Furthermore, these disabling bits are received, parsed, and stored in preferred embodiments as the protocol-related bits that control disabling one or more individual memory functions. These protocol-related bits are then stored in location **1206**.

Portion **1202** shows memory addresses by function. Much is similar to the memory addresses **702** of FIG. **7**. In addition, location **1206** is shown with the P-R-Bits.

It is preferred, but not necessary for practicing the invention, that memory location **1206** be able to accommodate more than just one bit. In a number of embodiments, each P-R-Bit nominally corresponds to disabling each individual memory function.

While a partial-kill command may include a single disabling bit, such a bit may disable one or more individual memory functions. This can be accomplished, for example, if there are rules among the bits.

In such implementations, when the second command is received, a second protocol-related bit is set, in addition to the first such bit. Furthermore, a second memory function is disabled, as per the above, without the tag becoming totally killed.

In some implementations combinations of memory functions are disabled for a broader effect. For example, when both writing to a memory portion and reading from it are disabled, then the memory portion itself is effectively disabled.

In these implementations, it is advantageous for the reply to be generated also from the set second protocol-related bit, to indicate that also the second memory function has been

disabled. This can be performed in any number of ways. For example, the reply can indicate a value of the set first and second protocol-related bit.

In some implementations, the first memory function includes disabling a later ability to lock the memory portion, and the second memory function includes reading the memory portion. These can be accomplished, therefore, with a single disabling bit.

Moreover, a partial-kill command may include any number of disabling bits. In some implementations there is a one-to-one correspondence between the disabling bits and the protocol-related bits. FIG. **12** illustrates an example with a one-to-one correspondence between three disabling bits and three protocol-related bits, namely 3SB, 2SB, and LSB. In this example, if a tag receives a reader command whose RFU/RECOM bits are 001, it asserts a "1" in the least significant bit (LSB) location **1208** of its protocol-related bits in tag memory.

Additionally, partial-kill commands may be received serially, with the tag successively disabling functions. For example, the above effect can be accomplished with two separate commands, one for disabling the first memory function, and one for disabling the second.

As described above, in some embodiments the P-R-Bits, once set, may not be unset. Continuing the previous example of a tag with three disabling bits and three protocol-related bits, upon receiving successive partial-kill commands the tag may assert additional disabling bits. For example, the tag may receive a subsequent partial-kill command containing "100" for the RFU/RECOM bits. In this case the tag will assert "1" for the 3SB bit of its XPC, resulting in the tag's stored XPC bits becoming "101".

The tag can use the protocol-related bits as its record of which (if any) of its memory functions have been disabled, as well as providing a record of other details of the partial-kill operation.

Additionally, and as mentioned above with reference to rules among the protocol control bits, some P-R-Bits may have priority over others. For example, an asserted LSB may indicate that the tag no longer supports permalocking of sub-portions of the user memory portion, whereas an asserted 2SB may indicate that the user memory portion is killed. Here, a 2SB may take precedence over the LSB, meaning that if both are asserted then the user memory portion is killed.

An asserted 3SB may indicate that the tag has unlocked all un-lockable memory portions and/or locations, including those that were previously permalocked. These memory portions may be locked and/or permalocked by a subsequent "Lock" command.

It will have been observed that many of the memory functions that can be disabled involve accessing the contents of the memory. These can be accomplished with controlling lock bits of the memory portions, as described immediately below. As written above, in a number of embodiments, the memory function is disabled by adjusting a first lock bit. In some examples, such a lock bit can be adjusted in association with setting a related protocol-related bit.

FIG. **13** is a diagram illustrating how lock bits can be used to control access of a memory that is partitioned and organized as the memory of FIG. **12**, and in which further the lock bits are controlled by protocol-related bits that are mapped within the controlled memory.

Diagram **1300** shows a tag memory with portions **1352**, **1354**, **1356**, and **1358** as described previously. In a tag circuit according to embodiments, each memory portion may be assigned one or more lock bits such as lock bits **1372**, **1374**, **1376**, and **1378**, respectively.

A distinction is now made: the contents of memory portions **1352**, **1354**, **1356**, **1358** can be backscattered to a reader, and thus a user, if properly accessed and if unlocked. Lock bits **1372**, **1374**, **1376**, and **1378**, however, in some embodiments cannot be backscattered. In other embodiments, they can be backscattered. An advantage of the invention is that, by defining location **1306** of the protocol-related bits within portion **1356**, the protocol-related bits can themselves be backscattered, and thus the user can ascertain that a tag has indeed been partially killed.

FIG. **14** is a conceptual diagram illustrating how an RFID tag with a memory partitioned and organized as in the memory of FIG. **12** could reset its memory lock bits upon receiving a "Partial Kill" command, and also for describing a problem.

According to diagram **1400**, reader **1410** transmits a partial-kill command **1412** to tag **1420**. Such a partial-kill command can be a command to unlock user memory. In such unlocking, all relevant bits could be reset, e.g. to 0. Such unlocking could be permanent or reversible. If reversible, it might take place again. Even if reversible, however, the protocol-related bit can still indicate that this unlocking has happened at least once in the lifetime of the tag.

Upon receiving the partial-kill command (**1462**), the tag may write its protocol-related bits (**1464**) based on the value of the protocol-related bits in the partial-kill command's payload, which are intended to disable.

Then, the tag may reset or adjust its lock bits (**1466**) based on the (newly) written protocol-related bits. The reset lock bits determine which memory portions are locked or unlocked for access by subsequent Read, Write, Lock, and other commands, so as to implement the commanded disabling.

After resetting the lock bits, the tag may optionally backscatter an affirmative response such as a reply (**1468**) to the reader, acknowledging the disabling or not of the memory function.

Thus, some or all of the partially killed states of the tag can correspond to a received and stored disabling bit, or combination of bits.

FIG. **15** is a block diagram illustrating a memory section whose access is controlled by one or more alternative lock bits according to embodiments.

As described above, RFID tags may use lock bits to control access to memory sections. A tag according to Gen2 specification may have 10 lock bits for controlling access to different sections of the NVM memory. In a conventional tag, these bits may be set and not allowed to be changed afterwards. Setting can be at manufacturing, or other contexts. On the other hand, a tag capable of performing partial kill operations may allow particular sections of the tag memory to be locked and then unlocked by reader commands, utilizing the protocol-related bits for "resetting" the lock bits.

However, writing a set of protocol-related bits followed by the lock bits based on the protocol-related bits may require two sets of operations, as discussed previously, and a tag may not be capable of performing these two write operations within the standard prescribed 20 ms reply time.

An RFID tag according to embodiments may utilize two sets of alternative lock bits (as a minimum two alternative bits). As shown in the figure, first set of lock bits **1572** may cause the memory section **1552** to function in one manner, while the other set of lock bits **1573** may cause the memory section **1552** to function in another manner.

For example, memory section **1552** may be accessible for read operations only if the first set of lock bits are used and the memory section may be accessible for read or write operations if the second set is used.

The questions of which set of lock bits is to be used, is determined by the operator **1592** to be described later.

FIG. **16** is a block diagram illustrating a memory that is partitioned into sections and organized as the memory of FIG. **12**, and where further access to each of these sections is controlled by one or more alternative lock bits according to embodiments.

Diagram **1600** illustrates specific examples of alternative lock bit use for a tag memory **1650** with user section **1652**, TID section **1654**, EPC section **1656**, and Reserved section **1658**.

Pairs of lock bit sets (**1672**-**1679**) are shown. Each pair is assigned to each memory section, as alternative sets. As in FIG. **15**, operators **1692**, **1694**, **1696**, and **1698** may determine which lock bit set is to be used for a particular memory section.

According to one embodiment, the operator for determining the lock bit set to be used may be a pointer for each alternative bit set. The tag may look up the pointer (e.g. at power up) and determine which lock bit set to use when performing reader requested operations.

According to a further embodiment, the pointers for the alternative lock bit sets may be determined by the protocol-related bits (**1606**). Thus, a tag does not need to perform two sets of write operations for first saving the protocol-related bits and second setting the lock bits. Instead once the protocol-related bits are written into tag memory (e.g. EPC section **1656**), the pointer for the lock bits is determined and the lock bits to be used are also determined.

In an example embodiment, one of the protocol-related bits, such as the third least significant bit (3SB) may be used to select the lock bit set among the alternative pair. Thus, the protocol-related bit itself may be the pointer. In another embodiment, the pointer may be a state machine flag in the tag set by the 3SB of the protocol-related bits.

FIG. **17** is a conceptual diagram illustrating how an RFID tag with a memory partitioned and organized as in the memory of FIG. **12** could automatically reset its memory lock bits upon receiving a partial-kill command, because they are alternative memory lock bits as per the embodiment of FIG. **13**.

Reader **1710** transmits a partial kill command **1712** to tag **1720**. In response to receiving the partial kill command (**1762**), the tag writes the protocol-related bits in its memory (e.g. EPC section).

Because the lock bit set to be used for particular sections of the memory is determined based on one or more of the protocol-related bits, there is no need for a second operation to reset the lock bits (**1766**). Instead, the pointer can "switch" to indicating the alternative lock bit set.

The tag may optionally reply with an affirmative response indicating to the reader that the protocol-related bits have been written and/or the lock bit set is selected.

FIG. **18** is a conceptual diagram illustrating how an RFID tag could chose among alternative memory lock bits at power-up, as may have been determined by resetting them upon receiving the partial-kill command of FIG. **14**.

The lock bits may be used in conjunction with a number of reader commands which involve a section of the tag memory (e.g. writing to a section, reading a section, etc.). The protocol-related bit(s) (e.g. 3SB) may be set following receipt of a partial kill command. In some instances, a passive tag powers down after it loses power from the reader. Thus, the tag may power down following the partial kill command.

When the tag receives another command involving a section of the memory, it may read the previously set protocol-related bit(s). Alternatively, the tag may read and exercise the previously set protocol-related bit at power-up (**1884**). Upon reading the protocol-related bit(s), the tag determines which set of lock bits to use. In the example of FIG. **18**, the tag uses the first set of lock bits of the 3SB if the protocol-related bits is "0" (**1886-1**) and it uses the second set of lock bits of the 3SB of the protocol-related bits is "1" (**1886-2**).

According to some embodiments, an RFID tag circuit includes a memory that includes a first location for storing a first lock bit, a second location for storing a second lock bit, and a third location for storing a pointer configured to point to the first lock bit or the second lock bit. The memory further includes a section that has an operable functionality if the pointed to one of the first and the second lock bits has a first value, but lacks the operable functionality if the pointed to one of the first and the second lock bits has a second value. The tag circuit also includes a modulator able to cause a reply to be backscattered regardless of whether the pointer is configured to point to the first lock bit or to the second lock bit.

The operable functionality may be reading, writing to, write-locking, or read locking the memory section. The first lock bit and the second lock bit may have different values and the pointer may be looked up at tag power-up.

According to other embodiments, the pointer may be configurable to stop pointing to the first lock bit and start pointing instead to the second lock bit, responsive to receiving a partial-kill command Once the pointer has been configured by the partial-kill command, it cannot be configured to start pointing back to the first lock bit. Furthermore, the pointer becomes configured by acquiring a value that is carried as a payload of the partial-kill command.

According to further embodiments, the tag described above may lose power after receiving a first command, receive power again, power up responsive to receiving power again, then receive a second command, and backscatter the reply in response to the second command, but not backscatter a reply in response to the first command.

The tag circuit may be integrated into an RFID tag which has an antenna in addition to the tag circuit.

As mentioned above, the invention includes methods of operation of an RFID tag or an RFID tag circuit and methods for controlling an RFID tag or RFID tag circuit. Some of these methods, particularly according to embodiments, are now described in more detail.

FIG. **19** is a flowchart for illustrating methods for an RFID tag to respond to a command, by using a set of lock bits chosen as illustrated with reference to FIG. **16** as per embodiments of the invention. Such methods can be implemented by many tags, including for example a tag that includes in its memory a first lock bit, a second lock bit, and a pointer configured to point to one of the first lock bit and the second lock bit.

According to operation **1920**, a tag receives a command requesting a functionality of a section of the memory to be performed.

According to next decision operation **1920**, a determination is made whether the pointer points to the first lock bit. If the pointer points to the first lock bit, the requested functionality is performed based on the first lock bit at next operation **1930**.

After operation **1930**, the tag may backscatter a reply at optional operation **1960**.

If the pointer is not pointing to the first lock bit, another determination is made at optional decision operation **1940** whether the pointer is pointing to the second lock bit.

If the pointer is not pointing to the second lock bit either, the tag may perform another operation such as transmitting the reader an error message at subsequent operation **1970**.

If the pointer is pointing to the second lock bit, the functionality is performed based on the second lock bit at following operation **1950**. As discussed above the section of the memory may be configured to perform the functionality differently depending on which lock bit is used.

Following operation **1950**, the tag may again backscatter a reply at optional operation **1960**.

The operations included in process **1900** are for illustration purposes only. Employing alternative lock bits using protocol-related bits in an RFID tag may be implemented by similar processes with fewer or additional steps, as well as in different order of operations using the principles described herein.

FIG. **20** is a diagram illustrating a reader command and corresponding tag response with protocol-control bits as payload, according to embodiments.

A reader command (**2012**) typically includes a command code and a command payload. For example, a partial-kill command according to embodiments may comprise the command code of a "Kill" command and include within its payload the disabling bits (for example, RFU/RECOM bits).

Once the command is transmitted, the tag is required to respond within a preset time period TREPLY (e.g. 20 ms). The tag response (**2088**) typically includes a preamble (**2034**), a handle (**2036**), and a Cyclical Redundancy Check (CRC) bit or bits (**2038**).

If the reader is also requesting the tag to report its partial kill status, the response may optionally include the tag's protocol-related bits to affirm to the reader the tag's status (**2088**).

As discussed above, in response to a partial-kill command, the tag both writes its XPC bits, and resets its lock bits. By implementing the above described embodiments, the XPC bits can be written (**2032**) and the lock bits reset in a single write operation within the preset time period TREPLY of FIG. **20**.

The electrical circuit(s) described in this document can be manufactured in any number of ways, as will be appreciated by the persons skilled in the art. One such way is as integrated circuit(s), as described below.

Schematic-type inputs can be provided for the purpose of preparing one or more layouts. These inputs can include as little as a schematic of a circuit, to more including relative sizes of circuit components and the like, as will be appreciated by a person skilled in the art for such inputs. These inputs can be provided in any suitable way, such as merely in writing, or electronically, as computer files and the like. Some of these computer files can be prepared with the assistance of suitable design tools, often provided as computer software. Such tools often include instrumentalities for simulating circuit behaviors and the like.

These inputs can be provided to a person skilled in the art of preparing layouts. This, whether the person is within the same company, or another company, such as under a contract.

A layout can be prepared that embodies the provided schematic-type inputs by the person skilled in the art. The layout is itself preferably prepared as a computer file. It may be additionally checked for errors, modified as needed, and so on.

In the above, computer files can be made from portions of computer files. For example, suitable individual designs can be assembled for the electrical components and circuits indicated in the schematic-type inputs. The individual designs can be generated anew, or selected from existing libraries for such items. In the layout phase, the assembled designs can be arranged to interoperate, so as to implement as integrated circuit(s) the electrical circuit(s) of the provided schematic-type inputs. These computer files can be stored in storage media, such as memories, whether portable or not, and the like.

Then a special type of computer file can be synthesized from the prepared layout, in a manner that incorporates the prepared layout that has the embodied schematic-type inputs. Such files are known in the industry as IC chip design files or tapeout files, and express instructions for machinery as to how to process a semiconductor wafer, so as to generate an integrated circuit that is arranged as in the incorporated layout. These IC chip design files or tapeout files can be stored on an article such as a memory device.

The synthesized tapeout file is then transferred to a semiconductor manufacturing plant, which is also known as a foundry, and so on. Transferring can be by any suitable means, such as over an electronic network. Or, a tapeout file can be recorded in a storage medium, which in turn is physically shipped to the mask manufacturer.

The received tapeout file is then used by mask making machinery as instructions for processing a semiconductor wafer. The wafer, as thus processed, now has one or more integrated circuits, each made according to the layout incorporated in the tapeout file. If more than one, then the wafer can be diced to separate them, and so on.

In this description, numerous details have been set forth in order to provide a thorough understanding. In other instances, well-known features have not been described in detail in order to not obscure unnecessarily the description.

A person skilled in the art will be able to practice the embodiments in view of this description, which is to be taken as a whole. The specific embodiments as disclosed and illustrated herein are not to be considered in a limiting sense. Indeed, it should be readily apparent to those skilled in the art that what is described herein may be modified in numerous ways. Such ways can include equivalents to what is described herein.

The following claims define certain combinations and sub-combinations of elements, features, steps, and/or functions, which are regarded as novel and non-obvious. Additional claims for other combinations and sub-combinations may be presented in this or a related document.

What is claimed is:

1. An RFID tag circuit, comprising:

a memory, the memory having

a first location for storing a first lock bit,

a second location for storing a second lock bit, wherein the first lock bit and the second lock bit have different values,

a third location for storing a pointer configured to point to one of the first lock bit and the second lock bit, wherein the pointer is configurable to stop pointing to the first lock bit and start pointing instead to the second lock bit responsive to the tag circuit receiving a partial-kill command, and

a section having an operable functionality if the pointed to one of the first and the second lock bits has a first value, but lacking the operable functionality if the pointed to one of the first and the second lock bits has a second value; and

a modulator able to cause a reply to be backscattered regardless of whether the pointer is configured to point to the first lock bit or to the second lock bit.

2. The circuit of claim **1**, in which

the operable functionality includes reading the memory section.

3. The circuit of claim **1**, in which

the operable functionality includes writing to the memory section.

4. The circuit of claim **1**, in which

the operable functionality includes read-locking the memory section.

5. The circuit of claim **1**, in which

the operable functionality includes write-locking the memory section.

6. The circuit of claim **1**, in which

the pointer is determined at tag power-up.

7. The circuit of claim **1**, in which

once the pointer has been configured by the partial-kill command, it cannot be configured to start pointing back to the first lock bit.

8. The circuit of claim **1**, in which

the pointer becomes configured by acquiring a value that is carried as a payload of the partial-kill command.

9. A method for an RFID tag, comprising:

receiving a first command;

responsive to the first command, operating a functionality of a section of a memory of the RFID tag if a pointed to one of a first lock bit and a second lock bits stored in the memory has a first value, but not operating the functionality if the pointed to one of the first and second lock bits has a second value, the pointing by a pointer configured to point to one of the first and second lock bits, wherein the first lock bit and the second lock bit have different values and the pointer is configurable to stop pointing to the first lock bit and start pointing instead to the second lock bit responsive to the tag circuit receiving a partial-kill command; and

backscattering a reply regardless of whether the functionality was operated or not.

10. The method of claim **9**, in which

the reply is backscattered in response to the first command.

11. The method of claim **9**, further comprising:

losing power;

receiving power again;

powering up responsive to receiving power again;

then receiving a second command; and

in which the reply is backscattered in response to the second command, but no reply is backscattered in response to the first command.

12. The method of claim **9**, in which

the operable functionality includes reading the memory section.

13. The method of claim **9**, in which

the operable functionality includes writing to the memory section.

14. The method of claim **9**, in which

the operable functionality includes read-locking the memory section.

15. The method of claim **9**, in which

the operable functionality includes write-locking the memory section.

16. The method of claim **9**, further comprising:

powering up before receiving the first command, and

in which the pointer is looked up responsive to powering up.

17. The method of claim **9**, in which

once the pointer has been configured by the partial-kill command, it cannot be configured to start pointing back to the first lock bit.

18. The method of claim **9**, in which

the pointer becomes configured by acquiring a value that is carried as a payload of the partial-kill command.

19. An RFID tag, comprising:

an antenna;

a memory, the memory having

a first location for storing a first lock bit,

a second location for storing a second lock bit, wherein the first lock bit and the second lock bit have different values,

a third location for storing a pointer configured to point to one of the first lock bit and the second lock bit, wherein the pointer is configurable to stop pointing to the first lock bit and start pointing instead to the second lock bit responsive to the tag receiving a partial-kill command, and

a section having an operable functionality if the pointed to one of the first and the second lock bits has a first value, but lacking the operable functionality if the pointed to one of the first and the second lock bits has a second value; and

a modulator able to cause the antenna to backscatter a reply regardless of whether the pointer is configured to point to the first lock bit or to the second lock bit.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

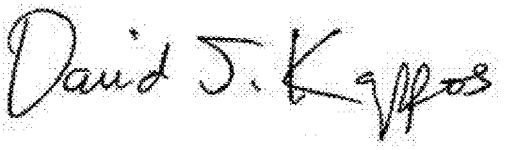
PATENT NO. : 7,872,582 B1
APPLICATION NO. : 11/872774
DATED : January 18, 2011
INVENTOR(S) : Diorio et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 9, line 30, please delete "“1”" and insert -- "1" --, therefor.

Column 11, line 16, please delete "command" and insert -- command. --, therefor.

Signed and Sealed this
Fifth Day of April, 2011



David J. Kappos
Director of the United States Patent and Trademark Office