US00RE43382E

(19) **United States**

(12) **Reissued Patent**

Wood, Jr.

(10) **Patent Number: US RE43,382 E**

(45) **Date of Reissued Patent: *May 15, 2012**

(54) **METHOD OF ADDRESSING MESSAGES AND COMMUNICATIONS SYSTEMS**

(75) Inventor: **Clifton W. Wood, Jr.**, Tulsa, OK (US)

(73) Assignee: **Round Rock Research, LLC**, Mount Kisco, NY (US)

(*) Notice: This patent is subject to a terminal disclaimer.

(21) Appl. No.: **12/701,563**

(22) Filed: **Feb. 7, 2010**
(Under 37 CFR 1.47)

Related U.S. Patent Documents

Reissue of:

(64) Patent No.: **6,307,847**
Issued: **Oct. 23, 2001**
Appl. No.: **09/617,390**
Filed: **Jul. 17, 2000**

U.S. Applications:

(63) Continuation of application No. 10/693,696, filed on Oct. 23, 2003, now Pat. No. Re. 41,530, which is a continuation of application No. 09/026,043, filed on Feb. 19, 1998, now Pat. No. 6,118,789.

(51) **Int. Cl.**
H04W 4/00 (2009.01)

(52) **U.S. Cl.** **370/329**; 370/346; 370/347

(58) **Field of Classification Search** 370/329, 370/346, 347, 460, 408, 230, 437, 441, 442, 370/449, 458, 463, 342, 447, 445, 448, 432, 370/461, 475, 345, 348
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,075,632 A 2/1978 Baldwin et al.
(Continued)

FOREIGN PATENT DOCUMENTS

EP 779520 9/1997
(Continued)

OTHER PUBLICATIONS

Auto-ID Center, Massachusetts Institute of Technology, "13.56 MHz ISM Band Class 1 Radio Frequency Identification Tag Interface Specification: Recommended Standard," Technical Report, Feb. 1, 2003.
(Continued)

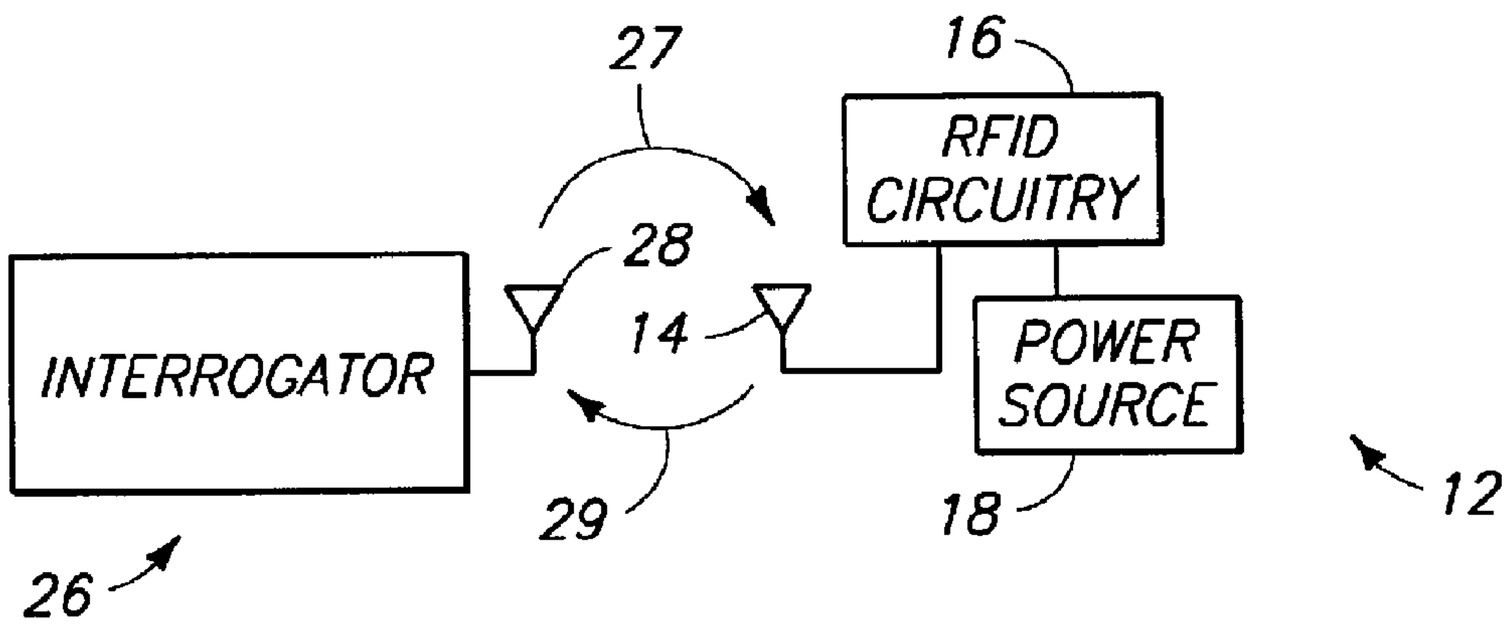
Primary Examiner — Brian Nguyen

(74) *Attorney, Agent, or Firm* — Gazdzinski & Associates, PC

(57) **ABSTRACT**

A method **[**of**]** *and apparatus for* establishing wireless communications between an interrogator and individual ones of multiple wireless identification devices**[**, the method comprising utilizing a tree search method to establish communications without collision between the interrogator and individual ones of the multiple wireless identification devices, a search tree being defined for the tree search method, the tree having multiple levels respectively representing subgroups of the multiple wireless identification devices, the method further comprising starting the tree search at a selectable level of the search tree. A communications system comprising an interrogator, and a plurality of wireless identification devices configured to communicate with the interrogator in a wireless fashion, the respective wireless identification devices having a unique identification number, the interrogator being configured to employ a tree search technique to determine the unique identification numbers of the different wireless identification devices so as to be able to establish communications between the interrogator and individual ones of the multiple wireless identification devices without collision by multiple wireless identification devices attempting to respond to the interrogator at the same time, wherein the interrogator is configured to start the tree search at a selectable level of the search tree**]**. *In one embodiment, the interrogator transmits a first request indicating a subgroup of random numbers out of a total number of possible random numbers. The wireless identification devices each determine if the random number generated by each wireless identification device falls within the subgroup, and if so, the wireless identification device responds to the interrogator. If a collision between wireless identification device responses is detected by the interrogator, the interrogator transmits a second request indicating a subgroup of random numbers.*

46 Claims, 3 Drawing Sheets



U.S. PATENT DOCUMENTS

4,761,778	A	8/1988	Hui	
4,796,023	A	1/1989	King	
4,799,059	A	1/1989	Grindahl et al.	
4,845,504	A	7/1989	Roberts et al.	
4,862,453	A	8/1989	West et al.	
4,926,182	A	5/1990	Ohta et al.	
4,955,018	A	9/1990	Twitty et al.	
4,969,146	A	11/1990	Twitty et al.	
5,019,813	A	5/1991	Kip et al.	
5,025,486	A	6/1991	Klughart	
5,046,066	A	9/1991	Messenger	
5,055,968	A	10/1991	Nishi et al.	
5,121,407	A	6/1992	Partyka et al.	
5,124,697	A	6/1992	Moore	
5,142,694	A	8/1992	Jackson et al.	
5,144,313	A	9/1992	Kirknes	
5,144,668	A	9/1992	Malek et al.	
5,150,114	A	9/1992	Johansson	
5,150,310	A	9/1992	Greenspun et al.	
5,164,985	A	11/1992	Nysen et al.	
5,168,510	A	12/1992	Hill	
5,194,860	A	3/1993	Jones et al.	
5,231,646	A	7/1993	Heath et al.	
5,266,925	A	11/1993	Vercellotti et al.	
5,307,463	A	4/1994	Hyatt et al.	
5,365,551	A	11/1994	Snodgrass et al.	
5,373,503	A	12/1994	Chen	
5,449,296	A	9/1995	Jacobsen et al.	
5,461,627	A	10/1995	Rypinski	
5,479,416	A	12/1995	Snodgrass et al.	
5,500,650	A	3/1996	Snodgrass et al.	
5,530,702	A	6/1996	Palmer et al.	
5,550,547	A	8/1996	Chan et al.	
5,583,850	A	12/1996	Snodgrass et al.	
5,608,739	A	3/1997	Snodgrass et al.	
5,619,648	A	4/1997	Canale et al.	
5,621,412	A	4/1997	Sharpe et al.	
5,625,628	A	4/1997	Heath	
5,627,544	A	5/1997	Snodgrass et al.	
5,640,151	A	6/1997	Reis et al.	
5,649,296	A	7/1997	MacLellan et al.	
5,686,902	A	11/1997	Reis et al.	
5,790,946	A	8/1998	Rotzoll	
5,805,586	A	9/1998	Perreault et al.	
5,841,770	A	11/1998	Snodgrass et al.	
5,914,671	A	6/1999	Tuttle	
5,936,560	A	8/1999	Higuchi	
5,940,006	A	8/1999	MacLellan et al.	
5,942,987	A	8/1999	Heinrich et al.	
5,952,922	A	9/1999	Shober	
5,966,471	A	10/1999	Fisher et al.	
5,974,078	A	10/1999	Tuttle et al.	
5,988,510	A	11/1999	Tuttle et al.	
6,038,455	A	3/2000	Gardner et al.	
6,061,344	A	5/2000	Wood, Jr.	
6,072,801	A	6/2000	Wood, Jr. et al.	
6,075,973	A	6/2000	Greeff et al.	
6,097,292	A	8/2000	Kelly et al.	
6,104,333	A	8/2000	Wood, Jr.	
6,118,789	A	9/2000	Wood, Jr.	
6,130,602	A	10/2000	O'Toole et al.	
6,130,623	A *	10/2000	MacLellan et al.	340/5.1
6,150,921	A	11/2000	Werb et al.	
6,157,633	A	12/2000	Wright	
6,169,474	B1	1/2001	Greeff et al.	
6,177,858	B1	1/2001	Raimbault et al.	
6,185,307	B1	2/2001	Johnson, Jr.	
6,192,222	B1	2/2001	Greeff et al.	
6,216,132	B1	4/2001	Chandra et al.	
6,226,300	B1	5/2001	Hush et al.	
6,229,987	B1	5/2001	Greeff et al.	
6,243,012	B1	6/2001	Shober et al.	
6,265,962	B1	7/2001	Black et al.	
6,265,963	B1	7/2001	Wood, Jr.	
6,275,476	B1	8/2001	Wood, Jr.	
6,282,186	B1	8/2001	Wood, Jr.	
6,288,629	B1	9/2001	Cofino et al.	
6,289,209	B1	9/2001	Wood, Jr.	
6,297,727	B1 *	10/2001	Nelson, Jr.	340/10.1
6,307,847	B1	10/2001	Wood, Jr.	
6,307,848	B1	10/2001	Wood, Jr. et al.	
6,324,211	B1	11/2001	Ovard et al.	
6,356,535	B1 *	3/2002	Smith	370/278
6,415,439	B1	7/2002	Randell et al.	
6,459,726	B1	10/2002	Ovard et al.	
6,483,427	B1	11/2002	Werb	
6,566,997	B1	5/2003	Bradin	
6,570,487	B1	5/2003	Steeves	
6,707,376	B1	3/2004	Patterson et al.	
6,714,559	B1	3/2004	Meier	
6,771,634	B1	8/2004	Wright	
6,778,096	B1 *	8/2004	Ward et al.	713/1
6,784,787	B1	8/2004	Atkins	
6,850,510	B2	2/2005	Kubler et al.	
6,919,793	B2	7/2005	Heinrich et al.	
7,026,935	B2	4/2006	Diorio et al.	
7,315,522	B2	1/2008	Wood, Jr.	
7,385,477	B2	6/2008	O'Toole et al.	
RE40,686	E	3/2009	Wood, Jr. et al.	
7,639,638	B2	12/2009	Wood, Jr.	
7,672,260	B2	3/2010	Wood, Jr.	
2003/0235184	A1	12/2003	Dorenbosch	
2005/0060069	A1	3/2005	Breed et al.	
2005/0207364	A1	9/2005	Wood, Jr.	
2006/0022800	A1	2/2006	Krishna et al.	
2006/0022801	A1	2/2006	Husak et al.	
2006/0022815	A1	2/2006	Fischer	
2006/0056325	A1	3/2006	Wood, Jr.	
2007/0139164	A1	6/2007	O'Toole et al.	
2007/0176751	A1	8/2007	Cesar et al.	
2008/0007412	A1	1/2008	Wood, Jr.	
2008/0042806	A1	2/2008	Wood, Jr.	
2008/0048832	A1	2/2008	O'Toole et al.	
2008/0048835	A1	2/2008	O'Toole et al.	
2008/0129485	A1	6/2008	Tuttle	
2008/0180221	A1	7/2008	Tuttle	
2008/0297324	A1	12/2008	Tuttle	
2009/0322491	A1	12/2009	Wood, Jr.	

FOREIGN PATENT DOCUMENTS

EP	1072128	5/2008
JP	9054213	2/1997
JP	2002228809	8/2002
WO	9748216	12/1997
WO	WO 97/48216	12/1997
WO	9943127	8/1999
WO	2008094728	8/2008

OTHER PUBLICATIONS

Capetanakis, John I., "Generalized TDMA: The Multi-Accessing Tree Protocol," IEEE Transactions on Information Theory, vol. Com. 27, No. 10, pp. 1476-1484, Oct. 1979.

Capetanakis, John I., "Tree Algorithms for Packet Broadcast Channels," IEEE Transactions on Information Theory, vol. IT-25, No. 5, pp. 505-515, Sep. 1979.

CNN Money, "Manhattan Associates Announces Next-Generation Microsoft-Based RFID Solutions," located at http://money.cnn.com/services/tickerheadlines/prn/cltu045.PI.09162003122727.24911.htm, Sep. 16, 2003.

Engels, Daniel, "The Use of the Electronic Product Code," Auto-ID Center, Massachusetts Institute of Technology, Technical Report, Feb. 1, 2003.

EPC Global, Inc. "EPC Radio Frequency Identity Protocols—Class-1 Generation-2 UHF RFID—Protocol for Communications at 860 MHz-960MHz," version 1.0.9, cover sheet and pp. 37-38, Jan. 2005.

eRetailNews, "The Electronic Product Code (EPC)—A Technology Revolution?" located at http://www.eretailnews.com/features/0105epc1.htm, accessed Oct. 15, 2003.

eRetailNews, "The Electronic Product Code (EPC)," located at http://www.eretailnews.com/features/epc/htm, accessed Oct. 15, 2003.

eRetailNews, "The Electronic Product Code Schematic," located at http://eee.eretailnews.com/features/0105epcschema.htm, accessed Oct. 15, 2003.

Extended Search Report and Search Opinion for EP Patent Application No. 05016513.3, Jan. 22, 2007.
Extended Search Report and Search Opinion for EP Patent Application No. 05016514.1, Jan. 26, 2007.
Finkenzeller, Klaus, "Radio Frequency Idenitifcation—The Authors Homepage of the RFID Handbook," located at http://www.rfid-handbook.com, accessed Feb. 22, 2007.
High Tech Aid, "ISO/IEC 18000—RFID Air Interface Standards," located at http://www.hightechaid.com/standards/18000.htm, Feb. 1, 2003.
Humblet, Pierre A. et al., "Efficient Accessing of a Multiaccess Channel," Proceedings of the 19th IEEE Conference on Decision and Control including the Symposium on Adaptive Processes, pp. 624-627, Dec. 1980.
International Application No. PCT/US08/50630, International Search Report, Jun. 27, 2008.
International Application No. PCT/US08/50630, Written Opinion, Jun. 27, 2008.
International Application No. PCT/US99/02288, International Search Report, Aug. 3, 1999.
International Application No. PCT/US99/02288, Written Opinion, Jan. 27, 2000.
ISO/IEC, "Automatic Identification—Radio Frequency Identification for Item Management—Communications and Interfaces—Part 3: Physical Layer, Anti Collision System and Protocol Values at 13.56 MHz Mode 4," ISO/IEC 18000-3-4, Mar. 1, 2001.
ISO/IEC, "Automatic Identification—Radio Frequency Identification for Item Management—Communications and Interfaces—Part 3: Physical Layer, Anti-Collision System and Protocol Values at 13.56 MHz Mode 1," ISO/IEC 18000-3-1, Mar. 1, 2001.
ISO/IEC, "Identification Cards—Contactless Integrated Circuit(s) Cards—Proximity Cards—Part 1: Physical Characteristics," ISO/IEC FCD 14443-1, 1997.
ISO/IEC, "Identification Cards—Contactless Integrated Circuit(s) Cards—Proximity Cards—Part 2: Radio Frequency Power and Signal Interface," ISO/IEC FCD 14443-2, Mar. 26, 1999.
ISO/IEC, "Identification Cards—Contactless Integrated Circuit(s) Cards—Proximity Cards—Part 3: Initiation and Anticollision," ISO/IEC FDIS 14443-3:2000(E), Jul. 13, 2000.
ISO/IEC, "Identification Cards—Contactless Integrated Circuit(s) Cards—Proximity Cards—Part 4: Transmission Protocol," ISO/IEC FDIS 14443-4:2000(E), Jul. 13, 2000.
ISO/IEC, "Identification Cards—Contactless Integrated Circuit(s) Cards—Vicinity Cards—Part 1: Physical Characteristics," ISO/IEC FDIS 15693-1:2000(E), May 19, 2000.
ISO/IEC, "Identification Cards—Contactless Integrated Circuit(s) Cards—Vicinity Cards—Part 2: Interface and Initialization," ISO/IEC FDIS 15693-2:2000(E), Feb. 3, 2000.
ISO/IEC, "Identification Cards—Contactless Integrated Circuit(s) Cards—Vicinity Cards—Part 3: Anitcollision and Transmission Protocol," ISO/IEC CD 15693-3:1999(E), Nov. 17, 1999.
ISO/IEC, "Information Technology AIDC Techniques—RFID for Item Management—Air Interface—Part 3: Paramenters for Air Interface Communications at 13.56 MHz," ISO/IEC 18000-3 FCD, May 27, 2002.
Mullin, Eileen, "Electronic Product Code," Baseline Magazine, located at www.baselinemag.com/article2/0,3959,655991,00.asp, Sep. 5, 2002.
RFID Journal, "Second Source of Class 1 EPC Chips," located at http://www.rfidjournal.com/article/articleview/473/1/1/, Jun. 26, 2003.
Smart Active Labels Consortium, organization homepage located at http://www.sal-c.org, accessed Feb. 22, 2007.
Symbol Technologies, Inc., "Understanding Gen 2: What It Is, How You Will Benefit and Criteria for Vendor Assessment," white paper, Jan. 2006.
Wolf, Jack Keil, "Principles of Group Testing and an Application to the Design and Analysis of Multi-Access Protocols," NATO ASI Series E, Applied Sciences, No. 91, pp. 237-257, 1985.
Wood, Jr., Clifton W., Reissue U.S. Appl. No. 10/693,696, filed Oct. 23, 2003.
Wood, Jr., Clifton W., Reissue U.S. Appl. No. 11/859,360, filed Sep. 21, 2007.
Wood, Jr., Clifton W., Reissue U.S. Appl. No. 11/859,364, filed Sep. 21, 2007.
Wood, Jr., Clifton W., Reissue U.S. Appl. No. 11/862,121, filed Sep. 26, 2007.
Wood, Jr., Clifton W., Reissue U.S. Appl. No. 11/862,124, filed Sep. 26, 2007.
Wood, Jr., Clifton W., Reissue U.S. Appl. No. 11/862,130, filed Sep. 21, 2007.
Wood, Jr., Clifton W., Reissue U.S. Appl. No. 11/865,584, filed Oct. 1, 2007.
Wood, Jr., Clifton W., Reissue U.S. Appl. No. 12/541,882, filed Aug. 14, 2009.
Wright, Jim, "Trends and Innovations in RF Indentification," Sun Microsystems Inc. presentation, Mar. 2005.
Zebra Technologies Corporation, "Electronic Product Code (EPC)," located at http://www.rfid.zebra.com/epc/htm, accessed Oct. 15, 2003.
Wood, Jr., Clifton W., Reissue U.S. Appl. No. 10/693,697, filed Oct. 23, 2003.
Wood, Jr., Clifton W., Reissue U.S. Appl. No. 12/493,542, filed Jun. 29, 2009.
Wood, Jr., Clifton W., Reissue U.S. Appl. No. 11/865,580, filed Oct. 1, 2007.
* cited by examiner

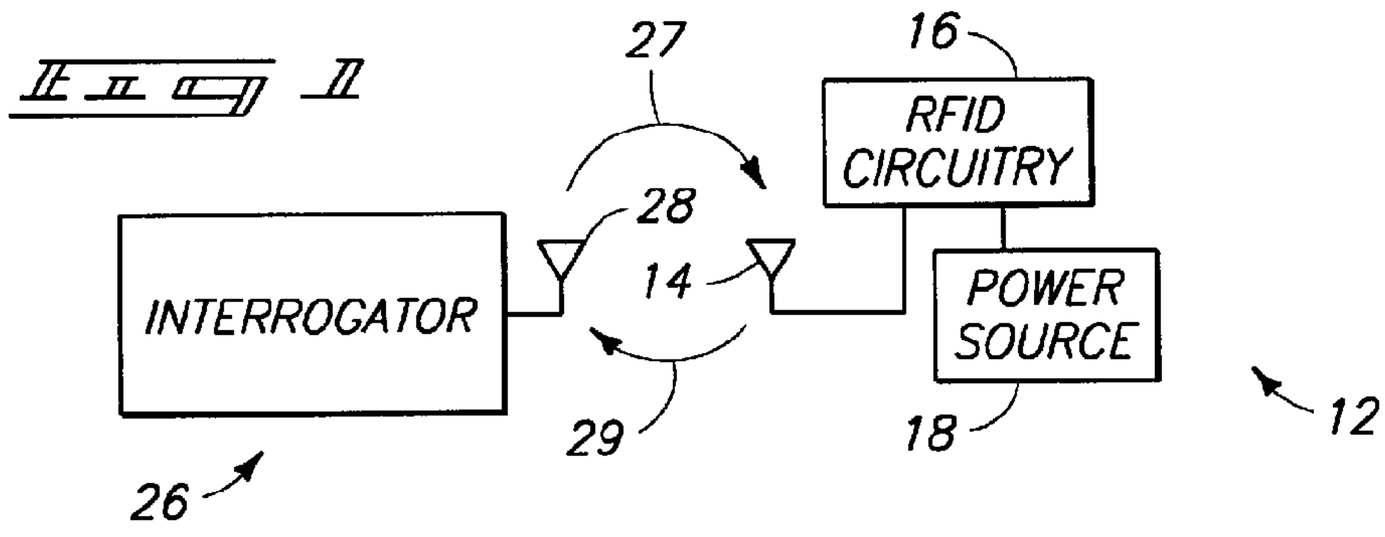


Fig. 1

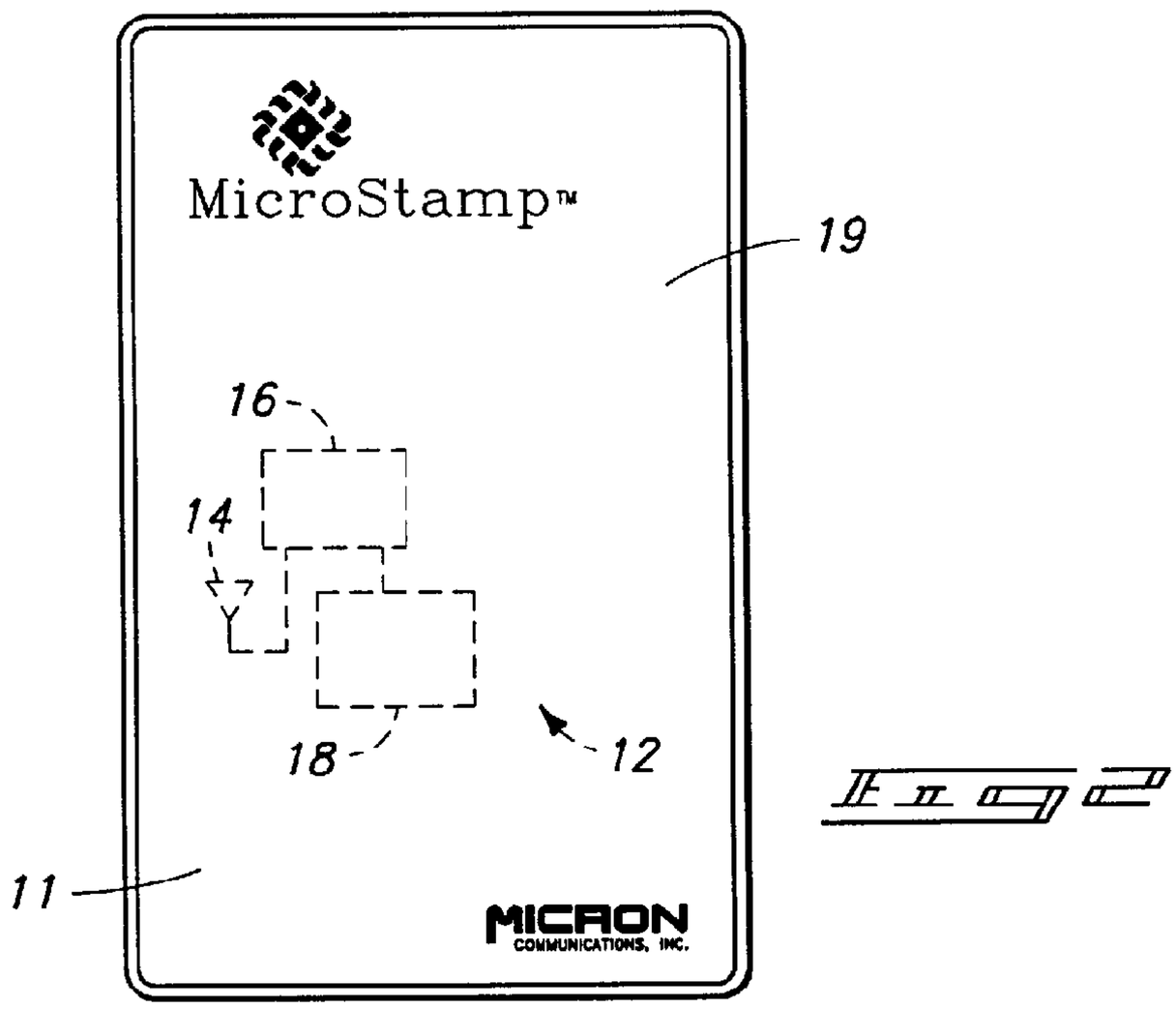


Fig. 2

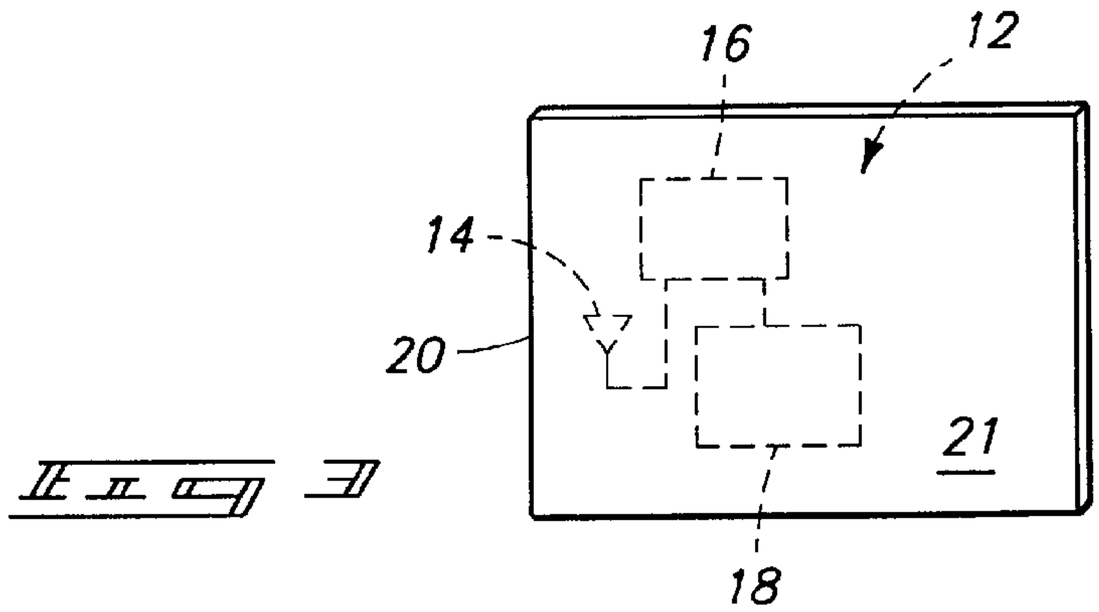


Fig. 3

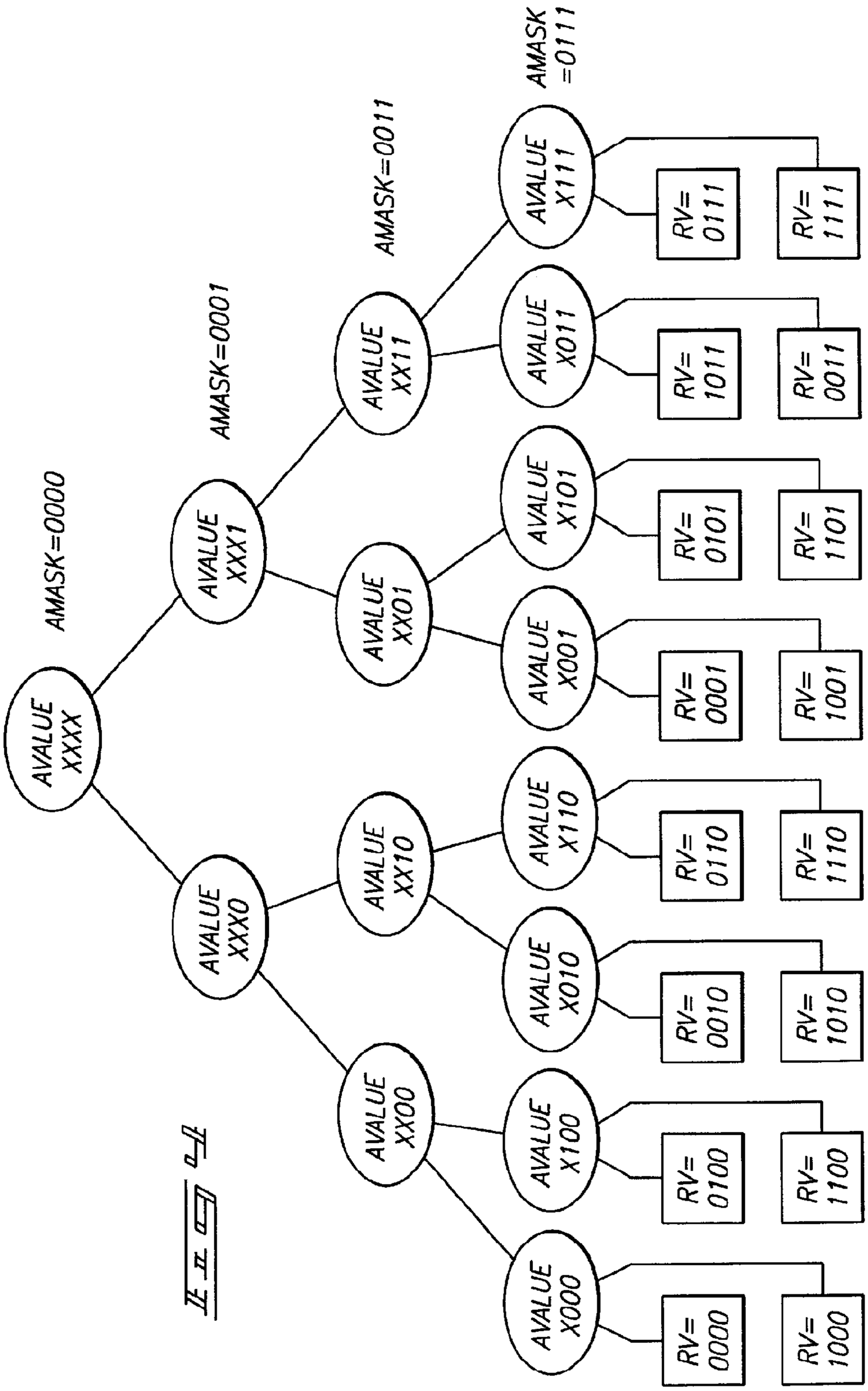

AMASK=0000
AVALUE XXXX
AMASK=0001
AVALUE XXX1
AMASK=0011
AVALUE XXX0
AMASK=0111
AVALUE XX11
AVALUE XX01
AVALUE XX10
AVALUE XX00
AVALUE X111
AVALUE X011
AVALUE X101
AVALUE X001
AVALUE X110
AVALUE X010
AVALUE X100
AVALUE X000
RV= 0111
RV= 1111
RV= 1011
RV= 0011
RV= 0101
RV= 1101
RV= 0001
RV= 1001
RV= 0110
RV= 1110
RV= 0010
RV= 1010
RV= 0100
RV= 1100
RV= 0000
RV= 1000

FIG 4

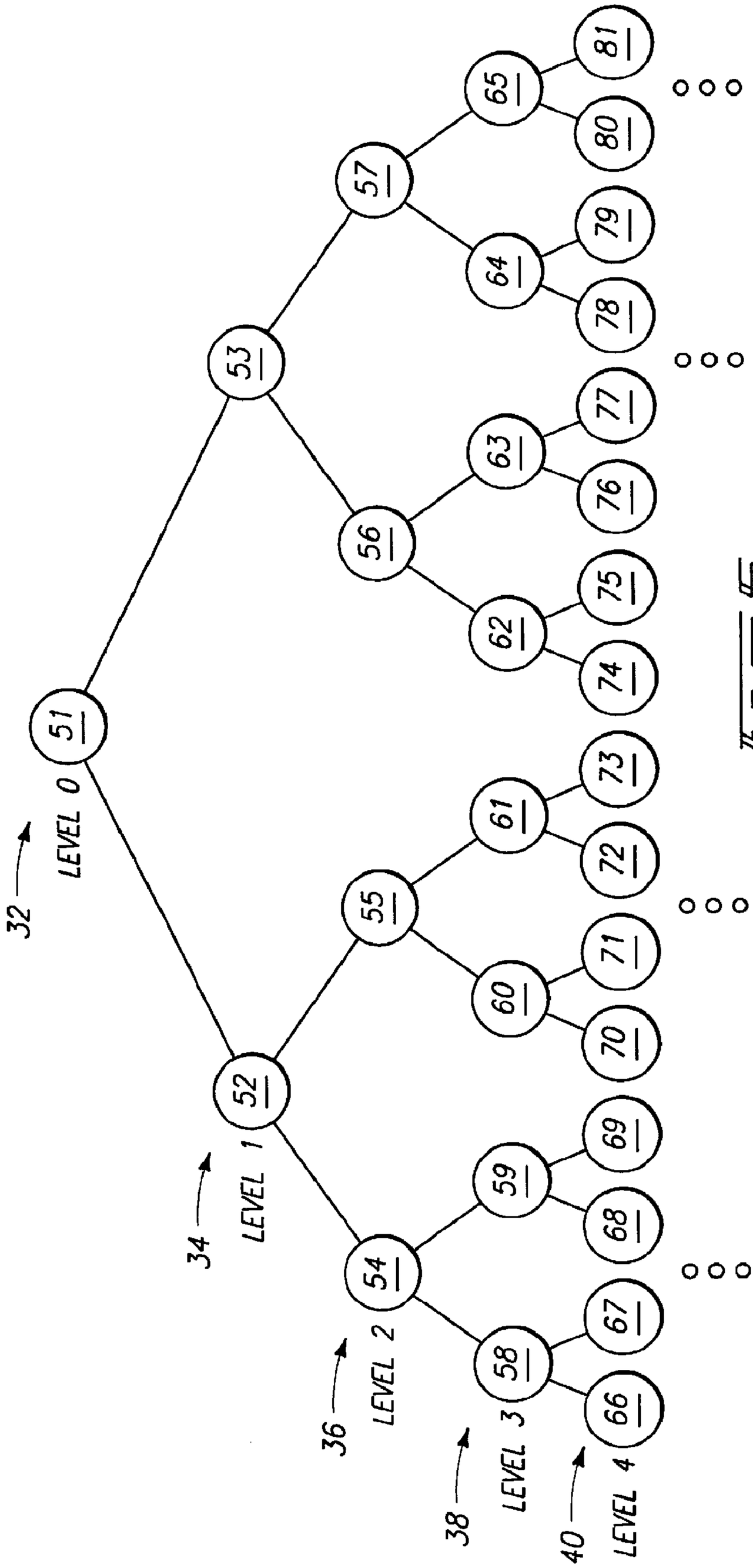

LEVEL 0
LEVEL 1
LEVEL 2
LEVEL 3
LEVEL 4
32
34
36
38
40
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81

FIG. 5

METHOD OF ADDRESSING MESSAGES AND COMMUNICATIONS SYSTEMS

Matter enclosed in heavy brackets [ ] appears in the original patent but forms no part of this reissue specification; matter printed in italics indicates the additions made by reissue.

CROSS REFERENCE TO RELATED APPLICATION

[This is a Continuation of U.S. patent application Ser. No. 09/026,043, filed Feb. 19, 1998, and titled "Method of Addressing Messages and Communications System" now U.S. Pat. No. 6,118,789.] *More than one reissue application has been filed for the reissue of U.S. Pat. No. 6,307,847, which reissue applications are the initial reissue application Ser. No. 10/693,696, filed Oct. 23, 2003, now Re. 41,530, a continuation reissue application Ser. No. 11/859,360, filed Sep. 21, 2007, a continuation reissue application Ser. No. 11/859,364, filed Sep. 21, 2007, a continuation reissue application Ser. No. 12/493,542, filed Jun. 29, 2009, and the present continuation reissue application which is a continuation application of U.S. patent application Ser. No. 10/693,696, filed Oct. 23, 2003, now Re. 41,530, which is a reissue application of U.S. Pat. No. 6,307,847 filed Jul. 12, 2000 and titled "Method of Addressing Messages and Communications Systems", which is a continuation application of U.S. patent application Ser. No. 09/026,043, filed Feb. 19, 1998, and titled "Method of Addressing Messages and Communications System", now U.S. Pat. No. 6,118,789, each of which is incorporated herein by reference in its entirety.*

TECHNICAL FIELD

This invention relates to communications protocols and to digital data communications. Still more particularly, the invention relates to data communications protocols in mediums such as radio communication or the like. The invention also relates to radio frequency identification devices for inventory control, object monitoring, determining the existence, location or movement of objects, or for remote automated payment.

BACKGROUND OF THE INVENTION

Communications protocols are used in various applications. For example, communications protocols can be used in electronic identification systems. As large numbers of objects are moved in inventory, product manufacturing, and merchandising operations, there is a continuous challenge to accurately monitor the location and flow of objects. Additionally, there is a continuing goal to interrogate the location of objects in an inexpensive and streamlined manner. One way of tracking objects is with an electronic identification system.

One presently available electronic identification system utilizes a magnetic coupling system. In some cases, an identification device may be provided with a unique identification code in order to distinguish between a number of different devices. Typically, the devices are entirely passive (have no power supply), which results in a small and portable package. However, such identification systems are only capable of operation over a relatively short range, limited by the size of a magnetic field used to supply power to the devices and to communicate with the devices.

Another wireless electronic identification system utilizes a large active transponder device affixed to an object to be monitored which receives a signal from an interrogator. The device receives the signal, then generates and transmits a responsive signal. The interrogation signal and the responsive signal are typically radio-frequency (RF) signals produced by an RF transmitter circuit. Because active devices have their own power sources, and do not need to be in close proximity to an interrogator or reader to receive power via magnetic coupling. Therefore, active transponder devices tend to be more suitable for applications requiring tracking of a tagged device that may not be in close proximity to an interrogator. For example, active transponder devices tend to be more suitable for inventory control or tracking.

Electronic identification systems can also be used for remote payment. For example, when a radio frequency identification device passes an interrogator at a toll booth, the toll booth can determine the identity of the radio frequency identification device, and thus of the owner of the device, and debit an account held by the owner for payment of toll or can receive a credit card number against which the toll can be charged. Similarly, remote payment is possible for a variety of other goods or services.

A communication system typically includes two transponders: a commander station or interrogator, and a responder station or transponder device which replies to the interrogator.

If the interrogator has prior knowledge of the identification number of a device which the interrogator is looking for, it can specify that a response is requested only from the device with that identification number. Sometimes, such information is not available. For example, there are occasions where the interrogator is attempting to determine which of multiple devices are within communication range.

When the interrogator sends a message to a transponder device requesting a reply, there is a possibility that multiple transponder devices will attempt to respond simultaneously, causing a collision, and thus causing an erroneous message to be received by the interrogator. For example, if the interrogator sends out a command requesting that all devices within a communications range identify themselves, and gets a large number of simultaneous replies, the interrogator may not be able to interpret any of these replies. Thus, arbitration schemes are employed to permit communications free of collisions.

In one arbitration scheme or system, described in commonly assigned U.S. Pat. Nos. 5,627,544; 5,583,850; 5,500,650; and 5,365,551, all to Snodgrass et al. and all incorporated herein by reference, the interrogator sends a command causing each device of a potentially large number of responding devices to select a random number from a known range and use it as that device's arbitration number. By transmitting requests for identification to various subsets of the full range of arbitration numbers, and checking for an error-free response, the interrogator determines the arbitration number of every responder station capable of communicating at the same time. Therefore, the interrogator is able to conduct subsequent uninterrupted communication with devices, one at a time, by addressing only one device.

Another arbitration scheme is referred to as the Aloha or slotted Aloha scheme. This scheme is discussed in various references relating to communications, such as Digital Communications: Fundamentals and Applications, Bernard Sklar, published January 1988 by Prentice Hall. In this type of scheme, a device will respond to an interrogator using one of many time domain slots selected randomly by the device. A problem with the Aloha scheme is that if there are many

devices, or potentially many devices in the field (i.e. in communications range, capable of responding) then there must be many available slots or many collisions will occur. Having many available slots slows down replies. If the magnitude of the number of devices in a field is unknown, then many slots are needed. This results in the system slowing down significantly because the reply time equals the number of slots multiplied by the time period required for one reply.

An electronic identification system which can be used as a radio frequency identification device, arbitration schemes, and various applications for such devices are described in detail in commonly assigned U.S. patent application Ser. No. 08/705,043, filed Aug. 29, 1996, **[**and**]** *now U.S. Pat. No. 6,130,602, which is* incorporated herein by reference.

SUMMARY OF THE INVENTION

The invention provides a wireless identification device configured to provide a signal to identify the device in response to an interrogation signal.

One aspect of the invention provides a method of establishing wireless communications between an interrogator and individual ones of multiple wireless identification devices. The method comprises utilizing a tree search method to establish communications without collision between the interrogator and individual ones of the multiple wireless identification devices. A search tree is defined for the tree search method. The tree has multiple levels respectively representing subgroups of the multiple wireless identification devices. The method further comprising starting the tree search at a selectable level of the search tree. In one aspect of the invention, the method further comprises determining the maximum possible number of wireless identification devices that could communicate with the interrogator, and selecting a level of the search tree based on the determined maximum possible number of wireless identification devices that could communicate with the interrogator. In another aspect of the invention, the method further comprises starting the tree search at a level determined by taking the base two logarithm of the determined maximum possible number, wherein the level of the tree containing all subgroups is considered level zero, and lower levels are numbered consecutively.

Another aspect of the invention provides a communications system comprising an interrogator, and a plurality of wireless identification devices configured to communicate with the interrogator in a wireless fashion. The respective wireless identification devices have a unique identification number. The interrogator is configured to employ a tree search technique to determine the unique identification numbers of the different wireless identification devices so as to be able to establish communications between the interrogator and individual ones of the multiple wireless identification devices without collision by multiple wireless identification devices attempting to respond to the interrogator at the same time. The interrogator is configured to start the tree search at a selectable level of the search tree.

One aspect of the invention provides a radio frequency identification device comprising an integrated circuit including a receiver, a transmitter, and a microprocessor. In one embodiment, the integrated circuit is a monolithic single die single metal layer integrated circuit including the receiver, the transmitter, and the microprocessor. The device of this embodiment includes an active transponder, instead of a transponder which relies on magnetic coupling for power, and therefore has a much greater range.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the invention are described below with reference to the following accompanying drawings.

FIG. **1** is a high level circuit schematic showing an interrogator and a radio frequency identification device embodying the invention.

FIG. **2** is a front view of a housing, in the form of a badge or card, supporting the circuit of FIG. **1** according to one embodiment the invention.

FIG. **3** is a front view of a housing supporting the circuit of FIG. **1** according to another embodiment of the invention.

FIG. **4** is a diagram illustrating a tree splitting sort method for establishing communication with a radio frequency identification device in a field of a plurality of such devices.

FIG. **5**. is a diagram illustrating a modified tree splitting sort method for establishing communication with a radio frequency identification device in a field of a plurality of such devices.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

This disclosure of the invention is submitted in furtherance of the constitutional purposes of the U.S. Patent Laws "to promote the progress of science and useful arts" (Article 1, Section 8).

FIG. **1** illustrates a wireless identification device **12** in accordance with one embodiment of the invention. In the illustrated embodiment, the wireless identification device is a radio frequency data communication device **12**, and includes RFID circuitry **16**. The device **12** further includes at least one antenna **14** connected to the circuitry **16** for wireless or radio frequency transmission and reception by the circuitry **16**. In the illustrated embodiment, the RFID circuitry is defined by an integrated circuit as described in the above-incorporated patent application Ser. No. 08/705,043, filed Aug. 29, 1996, *now U.S. Pat. No. 6,130,602*. Other embodiments are possible. A power source or supply **18** is connected to the integrated circuit **16** to supply power to the integrated circuit **16**. In one embodiment, the power source **18** comprises a battery.

The device **12** transmits and receives radio frequency communications to and from an interrogator **26**. An exemplary interrogator is described in commonly assigned U.S. patent application Ser. No. 08/907,689, filed Aug. 8, 1997 **[**and**]**, *now U.S. Pat. No. 6,289,209, which is* incorporated herein by reference. Preferably, the interrogator **26** includes an antenna **28**, as well as dedicated transmitting and receiving circuitry, similar to that implemented on the integrated circuit **16**.

Generally, the interrogator **26** transmits an interrogation signal or command **27** via the antenna **28**. The device **12** receives the incoming interrogation signal via its antenna **14**. Upon receiving the signal **27**, the device **12** responds by generating and transmitting a responsive signal or reply **29**. The responsive signal **29** typically includes information that uniquely identifies, or labels the particular device **12** that is transmitting, so as to identify any object or person with which the device **12** is associated.

Although only one device **12** is shown in FIG. **1**, typically there will be multiple devices **12** that correspond with the interrogator **26**, and the particular devices **12** that are in communication with the interrogator **26** will typically change over time. In the illustrated embodiment in FIG. **1**, there is no communication between multiple devices **12**. Instead, the devices **12** respectively communicate with the interrogator

26. Multiple devices **12** can be used in the same field of an interrogator **26** (i.e., within communications range of an interrogator **26**).

The radio frequency data communication device **12** can be included in any appropriate housing or packaging. Various methods of manufacturing housings are described in commonly assigned U.S. patent application Ser. No. 08/800,037, filed Feb. 13, 1997, **[**and**]** *now U.S. Pat. No. 5,988,510, which is* incorporated herein by reference.

FIG. **2** shows but one embodiment in the form of a card or badge **19** including a housing **11** of plastic or other suitable material supporting the device **12** and the power supply **18**. In one embodiment, the front face of the badge has visual identification features such as graphics, text, information found on identification or credit cards, etc.

FIG. **3** illustrates but one alternative housing supporting the device **12**. More particularly, FIG. **3** shows a miniature housing **20** encasing the device **12** and power supply **18** to define a tag which can be supported by an object (e.g., hung from an object, affixed to an object, etc.). Although two particular types of housings have been disclosed, the device **12** can be included in any appropriate housing.

If the power supply **18** is a battery, the battery can take any suitable form. Preferably, the battery type will be selected depending on weight, size, and life requirements for a particular application. In one embodiment, the battery **18** is a thin profile button-type cell forming a small, thin energy cell more commonly utilized in watches and small electronic devices requiring a thin profile. A conventional button-type cell has a pair of electrodes, an anode formed by one face and a cathode formed by an opposite face. In an alternative embodiment, the power source **18** comprises a series connected pair of button type cells. Instead of using a battery, any suitable power source can be employed.

The circuitry **16** further includes a backscatter transmitter and is configured to provide a responsive signal to the interrogator **26** by radio frequency. More particularly, the circuitry **16** includes a transmitter, a receiver, and memory such as is described in U.S. patent application Ser. No. 08/705,043, *now U.S. Pat. No. 6,130,602*.

Radio frequency identification has emerged as a viable and affordable alternative to tagging or labeling small to large quantities of items. The interrogator **26** communicates with the devices **12** via an electromagnetic link, such as via an RF link (e.g., at microwave frequencies, in one embodiment), so all transmissions by the interrogator **26** are heard simultaneously by all devices **12** within range.

If the interrogator **26** sends out a command requesting that all devices **12** within range identify themselves, and gets a large number of simultaneous replies, the interrogator **26** may not be able to interpret any of these replies. Therefore, arbitration schemes are provided.

If the interrogator **26** has prior knowledge of the identification number of a device **12** which the interrogator **26** is looking for, it can specify that a response is requested only from the device **12** with that identification number. To target a command at a specific device **12**, (i.e., to initiate point-on-point communication), the interrogator **26** must send a number identifying a specific device **12** along with the command. At start-up, or in a new or changing environment, these identification numbers are not known by the interrogator **26**. Therefore, the interrogator **26** must identify all devices **12** in the field (within communication range) such as by determining the identification numbers of the devices **12** in the field. After this is accomplished, point-to-point communication can proceed as desired by the interrogator **26**.

Generally speaking, RFID systems are a type of multiaccess communication system. The distance between the interrogator **26** and devices **12** within the field is typically fairly short (e.g., several meters), so packet transmission time is determined primarily by packet size and baud rate. Propagation delays are negligible. In such systems, there is a potential for a large number of transmitting devices **12** and there is a need for the interrogator **26** to work in a changing environment, where different devices **12** are swapped in and out frequently (e.g., as inventory is added or removed). In such systems, the inventors have determined that the use of random access methods work effectively for contention resolution (i.e., for dealing with collisions between devices **12** attempting to respond to the interrogator **26** at the same time).

RFID systems have some characteristics that are different from other communications systems. For example, one characteristic of the illustrated RFID systems is that the devices **12** never communicate without being prompted by the interrogator **26**. This is in contrast to typical multiaccess systems where the transmitting units operate more independently. In addition, contention for the communication medium is short lived as compared to the ongoing nature of the problem in other multiaccess systems. For example, in a RFID system, after the devices **12** have been identified, the interrogator can communicate with them in a point-to-point fashion. Thus, arbitration in a RFID system is a transient rather than steady-state phenomenon. Further, the capability of a device **12** is limited by practical restrictions on size, power, and cost. The lifetime of a device **12** can often be measured in terms of number of transmissions before battery power is lost. Therefore, one of the most important measures of system performance in RFID arbitration is total time required to arbitrate a set of devices **12**. Another measure is power consumed by the devices **12** during the process. This is in contrast to the measures of throughput and packet delay in other types of multiaccess systems.

FIG. **4** illustrates one arbitration scheme that can be employed for communication between the interrogator and devices **12**. Generally, the interrogator **26** sends a command causing each device **12** of a potentially large number of responding devices **12** to select a random number from a known range and use it as that device's arbitration number. By transmitting requests for identification to various subsets of the full range of arbitration numbers, and checking for an error-free response, the interrogator **26** determines the arbitration number of every responder station capable of communicating at the same time. Therefore, the interrogator **26** is able to conduct subsequent uninterrupted communication with devices **12**, one at a time, by addressing only one device **12**.

Three variables are used: an arbitration value (AVALUE), an arbitration mask (AMASK), and a random value ID (RV). The interrogator sends an Identify command (IdentifyCmnd) causing each device of a potentially large number of responding devices to select a random number from a known range and use it as that device's arbitration number. The interrogator sends an arbitration value (AVALUE) and an arbitration mask (AMASK) to a set of devices **12**. The receiving devices **12** evaluate the following equation: (AMASK & AVALUE)== (AMASK & RV) wherein "&" is a bitwise AND function, and wherein "==" is an equality function. If the equation evaluates to "1" (TRUE), then the device **12** will reply. If the equation evaluates to "0" (FALSE), then the device **12** will not reply. By performing this in a structured manner, with the number of bits in the arbitration mask being increased by one each time, eventually a device **12** will respond with no collisions. Thus, a binary search tree methodology is employed.

An example using actual numbers will now be provided using only four bits, for simplicity, reference being made to FIG. **4**. In one embodiment, sixteen bits are used for AVALUE and AMASK. Other numbers of bits can also be employed depending, for example, on the number of devices **12** expected to be encountered in a particular application, on desired cost points, etc.

Assume, for this example, that there are two devices **12** in the field, one with a random value (RV) of 1100 (binary), and another with a random value (RV) of 1010 (binary). The interrogator is trying to establish communications without collisions being caused by the two devices **12** attempting to communicate at the same time.

The interrogator sets AVALUE to 0000 (or "don't care" for all bits, as indicated by the character "X" in FIG. **4**) and AMASK to 0000. The interrogator transmits a command to all devices **12** requesting that they identify themselves. Each of the devices **12** evaluate (AMASK & AVALUE)==(AMASK & RV) using the random value RV that the respective devices **12** selected. If the equation evaluates to "1" (TRUE), then the device **12** will reply. If the equation evaluates to "0" (FALSE), then the device **12** will not reply. In the first level of the illustrated tree, AMASK is 0000 and anything bitwise ANDed with all zeros results in all zeros, so both the devices **12** in the field respond, and there is a collision.

Next, the interrogator sets AMASK to 0001 and AVALUE to 0000 and transmits an identify command. Both devices **12** in the field have a zero for their least significant bit, and (AMASK & AVALUE)==(AMASK & RV) will be true for both devices **12**. For the device **12** with a random value of 1100, the left side of the equation is evaluated as follows (0001 & 0000)=0000. The right side is evaluated as (0001 & 1100)=0000. The left side equals the right side, so the equation is true for the device **12** with the random value of 1100. For the device **12** with a random value of 1010, the left side of the equation is evaluated as (0001 & 0000)=0000. The right side is evaluated as (0001 & 1010)=0000. The left side equals the right side, so the equation is true for the device **12** with the random value of 1010. Because the equation is true for both devices **12** in the field, both devices **12** in the field respond, and there is another collision.

Recursively, the interrogator next sets AMASK to 0011 with AVALUE still at 0000 and transmits an Identify command. (AMASK & AVALUE)==(AMASK & RV) is evaluated for both devices **12**. For the device **12** with a random value of 1100, the left side of the equation is evaluated as follows (0011 & 0000)=0000. The right side is evaluated as (0011 & 1100)=0000. The left side equals the right side, so the equation is true for the device **12** with the random value of 1100, so this device **12** responds. For the device **12** with a random value of 1010, the left side of the equation is evaluated as (0011 & 0000)=0000. The right side is evaluated as (0011 & 1010)=0010. The left side does not equal the right side, so the equation is false for the device **12** with the random value of 1010, and this device **12** does not respond. Therefore, there is no collision, and the interrogator can determine the identity (e.g., an identification number) for the device **12** that does respond.

De-recursion takes place, and the devices **12** to the right for the same AMASK level are accessed when AVALUE is set at 0010, and AMASK is set to 0011.

The device **12** with the random value of 1010 receives a command and evaluates the equation (AMASK & AVALUE)==(AMASK & RV). The left side of the equation is evaluated as (0011 & 0010)=0010. The right side of the equation is evaluated as (0011 & 1010)=0010. The right side equals the left side, so the equation is true for the device **12** with the random value of 1010. Because there are no other devices **12** in the subtree, a good reply is returned by the device **12** with the random value of 1010. There is no collision, and the interrogator **26** can determine the identity (e.g., an identification number) for the device **12** that does respond.

By recursion, what is meant is that a function makes a call to itself. In other words, the function calls itself within the body of the function. After the called function returns, de-recursion takes place and execution continues at the place just after the function call; i.e. at the beginning of the statement after the function call.

For instance, consider a function that has four statements (numbered **1**,**2**,**3**,**4**) in it, and the second statement is a recursive call. Assume that the fourth statement is a return statement. The first time through the loop (iteration **1**) the function executes the statement **2** and (because it is a recursive call) calls itself causing iteration **2** to occur. When iteration **2** gets to statement **2**, it calls itself making iteration **3**. During execution in iteration **3** of statement **1**, assume that the function does a return. The information that was saved on the stack from iteration **2** is loaded and the function resumes execution at statement **3** (in iteration **2**), followed by the execution of statement **4** which is also a return statement. Since there are no more statements in the function, the function de-recurses to iteration **1**. Iteration **1**, had previously recursively called itself in statement **2**. Therefore, it now executes statement **3** (in iteration **1**). Following that it executes a return at statement **4**. Recursion is known in the art.

Consider the following code which can be used to implement operation of the method shown in FIG. **4** and described above.

```
Arbitrate(AMASK, AVALUE)
  {
  collision=IdentifyCmnd(AMASK, AVALUE)
  if (collision) then
          {
              /* recursive call for left side */
            Arbitrate((AMASK>>l)+l, AVALUE)
              /* recursive call for right side */
       Arbitrate((AMASK>>l)+l, AVALUE+(AMASK+1))
    } /* endif */
}/* return */
```

The symbol "<<" represents a bitwise left shift. "<<" means shift left by one place. Thus, 0001<<1 would be 0010. Note, however, that AMASK is originally called with a value of zero, and 0000<<1 is still 0000. Therefore, for the first recursive call, AMASK=(AMASK<<1)+1. So for the first recursive call, the value of AMASK is 0000+0001=0001. For the second call, AMASK=(0001<<)+1=0010+1=0011. For the third recursive call, AMASK=(0011<<1)+1=0110+1=0111.

The routine generates values for AMASK and AVALUE to be used by the interrogator in an identify command "IdentifyCmnd." Note that the routine calls itself if there is a collision. De-recursion occurs when there is no collision. AVALUE and AMASK would have values such as the following assuming collisions take place all the way down to the bottom of the tree.

AVALUE	AMASK
0000	0000
0000	0001

-continued

AVALUE	AMASK
0000	0011
0000	0111
0000	1111*
1000	1111*
0100	0111
0100	1111*
1100	1111*

This sequence of AMASK, AVALUE binary numbers assumes that there are collisions all the way down to the bottom of the tree, at which point the Identify command sent by the interrogator is finally successful so that no collision occurs. Rows in the table for which the interrogator is successful in receiving a reply without collision are marked with the symbol "*". Note that if the Identify command was successful at, for example, the third line in the table then the interrogator would stop going down that branch of the tree and start down another, so the sequence would be as shown in the following table.

AVALUE	AMASK
0000	0000
0000	0001
0000	0011*
0010	0011
. . .	. . .

This method is referred to as a splitting method. It works by splitting groups of colliding devices **12** into subsets that are resolved in turn. The splitting method can also be viewed as a type of tree search. Each split moves the method one level deeper in the tree.

Either depth-first or breadth-first traversals of the tree can be employed Depth first traversals are performed by using recursion, as is employed in the code listed above. Breadth-first traversals are accomplished by using a queue instead of recursion. The following is an example of code for performing a breadth-first traversal.

```
Arbitrate(AMASK, AVALUE)
  {
  enqueue(0,0)
  while (queue !=empty)
    (AMASK,AVALUE) =0 dequeue( )
    collision=IdentifyCmnd(AMASK, AVALUE)
    if (collision) then
    {
      TEMP = AMASK+1
      NEW_AMASK = (AMASK>>1)+1
      enqueue(NEW_AMASK, AVALUE)
      enqueue(NEW_AMASK, AVALUE+TEMP)
      }/* endif */
  endwhile
  }/* return */
```

The symbol "!=" means not equal to. AVALUE and AMASK would have values such as those indicated in the following table for such code.

AVALUE	AMASK
0000	0000
0000	0001
0001	0001
0000	0011
0010	0011
0001	0011
0011	0011
0000	0111
0100	0111
. . .	. . .

Rows in the table for which the interrogator is successful in receiving a reply without collision are marked with the symbol "*".

FIG. **5** illustrates an embodiment wherein the interrogator **26** starts the tree search at a selectable level of the search tree. The search tree has a plurality of nodes **51**, **52**, **53**, **54** etc. at respective levels. The size of subgroups of random values decrease in size by half with each node descended. The upper bound of the number of devices **12** in the field (the maximum possible number of devices that could communicate with the interrogator) is determined, and the tree search method is started at a level **32**, **34**, **36**, **38**, or **40** in the tree depending on the determined upper bound. In one embodiment, the maximum number of devices **12** potentially capable of responding to the interrogator is determined manually and input into the interrogator **26** via an input device such as a keyboard, graphical user interface, mouse, or other interface. The level of the search tree on which to start the tree search is selected based on the determined maximum possible number of wireless identification devices that could communicate with the interrogator.

The tree search is started at a level determined by taking the base two logarithm of the determined maximum possible number. More particularly, the tree search is started at a level determined by taking the base two logarithm of the power of two nearest the determined maximum possible number of devices **12**. The level of the tree containing all subgroups of random values is considered level zero (see FIG. **5**), and lower levels are numbered **1**, **2**, **3**, **4**, etc. consecutively.

By determining the upper bound of the number of devices **12** in the field, and starting the tree search at an appropriate level, the number of collisions is reduced, the battery life of the devices **12** is increased, and arbitration time is reduced.

For example, for the search tree shown in FIG. **5**, if it is known that there are seven devices **12** in the field, starting at node **51** (level **0**) results in a collision. Starting at level **1** (nodes **52** and **53**) also results in a collision. The same is true for nodes **54**, **55**, **56**, and **57** in level **2**. If there are seven devices **12** in the field, the nearest power of two to seven is the level at which the tree search should be started. Log_2 8=3, so the tree search should be started at level **3** if there are seven devices **12** in the field.

AVALUE and AMASK would have values such as the following assuming collisions take place from level **3** all the way down to the bottom of the tree.

AVALUE	AMASK
0000	0111
0000	1111*
1000	1111*
0100	0111

-continued

AVALUE	AMASK
0100	1111*
1100	1111*

Rows in the table for which the interrogator is successful in receiving a reply without collision are marked with the symbol "*".

In operation, the interrogator transmits a command requesting devices **12** having random values RV within a specified group of random values to respond, the specified group being chosen in response to the determined maximum number. Devices **12** receiving the command respectively determine if their chosen random values fall within the specified group and, if so, send a reply to the interrogator. The interrogator determines if a collision occurred between devices that sent a reply and, if so, creates a new, smaller, specified group, descending in the tree, as described above in connection with FIG. **4**.

Another arbitration method that can be employed is referred to as the "Aloha" method. In the Aloha method, every time a device **12** is involved in a collision, it waits a random period of time before retransmitting. This method can be improved by dividing time into equally sized slots and forcing transmissions to be aligned with one of these slots. This is referred to as "slotted Aloha." In operation, the interrogator asks all devices **12** in the field to transmit their identification numbers in the next time slot. If the response is garbled, the interrogator informs the devices **12** that a collision has occurred, and the slotted Aloha scheme is put into action. This means that each device **12** in the field responds within an arbitrary slot determined by a randomly selected value. In other words, in each successive time slot, the devices **12** decide to transmit their identification number with a certain probability.

The Aloha method is based on a system operated by the University of Hawaii. In 1971, the University of Hawaii began operation of a system named Aloha. A communication satellite was used to interconnect several university computers by use of a random access protocol. The system operates as follows. Users or devices transmit at any time they desire. After transmitting, a user listens for an acknowledgment from the receiver or interrogator. Transmissions from different users will sometimes overlap in time (collide), causing reception errors in the data in each of the contending messages. The errors are detected by the receiver, and the receiver sends a negative acknowledgment to the users. When a negative acknowledgment is received, the messages are retransmitted by the colliding users after a random delay. If the colliding users attempted to retransmit without the random delay, they would collide again. If the user does not receive either an acknowledgment or a negative acknowledgment within a certain amount of time, the user "times out" and retransmits the message.

There is a scheme known as slotted Aloha which improves the Aloha scheme by requiring a small amount of coordination among stations. In the slotted Aloha scheme, a sequence of coordination pulses is broadcast to all stations (devices). As is the case with the pure Aloha scheme, packet lengths are constant. Messages are required to be sent in a slot time between synchronization pulses, and can be started only at the beginning of a time slot. This reduces the rate of collisions because only messages transmitted in the same slot can interfere with one another. The retransmission mode of the pure Aloha scheme is modified for slotted Aloha such that if a negative acknowledgment occurs, the device retransmits after a random delay of an integer number of slot times.

Aloha methods are described in [a] commonly assigned [patent application naming Clifton W. Wood, Jr. as an inventor,] U.S. patent application Ser. No. 09/026,248, filed Feb. 19, 1998, [titled "Method of Addressing Messages and Communications System," filed concurrently herewith, and] *now U.S. Pat. No. 6,275,476, which is* incorporated herein by reference.

In one alternative embodiment, an Aloha method (such as the method described in the commonly assigned patent application mentioned above) is combined with determining the upper bound on a set of devices and starting at a level in the tree depending on the determined upper bound, such as by combining an Aloha method with the method shown and described in connection with FIG. **5**. For example, in one embodiment, devices **12** sending a reply to the interrogator **26** do so within a randomly selected time slot of a number of slots.

In another embodiment, levels of the search tree are skipped. Skipping levels in the tree, after a collision caused by multiple devices **12** responding, reduces the number of subsequent collisions without adding significantly to the number of no replies. In real-time systems, it is desirable to have quick arbitration sessions on a set of devices **12** whose unique identification numbers are unknown. Level skipping reduces the number of collisions, both reducing arbitration time and conserving battery life on a set of devices **12**. In one embodiment, every other level is skipped. In alternative embodiments, more than one level is skipped each time.

The trade off that must be considered in determining how many (if any) levels to skip with each decent down the tree is as follows. Skipping levels reduces the number of collisions, thus saving battery power in the devices **12**. Skipping deeper (skipping more than one level) further reduces the number of collisions. The more levels that are skipped, the greater the reduction in collisions. However, skipping levels results in longer search times because the number of queries (Identify commands) increases. The more levels that are skipped, the longer the search times. Skipping just one level has an almost negligible effect on search time, but drastically reduces the number of collisions. If more than one level is skipped, search time increases substantially. Skipping every other level drastically reduces the number of collisions and saves battery power without significantly increasing the number of queries.

Level skipping methods are described in a commonly assigned patent application 09/026,045 naming Clifton W. Wood, Jr. and Don Hush as inventors, titled "Method of Addressing Messages, Method of Establishing Wireless Communications, and Communications Systems," filed concurrently herewith, now U.S. Pat. No. 6,072,801, and incorporated herein by reference.

In one alternative embodiment, a level skipping method is combined with determining the upper bound on a set of devices and starting at a level in the tree depending on the determined upper bound, such as by combining a level skipping method with the method shown and described in connection with FIG. **5**.

In yet another alternative embodiment, both a level skipping method and an Aloha method (as described in the commonly assigned applications described above) are combined with the method shown and described in connection with FIG. **5**.

In compliance with the statute, the invention has been described in language more or less specific as to structural and methodical features. It is to be understood, however, that the invention is not limited to the specific features shown and

described, since the means herein disclosed comprise preferred forms of putting the invention into effect. The invention is, therefore, claimed in any of its forms or modifications within the proper scope of the appended claims appropriately interpreted in accordance with the doctrine of equivalents.

What is claimed is:

[1. A method of establishing wireless communications between an interrogator and individual ones of multiple wireless identification devices, the wireless identification devices having respective identification numbers and being addressable by specifying identification numbers with any one of multiple possible degrees of precision, the method comprising utilizing a tree search in an arbitration scheme to determine a degree of precision necessary to establish one-on-one communications between the interrogator and individual ones of the multiple wireless identification devices, a search tree being defined for the tree search method, the tree having multiple selectable levels respectively representing subgroups of the multiple wireless identification devices, the level at which a tree search starts being variable the method further comprising starting the tree search at any selectable level of the search tree.]

[2. A method in accordance with claim 1 and further comprising determining the maximum possible number of wireless identification devices that could communicate with the interrogator, and selecting a level of the search tree based on the determined maximum possible number of wireless identification devices that could communicate with the interrogator.]

[3. A method in accordance with claim 2 and further comprising starting the tree search at a level determined by taking the base two logarithm of the determined maximum possible number, wherein the level of the tree containing all subgroups is considered level zero, and lower levels are numbered consecutively.]

[4. A method in accordance with claim 2 and further comprising starting the tree search at a level determined by taking the base two logarithm of the determined maximum possible number, wherein the level of the tree containing all subgroups is considered level zero, and lower levels are numbered consecutively, and wherein the maximum number of devices in a subgroup in one level is half of the maximum number of devices in the next higher level.]

[5. A method in accordance with claim 2 and further comprising starting the tree search at a level determined by taking the base two logarithm of the power of two nearest the determined maximum possible number, wherein the level of the tree containing all subgroups is considered level zero, and lower levels are numbered consecutively, and wherein the maximum number of devices in a subgroup in one level is half of the maximum number of devices in the next higher level.]

[6. A method in accordance with claim 1 wherein the wireless identification device comprises an integrated circuit including a receiver, a modulator, and a microprocessor in communication with the receiver and modulator.]

[7. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices, the method comprising:

establishing for respective devices unique identification numbers respectively having a first predetermined number of bits;

establishing a second predetermined number of bits to be used for random values;

causing the devices to select random values, wherein respective devices choose random values independently of random values selected by the other devices;

determining the maximum number of devices potentially capable of responding to the interrogator;

transmitting a command from the interrogator requesting devices having random values within a specified group of random values to respond, by using a subset of the second predetermined number of bits, the specified group being chosen in response to the determined maximum number;

receiving the command at multiple devices, devices receiving the command respectively determining if the random value chosen by the device falls within the specified group and, if so, sending a reply to the interrogator; and

determining using the interrogator if a collision occurred between devices that sent a reply and, if so, creating a new, smaller, specified group.]

[8. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices in accordance with claim 7 wherein sending a reply to the interrogator comprises transmitting the unique identification number of the device sending the reply.]

[9. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices in accordance with claim 7 wherein sending a reply to the interrogator comprises transmitting the random value of the device sending the reply.]

[10. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices in accordance with claim 7 wherein sending a reply to the interrogator comprises transmitting both the random value of the device sending the reply and the unique identification number of the device sending the reply.]

[11. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices in accordance with claim 7 wherein, after receiving a reply without collision from a device, the interrogator sends a command individually addressed to that device.]

[12. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices, the method comprising:

causing the devices to select random values for use as arbitration numbers, wherein respective devices choose random values independently of random values selected by the other devices, the devices being addressable by specifying arbitration numbers with any one of multiple possible degrees of precision;

transmitting a command from the interrogator requesting devices having random values within a specified group of a plurality of possible groups of random values to respond, the specified group being less than the entire set of random values, the plurality of possible groups being organized in a binary tree defined by a plurality of nodes at respective levels, wherein the size of groups of random values decrease in size by half with each node descended, wherein the specified group is below a node on the tree selected based on the maximum number of devices capable of communicating with the interrogator;

receiving the command at multiple devices, devices receiving the command respectively determining if the random value chosen by the device falls within the specified group and, if so, sending a reply to the interrogator; and, if not, not sending a reply; and

determining using the interrogator if a collision occurred between devices that sent a reply and, if so, creating a new, smaller, specified group by descending in the tree.]

[13. A method of addressing messages from an interrogator to a selected one or more of a number of communications

devices in accordance with claim **12** and further including establishing a predetermined number of bits to be used for the random values.]

[**14**. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices in accordance with claim **13** wherein the predetermined number of bits to be used for the random values comprises an integer multiple of eight.]

[**15**. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices in accordance with claim **13** wherein devices sending a reply to the interrogator do so within a randomly selected time slot of a number of slots.]

[**16**. A method of addressing messages from an interrogator to a selected one or more of a number of RFID devices, the method comprising:

establishing for respective devices a predetermined number of bits to be used for random values, the predetermined number being a multiple of sixteen;

causing the devices to select random values, wherein respective devices choose random values independently of random values selected by the other devices;

transmitting a command from the interrogator requesting devices having random values within a specified group of a plurality of possible groups of random values to respond, the specified group being equal to or less than the entire set of random values, the plurality of possible groups being organized in a binary tree defined by a plurality of nodes at respective levels, wherein the maximum size of groups of random values decrease in size by half with each node descended, wherein the specified group is below a node on a level of the tree selected based on the maximum number of devices known to be capable of communicating with the interrogator;

receiving the command at multiple devices, devices receiving the command respectively determining if the random value chosen by the device falls within the specified group and, only if so, sending a reply to the interrogator, wherein sending a reply to the interrogator comprises transmitting both the random value of the device sending the reply and the unique identification number of the device sending the reply;

using the interrogator to determine if a collision occurred between devices that sent a reply and, if so, creating a new, smaller, specified group using a level of the tree different from the level used in the interrogator transmitting, the interrogator transmitting a command requesting devices having random values within the new specified group of random values to respond; and

if a reply without collision is received from a device, the interrogator subsequently sending a command individually addressed to that device.]

[**17**. A method of addressing messages from an interrogator to a selected one or more of a number of RFID devices in accordance with claim **16** and further comprising determining the maximum possible number of wireless identification devices that could communicate with the interrogator.]

[**18**. A method of addressing messages from an interrogator to a selected one or more of a number of RFID devices in accordance with claim **16** wherein selecting the level of the tree comprises taking the base two logarithm of the determined maximum possible number, wherein a level of the tree containing all subgroups is considered level zero, and lower levels are numbered consecutively.]

[**19**. A method of addressing messages from an interrogator to a selected one or more of a number of RFID devices in accordance with claim **16** wherein selecting the level of the tree comprises taking the base two logarithm of the determined maximum possible number, wherein a level of the tree containing all subgroups is considered level zero, and lower levels are numbered consecutively, and wherein the maximum number of devices in a subgroup in one level is half of the maximum number of devices in the next higher level.]

[**20**. A method of addressing messages from an interrogator to a selected one or more of a number of RFID devices in accordance with claim **16** wherein selecting the level of the tree comprises taking the base two logarithm of the power of two nearest the determined maximum possible number, wherein the level of the tree containing all subgroups is considered level zero, and lower levels are numbered consecutively, and wherein the maximum number of devices in a subgroup in one level is half of the maximum number of devices in the next higher level.]

[**21**. A method of addressing messages from an interrogator to a selected one or more of a number of RFID devices in accordance with claim **16** wherein the wireless identification device comprises an integrated circuit including a receiver, a modulator, and a microprocessor in communication with the receiver and modulator.]

[**22**. A method of addressing messages from an interrogator to a selected one or more of a number of RFID devices in accordance with claim **16** and further comprising, after the interrogator transmits a command requesting devices having random values within the new specified group of random values to respond, determining, using devices receiving the command, if their chosen random values fall within the new smaller specified group and, if so, sending a reply to the interrogator.]

[**23**. A method of addressing messages from an interrogator to a selected one or more of a number of RFID devices in accordance with claim **22** and further comprising, after the interrogator transmits a command requesting devices having random values within the new specified group of random values to respond, determining if a collision occurred between devices that sent a reply and, if so, creating a new specified group and repeating the transmitting of the command requesting devices having random values within a specified group of random values to respond using different specified groups until all of the devices within communications range are identified.]

[**24**. A communications system comprising an interrogator, and a plurality of wireless identification devices configured to communicate with the interrogator in a wireless fashion, the wireless identification devices having respective identification numbers, the interrogator being configured to employ a tree search in a search tree having multiple selectable levels, to determine the identification numbers of the different wireless identification devices with sufficient precision so as to be able to establish one-on-one communications between the interrogator and individual ones of the multiple wireless identification devices, wherein the interrogator is configured to start the tree search at any selectable level of the search tree.]

[**25**. A communications system in accordance with claim **24** wherein the tree search is a binary tree search.]

[**26**. A communications system in accordance with claim **24** wherein the wireless identification device comprises an integrated circuit including a receiver, a modulator, and a microprocessor in communication with the receiver and modulator.]

[**27**. A system comprising:

an interrogator;

a number of communications devices capable of wireless communications with the interrogator;

means for establishing a predetermined number of bits to be used as random numbers, and for causing respective devices to select random numbers respectively having the predetermined number of bits;

means for inputting a predetermined number indicative of the maximum number of devices possibly capable of communicating with the receiver;

means for causing the interrogator to transmit a command requesting devices having random values within a specified group of random values to respond, the specified group being chosen in response to the inputted predetermined number;

means for causing devices receiving the command to determine if their chosen random values fall within the specified group and, if so, send a reply to the interrogator; and

means for causing the interrogator to determine if a collision occurred between devices that sent a reply and, if so, create a new, smaller, specified group.]

[**28**. A system in accordance with claim **27** wherein sending a reply to the interrogator comprises transmitting the random value of the device sending the reply.]

[**29**. A system in accordance with claim **27** wherein the interrogator further includes means for, after receiving a reply without collision from a device, sending a command individually addressed to that device.]

[**30**. A system comprising:

an interrogator configured to communicate to a selected one or more of a number of communications devices;

a plurality of communications devices;

the devices being configured to select random values, wherein respective devices choose random values independently of random values selected by the other devices, different sized groups of devices being addressable by specifying random values with differing levels of precision;

the interrogator being configured to transmit a command requesting devices having random values within a specified group of a plurality of possible groups of random values to respond, the specified group being less than the entire set of random values, the plurality of possible groups being organized in a binary tree defined by a plurality of nodes at respective levels, wherein the size of groups of random values decrease in size by half with each node descended, wherein the specified group is below a node on the tree selected based on a predetermined maximum number of devices capable of communicating with the interrogator;

devices receiving the command being configured to respectively determine if their chosen random values fall within the specified group and, if so, send a reply to the interrogator; and, if not, not send a reply; and

the interrogator being configured to determine if a collision occurred between devices that sent a reply and, if so, create a new, smaller, specified group by descending in the tree.]

[**31**. A system in accordance with claim **30** wherein the random values respectively have a predetermined number of bits.]

[**32**. A system in accordance with claim **30** wherein respective devices are configured to store unique identification numbers of a predetermined number of bits.]

[**33**. A system in accordance with claim **30** wherein respective devices are configured to store unique identification numbers of sixteen bits.]

[**34**. A system comprising:

an interrogator configured to communicate to a selected one or more of a number of RFID devices;

a plurality of RFID devices, respective devices being configured to store unique identification numbers respectively having a first predetermined number of bits, respective devices being further configured to store a second predetermined number of bits to be used for random values, respective devices being configured to select random values independently of random values selected by the other devices;

the interrogator being configured to transmit an identify command requesting a response from devices having random values within a specified group of a plurality of possible groups or random values, the specified group being less than or equal to the entire set of random values, the plurality of possible groups being organized in a binary tree defined by a plurality of nodes at respective levels, wherein the maximum size of groups of random values decrease in size by half with each node descended, wherein the specified group is below a node on a level of the tree selected based on the maximum number of devices known to be capable of communicating with the interrogator;

devices receiving the command respectively being configured to determine if their chosen random values fall within the specified group and, only if so, send a reply to the interrogator, wherein sending a reply to the interrogator comprises transmitting both the random value of the device sending the reply and the unique identification number of the device sending the reply;

the interrogator being configured to determine if a collision occurred between devices that sent a reply and, if so, create a new, smaller, specified group using a level of the tree different from the level used in previously transmitting an identify command, the interrogator transmitting an identify command requesting devices having random values within the new specified group of random values to respond; and

the interrogator being configured to send a command individually addressed to a device after communicating with a device without a collision.]

[**35**. A system in accordance with claim **34** wherein the interrogator is configured to input and store the predetermined number.]

[**36**. A system in accordance with claim **34** wherein the devices are configured to respectively determine if their chosen random values fall within a specified group and, if so, send a reply, upon receiving respective identify commands.]

[**37**. A system in accordance with claim **36** wherein the interrogator is configured to determine if a collision occurred between devices that sent a reply in response to respective identify commands and, if so, create further new specified groups and repeat the transmitting of the identify command requesting devices having random values within a specified group of random values to respond using different specified groups until all responding devices are identified.]

38. A method, comprising:

transmitting, from a reader, an initial wireless command to start identification of a plurality of radio frequency identification (RFID) tags, the initial wireless command specifying at least two bits and requesting first RFID tags having the at least two bits to reply with at least random numbers generated on the first RFID tags as identifiers to be used by the reader in subsequent communications to individually address the first RFID tags;

determining whether there is a collision in response to the initial wireless command; identifying, from a response to the initial command, a random number generated at

an RFID tag, if there is no collision in response to the initial wireless command; and

transmitting, from the reader, a subsequent wireless command to identify RFID tags, the subsequent command specifying at least the two bits to request replies.

39. The method of claim 38, wherein the first RFID tags are to select time slots, based on random numbers generated on the first RFID tags, to reply to the initial wireless command.

40. The method of claim 39, further comprising:

transmitting, from the reader, at least one command to indicate the time slots to the first RFID tags.

41. The method of claim 38, wherein the random number is a sixteen-bit random number.

42. The method of claim 38, wherein the subsequent wireless command includes one bit more than the at least two bits specified in the initial wireless command.

43. The method of claim 38, further comprising:

transmitting, from the reader, an acknowledge command in response to the random number being identified from the response.

44. The method of claim 38, wherein the RFID tag is to further communicate to the reader at least a portion of an identification code of the RFID tag.

45. A radio frequency identification (RFID) interrogator, comprising:

one or more antennas;

a controller;

a transmitter coupled to the controller and the one or more antennas to send a first wireless radio frequency (RF) signal to start identification of individual tags of a population of RFID tags, the first RF signal requesting RFID tags having first bits specified in the first RF signal to reply, the first bits having at least two bits; and

a receiver coupled to the controller and the one or more antennas to detect a collision in response to the first RF signal and, when there is no collision in response to the first RF signal, to determine an identifier of a first RFID tag from a reply to the first RF signal;

wherein the transmitter is to subsequently use the identifier, determined from the reply to the first RF signal, to address the first RFID tag, among the population of RFID tags, for a response from the first RFID tag.

46. The interrogator of claim 45, wherein the transmitter is to further send a second wireless RF signal to specify at least the first bits and to request RFID tags having bits specified in the second RF signal to reply.

47. The interrogator of claim 45, wherein the first RF signal requests the RFID tags having the first bits specified in the first RF signal to reply with at least random numbers generated on respective RFID tags; and the first RFID tag is identified via a random number provided by the first RFID tag in the reply to the first RF signal.

48. The interrogator of claim 45, wherein a random number provided by the first RFID tag in the reply to the first RF signal has sixteen bits.

49. The interrogator of claim 45, wherein the transmitter is to further send an acknowledge signal to the first RFID tag, in response to a random number being identified from the reply.

50. A radio frequency identification (RFID) system, comprising:

a plurality of RFID tags; and

an interrogator having a range for wireless communications, the plurality of RFID tags disposed within the range for communications with the interrogator, the interrogator comprising:

at least one antenna,

a transmitter coupled to the at least one antenna to transmit a first wireless radio frequency (RF) signal to initiate a search to identify the RFID tags, the first RF signal specifying at least two bits, wherein RFID tags having the at least two bits reply to the first RF signal with at least random numbers generated on respective RFID tags, and

a receiver coupled to the at least one antenna to identify, from at least one reply to the first RF signal, a random number generated by a first RFID tag, if there is no response collision in replying to the first RF signal;

wherein the transmitter is to subsequently use the random number, identified from the reply to the first RF signal, to request a response from the first RFID tag.

51. The RFID system of claim 50, wherein each of the RFID tags having the at least two bits generates a random value to determine a time slot to reply.

52. The RFID system of claim 51, wherein the transmitter is to further transmit a plurality of second signals to indicate a plurality of time slots to reply.

53. The RFID system of claim 50, wherein the transmitter is to transmit a second signal to cause the first RFID tag to generate the random number as an identifier.

54. The RFID system of claim 53, wherein the second signal is different from the first signal.

55. The RFID system of claim 50, wherein the random number is a sixteen-bit number.

56. The RFID system of claim 50, wherein the at least two bits are a portion of the random number.

57. A radio frequency identification (RFID) system, comprising:

an interrogator to transmit an initial wireless radio frequency (RF) signal to start a search to identify RFID tags, the initial wireless RF signal specifying at least two first bits and requesting replies; and

a set of RFID tags, each tag of the set having:

an antenna,

a memory storing a plurality of bits; and

a circuit coupled to the antenna to receive the initial RF signal, to compare the at least two first bits with corresponding bits stored in the memory, to independently generate a random number as an identifier, to generate a random value to select a time slot to reply, and to reply with the random number in accordance with the time slot, if there is a match between the at least two first bits specified in the initial RF signal and the corresponding bits stored in the memory;

wherein the interrogator is to individually address a first RFID tag among the set of RFID tags, using the random number of the first RFID tag identified from a reply to the first wireless RF signal, to request a response from the first RFID tag.

58. The system of claim 57, wherein the interrogator is to further transmit at least one signal to indicate subsequent time slots for RFID tags having the at least two first bits to reply.

59. The system of claim 57, wherein the interrogator is to transmit a separate signal to cause each tag of the set to generate the random number.

60. The system of claim 59, wherein the random number is a sixteen-bits number.

61. The system of claim 59, wherein the interrogator is to further transmit an acknowledge signal if a first RFID tag is identified from a response to the initial RF signal.

62. The system of claim 57, wherein each tag of the set is to transmit the random number via backscattering.

63. A radio frequency identification (RFID) method, comprising:

transmitting, from a reader, a first wireless command to initiate identification of a population of RFID tags and a plurality of subsequent wireless commands to continue the identification of a population of RFID tags, the first command including first bits, the first command to request a set of RFID tags having the first bits to reply with identifiers of the set of RFID tags, the identifiers including random numbers individually generated by the set of RFID tags, the first bits including at least two bits;

generating, by the set of RFID tags, the random numbers independent from each other;

generating, by the set of RFID tags, random values;

replying, by the set of RFID tags, to the first command and the subsequent command with at least the random numbers of the set of RFID tags, in an order in accordance with the random values;

receiving, at the reader, a reply to the first command from a first RFID tag;

determining whether there is a collision in replying to the first command;

if there is no collision in replying to the first command, identifying from the reply a random number generated by the first RFID tag; and

transmitting a second wireless command to address the first RFID tag using the random number, the second wireless command to request a response from the first RFID tag addressed by the random number.

64. The method of claim 63, further comprising:

transmitting a third wireless command from the reader to continue identification of a population of RFID tags, the third command including at least the first bits included in the first command.

65. The method of claim 64, wherein the third command includes one more bit than the first bits to address RFID tags.

66. The method of claim 63, wherein the random number is a sixteen-bit random number.

67. The method of claim 63, wherein the first bits is a portion of the random number.

68. The method of claim 63, wherein the subsequent commands comprise coordination pulses to indicate time slots.

69. The method of claim 63, wherein the first RFID tag further transmits at least a portion of an identification code to the reader.

70. The method of claim 63, wherein each of the subsequent wireless commands continues the request of the first wireless command.

71. The method of claim 63, wherein each of the subsequent wireless commands indicates a time slot for replying in accordance with the request of the first wireless command.

72. The method of claim 63, further comprising:

transmitting, from the reader, an acknowledge command in response to the random number being identified from the reply.

73. A radio frequency communications-based method of conducting a financial transaction, comprising:

sending a first wireless radio frequency (RF) signal to start identification of one or more radio frequency devices of a population of radio frequency devices, the first RF signal requesting one or more radio frequency devices having at least two first bits specified in the first RF signal to reply;

receiving a response via a receiver coupled to a controller and one or more antennas, said receiver, said controller and said one or more antennas configured to detect a collision in response to the first RF signal and, when there is no collision in response to the first RF signal, to determine an identifier of a first radio frequency device from a reply to the first RF signal;

addressing the first radio frequency device using the identifier determined from the reply to the first RF signal so as to elicit a subsequent response from the first radio frequency device; and

initiating a financial transaction based at least in part on said acts of sending, receiving and addressing, thereby resulting in the debiting of an account associated with said first radio frequency device.

74. The method of claim 73, wherein the financial transaction is associated with the payment of a toll.

75. The method of claim 74, wherein said receiver and said one or more antennas is disposed within a toll booth, and said method further comprises operating said receiver disposed within said toll booth at least when said first radio frequency device issuing said response to said first wireless RF signal is in proximity thereto.

76. The method of claim 74, wherein the financial transaction comprises receiving a credit card number against which the toll can be charged.

77. The method of claim 73, wherein the debiting of the account comprises charging a credit card number associated with an owner of the account.

78. The method of claim 73, wherein the financial transaction is for payment for goods or services.

79. The method of claim 78, further comprising:

transmitting a subsequent wireless command requesting one or more responses to continue the identification of one or more radio frequency devices within the population of radio frequency devices, the subsequent wireless command to identify a subset of the population of radio frequency devices and request the subset to reply with identification numbers.

80. The method of claim 73, wherein the response comprises further information about the first radio frequency communications device.

81. The method of claim 73, wherein the identifier comprises a unique identification code that uniquely identifies the first radio frequency device among the population of radio frequency devices.

82. The method of claim 73, wherein the identifier comprises a random number generated by the first radio frequency device.

83. The method of claim 73, wherein the first radio frequency device is configured to select a random value that determines a time slot in which the first radio frequency device provides the response.

* * * * *