(12) STANDARD PATENT (11) Application No. **AU 2007203558 C1**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Method and apparatus to facilitate transmission of an encrypted rolling code

(51) International Patent Classification(s)
H04L 9/00 (2006.01) ***G06F 21/00*** (2006.01)

(21) Application No: **2007203558** (22) Date of Filing: **2007.07.31**

(30) Priority Data

(31) Number	(32) Date	(33) Country
11/501455	**2006.08.09**	**US**

(43) Publication Date: **2008.02.28**
(43) Publication Journal Date: **2008.02.28**
(44) Accepted Journal Date: **2014.05.08**
(44) Amended Journal Date: **2014.11.20**

(71) Applicant(s)
The Chamberlain Group, Inc.

(72) Inventor(s)
Fitzgibbon, James J;Laird, Edward T

(74) Agent / Attorney
AJ PARK, L 9 Nishi 2 Phillip Law St, Canberra, ACT, 2601

(56) Related Art
US 5774065

METHOD AND APPARATUS TO FACILITATE TRANSMISSION OF AN ENCRYPTED ROLLING CODE

Abstract of the Disclosure

An encrypted rolling code (11), a plurality of differing data bit order patterns (13), and a plurality of differing data inversion patterns 14) are provided. One then selects (15) a particular one of each of these patterns and uses those selected patterns as transmission characteristics when transmitting (16) at least part of the encrypted rolling code.

2007203558 31 Jul 2007

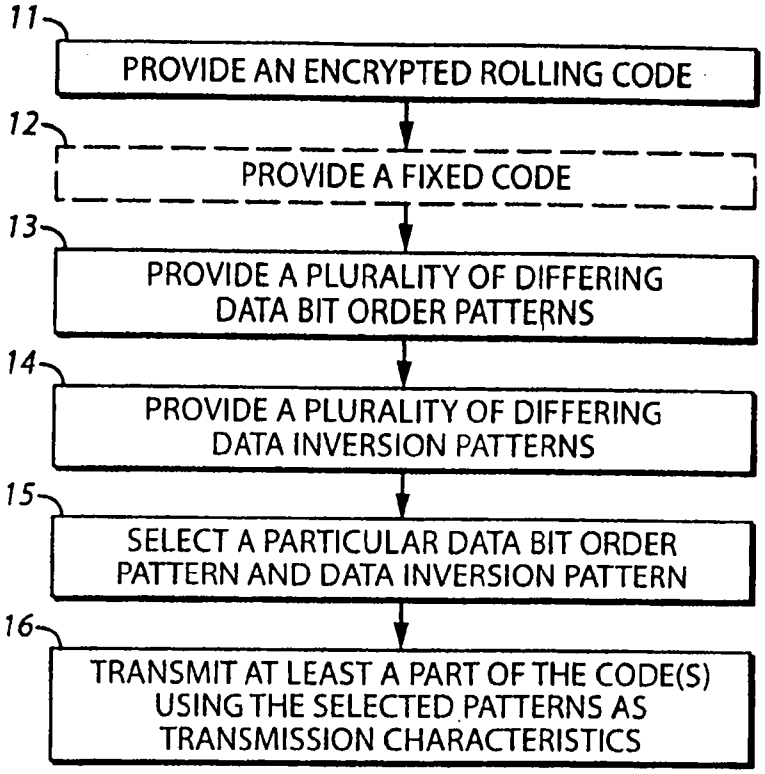

FIG. 1

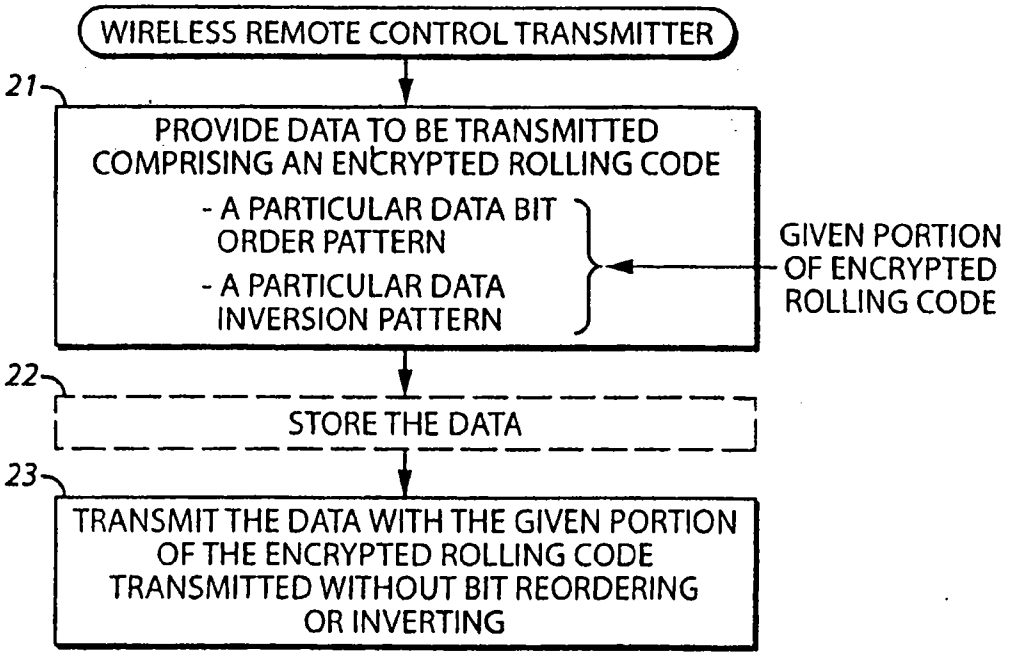

FIG. 2

2007203558 31 Jul 2007

S&F Ref: 820197

AUSTRALIA

PATENTS ACT 1990

COMPLETE SPECIFICATION

FOR A STANDARD PATENT

Name and Address of Applicant :	The Chamberlain Group, Inc., of 845 Larch Avenue, Elmhurst, Illinois, 60126, United States of America
Actual Inventor(s):	James J. Fitzgibbon Eric Gregori
Address for Service:	Spruson & Ferguson St Martins Tower Level 35 31 Market Street Sydney NSW 2000 (CCN 3710000177)
Invention Title:	Method and apparatus to facilitate transmission of an encrypted rolling code

The following statement is a full description of this invention, including the best method of performing it known to me/us:-

METHOD AND APPARATUS TO FACILITATE TRANSMISSION OF AN ENCRYPTED ROLLING CODE

Technical Field

[0001] This invention relates generally to encrypted rolling codes and more particularly to the transmission of encrypted rolling code information.

Background

[0002] Rolling codes are known in the art. Rolling codes are often used, for example, in conjunction with movable barrier operators of various kinds (with movable barrier operators of various kinds also being known in the art and including operators that effect the selective control and movement of single panel and segmented garage doors, pivoting, rolling, and swinging gates, guard arms, rolling shutters, and various other movable barriers). In such an application setting, a wireless transmitter can send a code to a corresponding movable barrier operator to cause the latter to effect a desired movement or other action with respect to, for example, a corresponding movable barrier.

[0003] When using rolling codes, the code transmitted by the wireless transmitter will change (often with each transmission) in accordance with a predetermined plan or algorithm that is also known to the movable barrier operator. Such an approach can foil the use of an intercepted code by an unauthorized party because that intercepted code will not typically again, at least in the near term, be honored by that movable barrier operator should the

unauthorized party attempt to themselves transmit that code. Without knowledge of the underlying scheme by which a next code is selected, the unauthorized party who gains access to a presently used code will still remain unable to leverage that knowledge in support of effecting unauthorized control over the movable barrier operator.

[0004] There may be instances, however, when additional security may be desired or appropriate. For example, a given rolling code instantiation may be open to brute force attacks or other weaknesses due to local and/or otherwise unique circumstances.

Brief Description of the Drawings

[0005] The above needs are at least partially met through provision of the method and apparatus to facilitate transmission of an encrypted rolling code described in the following detailed description, particularly when studied in conjunction with the drawings, wherein:

[0006] FIG. 1 comprises a flow diagram as configured in accordance with various embodiments of the invention;

[0007] FIG. 2 comprises a flow diagram as configured in accordance with various embodiments of the invention;

[0008] FIG. 3 comprises a depiction of prior art ternary encoding;

[0009] FIG. 4 comprises a flow diagram as configured in accordance with various embodiments of the invention;

[00010] FIG. 5 comprises a flow diagram as configured in accordance with various embodiments of the invention;

[00011] FIG. 6 comprises a mapping table as configured in accordance with various embodiments of the invention;

[0010] FIG. 7 comprises a schematic view of bit processing and parsing in accordance with various embodiments of the invention;

[0011] FIG. 8 comprises a comprises a schematic joint message diagram as configured in accordance with various embodiments of the invention;

[0012] FIG. 9 comprises a schematic view of bit selection and parsing as configured in accordance with various embodiments of the invention;

[0013] FIG. 10 comprises an illustrative example of a lookup table as configured in accordance with various embodiments of the invention;

[0014] FIG. 11 comprises a schematic view of two joint messages as configured in accordance with various embodiments of the invention;

[0015] FIG. 12 comprises a schematic view of bit parsing as configured in accordance with various embodiments of the invention;

[0016] FIG. 13 comprises a schematic view of a joint message as configured in accordance with various embodiments of the invention;

[0017] FIG. 14 comprises an illustrative example of a lookup table as configured in accordance with various embodiments of the invention;

[0018] FIG. 15 comprises a schematic view of bit processing and parsing as configured in accordance with various embodiments of the invention;

[0019] FIG. 16 comprises a schematic view of a joint message as configured in accordance with various embodiments of the invention;

[0020] FIG. 17 comprises an illustrative example of a lookup table as configured in accordance with various embodiments of the invention; and

[0021] FIG. 18 comprises a block diagram as configured in accordance with various embodiments of the invention.

[0022] Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been drawn to scale. For example, the dimensions and/or relative positioning of some of the elements in the figures may be exaggerated relative to other elements to help to improve understanding of various embodiments of the present invention. Also, common but well-understood elements that are useful or necessary in a commercially feasible embodiment are often not depicted in order to facilitate a less obstructed view of these various embodiments of the present invention. It

will also be understood that the terms and expressions used herein have the ordinary meaning as is accorded to such terms and expressions with respect to their corresponding respective areas of inquiry and study except where specific meanings have otherwise been set forth herein.

Detailed Description

[0023] Generally speaking, pursuant to these various embodiments, an encrypted rolling code, a plurality of differing data bit order patterns, and a plurality of differing data inversion patterns are provided. One selects a particular one of each of the bit order patterns and the data inversion patterns to provide selected patterns and then uses those selected patterns as transmission characteristics when transmitting at least part of the encrypted rolling code.

[0024] By these teachings, for example, a wireless remote control transmitter can be provided with data to be transmitted, where that data comprises, at least in part, at least portions of an encrypted rolling code and where that data comports with a particular data bit order pattern and a particular data inversion pattern as a function of a given portion of that rolling code. That data can then be transmitted in combination with the given portion of the encrypted rolling code wherein that given portion of the rolling code is not transmitted with any of its bits reordered or inverted as a function of the given portion itself. Accordingly, a receiver that receives the data can then properly recover the re-ordered/inverted portions of the encrypted rolling code as a function of the given portion of the encrypted rolling code.

[0025] By one approach, if desired, the aforementioned data can comprise ternary data that is presented in a binary format. The use of ternary data can aid in facilitating compatible interaction with at least some movable barrier operators while also achieving an encryption effect at the same time as tending to ensure compatible use with binary peripheral platforms and the like. By one approach, this can comprise mapping each trit of the ternary data to a corresponding pair of binary bits. A pair of binary bits can represent 4 discrete information elements and by one approach, three of these discrete information elements can each correspond to one of the three trit states/levels while the fourth discrete information element (which otherwise comprises an illegal value) can serve a synchronization function.

[0026] If desired, in addition to the aforementioned encrypted rolling code, a fixed code can also be included in the transmission. By one approach, for example, both the aforementioned part of the encrypted rolling code and this fixed code can be transmitted using the above-described selected patterns as transmission characteristics.

[0027] These and other benefits may become clearer upon making a thorough review and study of the following detailed description. Referring now to the drawings, and in particular to FIG. 1, an illustrative process in this regard provides 11 an encrypted rolling code. As will be illustrated in more detail below, this can comprise, if desired, providing an encrypted rolling code as a plurality of bit pairs as correspond to a ternary data set.

[0028] If desired, this process will also optionally accommodate providing 12 a fixed code. This fixed code can vary with the needs, requirements, and/or opportunities of a given application setting, but can, for example, comprise a value that is substantially unique to a given transmitter and hence comprises a value that will serve to identify that given transmitter. Such an approach can be useful, for example, when used in conjunction with a remote control movable barrier operator transmitter.

[0029] This process also provides 13 a plurality of differing data bit order patterns. By one approach, for example, this can comprise data bit order patterns that each comprise a pattern for exactly three bits. As will be shown below, this can be particularly beneficial when used in conjunction with bit pairs that correlate to corresponding ternary data. Similarly, this process provides 14 a plurality of different data inversion patterns. As before, if desired, this can comprise providing patterns that each comprise a pattern for exactly three bits. The number of patterns provided in either case can vary as desired. By one approach, however, this can comprise providing at least nine different bit order patterns and nine different data inversion patterns. Illustrative examples in this regard are provided further herein.

[0030] This process then provides for selecting 15 a particular one of each of the data bit order patterns and the data inversion patterns to provide resultant corresponding selected patterns. There are various ways by which such selections can be made. By one approach, one may use a predetermined portion of the previously provided encrypted rolling code to inform the making of these selections. For example (and as will be illustrated in more detail

herein), this can comprise using a predetermined four bit pairs of the encrypted rolling code as a basis for selecting the particular data bit order pattern and the particular data inversion pattern. As another example in this regard, in combination with the foregoing or in lieu thereof, this can comprise using a first predetermined portion of the encrypted rolling code to select a first particular data bit order pattern and a first data inversion pattern and using a second predetermined portion of the encrypted rolling code (that is, for example, discrete with respect to the first predetermined portion of the encrypted rolling code though this is not a fundamental requirement) to select a second particular data bit order pattern and a second data inversion pattern.

[0031] This process then provides for transmitting 16 at least a part of the encrypted rolling code itself (as well as at least a part of the above-described fixed code when present) using the aforementioned selected patterns as transmission characteristics. By one approach this can comprise making such a transmission using Manchester encoding as is known in the art.

[0032] So configured, these teachings are readily employed, for example, to facilitate the transmission of a remote control message. This can comprise, for example, providing a fixed message having at least a first part and a second part along with an encrypted rolling code that has a first through a fourth part. The first part of the encrypted rolling code can then be used to select a particular data bit order pattern and a data inversion pattern to use as a set of first selected patterns while the second part of the encrypted rolling code can be used to select a second set of patterns from amongst the available candidate patterns. One can then transmit the first part of the fixed message and the third part of the encrypted rolling code using the first selected patterns as transmission characteristics while transmitting the second part of the fixed message and the fourth art of the encrypted rolling code using the second selected patterns as transmission characteristics.

[0033] By one approach, in this illustrative example this can also comprise transmitting the first and second parts of the encrypted rolling code without using either the first or selected patterns as transmission characteristics. So configured, the first and second parts of the encrypted rolling code are then readily usable as recovery identifiers that can be used by a receiver to recover the first and second parts of the fixed message and the third and fourth parts of the encrypted rolling code.

[0034] To illustrate further in this regard, these first and second parts of the encrypted rolling code could each comprise four bit pairs as correspond to the aforementioned ternary data. In such a case, two of the bit pairs as comprise the first part of the encrypted rolling code can be used with a lookup table to correlate those two bit pairs to a corresponding data bit order pattern. In a similar manner the remaining bit pairs can be used with a second lookup table (which may, if desired, actually comprise a part of the first lookup table) to correlate these bit pairs with a corresponding data inversion pattern. In a similar fashion, two of the bit pairs of the four bit pairs as comprise the second part of the encrypted rolling code can be used with that first lookup table to identify another data bit order pattern while the remaining two bit pairs can be used with the second lookup table to identify a corresponding data inversion pattern.

[0035] In such a case, the aforementioned transmission can then comprise transmitting the second part of the fixed message and the fourth part of the encrypted rolling code using the second selected patterns as transmission characteristics only after not transmitting for at least a predetermined period of time following transmission of the first part of the fixed message and the third part of the encrypted rolling code using the first selected patterns as transmission characteristics. The duration of this predetermined period of time can vary with the needs and opportunities of a given application setting, but a duration of about 75 milliseconds will suffice for many expected purposes.

[0036] In addition to facilitating a transmission of an encrypted rolling code and other content that comprises, for example, information that is unique to a given transmitter (such as a unique identifier for that transmitter), these teachings will further readily accommodate the transmission of additional data that is not substantially unique to the transmitter. This can comprise, for example, providing a data payload (such as a remote control instruction such as OPEN, CLOSE, VACATION MODE, LIGHTS ON, LIGHTS OFF, and so forth) that is not substantially unique to a given transmitter and then transmitting the first part of the fixed message, the third part of the encrypted rolling code, and a first part of this data payload while using the first selected patterns as transmission characteristics and transmitting the second part of the fixed message, the fourth part of the encrypted rolling code, and a second (remaining) portion of the data payload using the second selected patterns as transmission characteristics. When the data payload comprises a relatively large quantity of data as

compared to the fixed message and/or the encrypted rolling code, additional portions of the data payload as are not accommodated by the just-described process can then be supplementally transmitted using one of the already selected patterns (or other patterns, if desired) as transmission characteristics.

[0037] As another specific illustrative example in this regard, and referring now to FIG. 2, a wireless remote control transmitter (such as a movable barrier operator remote control) can be configured and arranged to provide 21 data to be transmitted. This data can comprise, at least in part, at least portions of an encrypted rolling code. In any event, this data will comport with a particular data bit order pattern and a particular data inversion pattern as a function of a given portion of the rolling code. By one approach, if desired, this process can further comprise, at least in part, storing 22 this data in a memory prior to transmitting the data. The duration of such storage can vary considerably depending upon the specifics of a given application setting.

[0038] This wireless remote control transmitter can then transmit 23 this data in combination with the given portion of the encrypted rolling code such that the given portion of the encrypted rolling code is not transmitted with any of its bits reordered or inverted as a function of the given portion of the encrypted rolling code. So configured, a receiver that receives this data can properly recover the modified portions of the encrypted rolling code as a function, at least in part, of the unmodified given portion of the encrypted rolling code.

[0039] As noted above, these teachings are readily applied in a context that makes use of ternary data. It may therefore be helpful to first describe in more detail a typical ternary data protocol as one finds often deployed in conjunction with many movable barrier operators. Pursuant to one approach, pulses of similar amplitude have one of three different durations. For example, and referring now to FIG. 3, a first pulse 31, having a shortest duration, can represent the data element "0." A second pulse 32, having a medium length duration, can represent the data element or state "1." And a third pulse 33, having a longest duration, can represent the data element or state "2." Such a data mapping protocol serves well to effect a base three-based data exchange. The present teachings can accommodate use and leveraging of a ternary approach to effect relatively secure and compatible communications between a movable barrier operators and corresponding peripheral components of choice. These

teachings are also compatible for use with an approach that eschews the specific ternary approach just described.

[0040] Referring now to FIG. 4, in general, these teachings will accommodate a process 40 that itself provides 41 ternary data as corresponds to a movable barrier operator and then converts 42 that ternary data to a binary format to provide resultant binary information. This binary information is then transmitted 43 from one platform to another. As will be shown below, this ternary-to-binary conversion process serves, at least in part, as a kind of encryption process which in turn aids in ensuring the authenticity and accuracy of the information being transmitted.

[0041] The ternary data itself can comprise, at least in part, bearer data. More particularly, and referring momentarily to FIG. 5, pursuant to one (optional) approach, provision of ternary data can comprise prior provision 51 of binary bits comprising information that corresponds to the movable barrier operator (for example, information sourced by, or intended for, a movable barrier operator). Such information can optionally comprise, for example, movable barrier operator fixed information 52 such as identifying information for a particular movable barrier operator, a particular peripheral component, or the like. Such information can also optionally comprise (in addition to or in lieu of fixed information 52) non-fixed information 53 such as the aforementioned data payload as again corresponds to the movable barrier operator. This non-fixed information 53 can comprise bearer data/information (such as, but not limited to, platform status information, commands, acknowledgments, and so forth). As already noted, this non-fixed information 53 can also comprise varying quantities of data if desired.

[0042] These binary bits are then converted 54 into the aforementioned ternary data. This could comprise, in an appropriate platform, a conversion of the binary data into ternary data such as that described above with respect to FIG. 3. In general, such an approach need not be used. Instead, the binary data can be converted into a binary-bit-based ternary format (with an illustrative example being provided further below).

[0043] By one approach, however, this does not comprise a simple reversal of the binary-to-ternary process just described. Instead, the ternary-to-binary conversion step can comprise mapping each trit of the ternary data to a corresponding pair of binary bits. To illustrate such

a map 61, and referring momentarily to FIG. 6, the ternary data element "0" (which corresponds to the usual binary data element "0") maps to the binary pair "00." In similar fashion, ternary "1" (which corresponds to usual binary "1") maps to the binary pair "01" and ternary "2" (which corresponds to usual binary "11") maps to the binary pair "01."

[0044] This leaves an otherwise unused binary pair "11." Pursuant to a preferred approach, this otherwise illegal value can serve a synchronization function when facilitating communications as between a movable barrier operator and one or more peripheral components when using a binary format that otherwise has no synchronization mechanism built into its format (for example, a stream of binary bits such as:

01101111111010011101110110111111101001110111011011111111010011101111

which format lacks a frame marker or other point of synchronization). To illustrate, a synchronization signal/marker comprising this "11" binary pair can be used to indicate, for example, the regular end and/or start of a frame or message as in the following example:

1101101111111*01*1101110111101101111111*01*1111011111111011011111111*01*1*11*

where the bold font "11" regularly spaced binary pairs serve as frame markers (and which, due to their synchronized regular spacing, are readily distinguishable from other "11" pairs as may occur for whatever reason (illustratively depicted in the above example with italic font).

[0045] Those skilled in the art will appreciate that this process of converting binary information into ternary information, followed by conversion of that ternary information into corresponding binary pairs, yields, in most cases, a different bit sequence (and even a different number of bits) as compared to the initial binary information. This difference serves, at least in part, as a non-key-based encryption technique and hence provides a way of effecting the provision of an encrypted rolling code.

[0046] Referring now to FIG. 7, a more detailed illustrative embodiment will be presented. In this first illustrative example, the only substantive content to be associated and transmitted with a 28 bit rolling code 71 comprises a 40 bit value that represents fixed information 72. This fixed information 72 may serve, for example, to uniquely identify the transmitter that will ultimately transmit this information as noted above.

[0047] In this particular illustrative embodiment, the bits comprising the rolling code 71 are encrypted 73 by mirroring the bits and then translating those mirrored bits into ternary

values as suggested above to provide corresponding bit pairs (in this example, this would comprise 18 such bit pairs) to thereby provide a resultant encrypted rolling code 74. This mirroring can be applied to specific groupings of bits in the rolling code creating mirrored groups or can involve the entire value. In this illustrative example, the encrypted rolling code 74 is presented for further processing as four groups. In this example, these four groups comprise a roll group E 74A comprised of four binary bit pairs, a roll group F 74B comprised of five binary bit pairs, a roll group G 74C comprised of four binary bit pairs, and a roll group H 74D comprised of five binary bit pairs.

[0048] The 40 bit fixed information 72 is subdivided in a similar manner albeit sans encryption. This comprises, in this particular illustrative approach, forming four subgroups comprising a fixed group A 75A, a fixed group B 75B, a fixed group C 75C, and a fixed group D 75D, wherein each such group is comprised of 10 bits of the original 40 bit value.

[0049] These variously partitioned data groups can then be used as shown in FIG. 8 to effect a desired transmission. In this example, one or more joint messages 80 provide a primary vehicle by which to communicate the desired information (which includes both the encrypted rolling code and fixed information data as modified as a function of a given portion of the encrypted rolling code along with a recovery identifier that represents that given portion of the encrypted rolling code). This joint message 80 comprises, generally speaking, a first 20 bit portion 81 and a second 30 bit portion 82.

[0050] The first portion 81 comprises, in this embodiment, the following fields:

"0000" – these bits 81A serve to precharge the decoding process and effectively establish an operational threshold;

"1111" – these bits 81B comprise two bit pairs that present the illegal state "11" ("illegal" because this corresponds to a fourth unassigned state in the ternary context of these communications) and serve here as a basis for facilitating synchronization with a receiving platform;

"00" – this bit pair 81C identifies a type of payload being borne by the joint message (in this embodiment, "00" corresponds to no payload other than the fixed identifying information for the transmitter itself, "01" corresponds to a

supplemental data payload, and "10" corresponds to a supplemental data-only payload – further explanation regarding these payload types appears further below);

"Xx" – this bit pair 81D presents a frame identifier that can be used by a receiver to determine whether all required joint messages 80 have been received and which can also be used to facilitate proper reconstruction of the transmitted data;

"B3, B2, B1, B0" – these two bit pairs 81E comprise an inversion pattern recovery identifier and are selected from the bits that comprise the encrypted rolling code 74 described above;

"B7, B6, B5, B4" – these two bit pairs 81F comprise a bit order pattern recovery identifier and are also selected from the bits that comprise the encrypted rolling code 74 described above.

[0051] There are various ways by which these recover identifier values can be selected. Referring momentarily to FIG. 9, by one approach, eight bits from the encrypted roll group 74 are selected to form a corresponding roll sub-group 91. These might comprise, for example, the first or the last eight bits of the encrypted roll group 74 (in a forward or reversed order). These might also comprise, for example, any eight consecutive bits beginning with any pre-selected bit position (such as, to illustrate, the seventh bit, the 21st bit, and so forth). Other possibilities also exist. For example, only even position bits or odd position bits could serve in this regard. It would also be possible, for example, to use preselected bits as comprise one or more of the previously described roll group sub-groups such as roll group E 74A or roll group G 74C.

[0052] It would also be possible to vary the selection mechanism from, for example, joint message to joint message. By one simple approach in this regard, for example, the first eight bits of the encrypted roll group 74 could be used to form the roll sub-group 91 with the last eight bits of the encrypted roll group 74 being used in a similar fashion in an alternating manner.

[0053] The eight bits that comprise this roll sub-group 91 are then further parsed to form the two recovery indicators 81E and 81F mentioned above. Again, there are numerous ways by which one may use the bits that comprise the roll sub-group 91 to form these recovery indicators 81E and 81F. By one simple approach, for example, the bits as comprise the roll sub-group 91 can be used in their existing (or reversed) order to form roll group 1 81E and roll group 2 81F. Using this approach, for example, bit B3 of roll group 1 81E would comprise bit seven from the roll sub-group 91 with bit B2 then corresponding to bit six and so forth.

[0054] By another approach, if desired, every other bit can be applied in this manner. So configured, for example, bit B3 could comprise bit six from the roll sub-group 91, bit B2 could comprise bit four from the roll sub-group 91, and so forth. In such a case, bit B7 would then comprise bit seven from the roll sub-group 91, bit B6 would comprise bit five from the roll sub-group 91, and so forth.

[0055] Referring again to FIG. 8, in this embodiment, the "B7, B6, B5, B4" values from the corresponding recovery indicator are used in conjunction with one or more lookup tables to determine a data bit order pattern to use with respect to formatting the data as comprises the second portion 82 of the joint message 80. Similarly, the "B3, B2, B1, B0" values are used in conjunction with a lookup table to determine a data bit order pattern to also use with that second portion 82 of the joint message 80.

[0056] Before providing further elaboration regarding an illustrative example of such lookup tables and their use, it will be helpful to first note that, in this example, the data in the second portion 82 of the joint message comprises 10 bits from roll group F (or H) and 10 bits each from fixed group A (or C) and fixed group B (or D) for a total of 30 bits. These bits are organized into triplets (shown in FIG. 8 in the form "(F, B, A)" and "(H, D, C)" to indicate that each such triplet includes one bit from a roll group F or H and one bit each from the two fixed groups B and A or D and C.

[0057] Those skilled in the art will note that, in this illustrative example, bits from roll group E 74A and roll group G 74C are not present in the second portion 82 of the joint message 80. This is because, in this example, it is presumed that the contents of these two roll groups are used to form the recovery indicators that appear in the first portion 81 of the joint

message 80. Other accommodations can of course be made in this regard. In general, however, these teachings will accommodate not including those encrypted rolling code bits that are used as recovery indicators in the second portion 82 of the joint message 80.

[0058] In the example shown, the order of the bits in each triplet is "F, B, A" (or "H, D, C" as appropriate). This order is neither arbitrary nor static. Instead, for this particular joint message 80, this order of the bits in each triplet is dictated by the values B7, B6, B5, B4 noted above. In this case, and referring now to FIG. 10, a lookup table 101 serves to correlate various values for these two bit pairs with corresponding data bit order patterns. In this example, presuming that the values of these four bits happens to be "0000," the corresponding order of bits for each triplet is established as "F/H, B/D, A/C" and hence the ordering of the bits depicted in FIG. 8.

[0059] Those skilled in the art will note that this lookup table 101 provides no patterns that would correlate to two bit pairs having the value "11." This is because, in this embodiment, "11" as a bit pair value comprises an illegal value and hence is not expected to occur. Accordingly there are no bit order patterns presented to correlate with such values as "11XX," "XX11," or "1111." This creates 9 possible selections for the order of bits and the inversion value. The number of possible unique order of three bits leads to only six different bit order patterns. This degree of diversity should suffice for most if not all purposes.

[0060] The aforementioned B3, B2, B1, B0 values 81F are employed in a similar fashion with this lookup table 101 to identify a particular inversion pattern to be employed with the data triplets of the second portion 82 of the joint message 80. For example, when these bits are "0000," this lookup table provides for no inversion of any of the bits in each triplet. On the other hand, when these bits are "1010," each bit of each triplet is to be inverted. In this case, up to eight different inversion patterns are possible.

[0061] To illustrate further, when a given data triplet happens to have the values "110" and the inversion indicator has the values "0100," the lookup table will return a data inversion pattern of "normal invert invert." As a result, this particular data triplet will instead have the values "101" because the second and third values in each triplet are now to be inverted in value.

[0062] So configured, a first portion of a joint message is seen to include a recovery indicator that itself comprises a selected portion of an encrypted rolling code. A second portion of that joint message, in turn, contains data triplets having bits that are arranged in a particular order and that observe a particular inversion pattern as a function of that joint indicator. Accordingly, it will not be sufficient for an unauthorized party to simply glean, in some fashion, the basis of the rolling code itself. Instead, now, this unauthorized party must also now understand how a particular portion of that rolling code is used to modify the transmission of other portions of that rolling code in addition to fixed information as may also accompany the rolling code.

[0063] In many application settings it may be desirable to present more than one such joint message to present a complete transmission. For example, and referring now to FIG. 11, it may be desirable to use two (or more) such joint messages 80A and 80B in order to present the complete rolling code and the complete fixed content and was described above. In such a case, for example, the first joint message 80A can present and use a first roll sub-group 91 as defined above as a recovery identifier (which comprises, in this illustrative example, roll group E 74A) while the second joint message 80B presents and uses a second, different roll sub-group B 91 (which comprises, in this illustrative example, roll group G 74C) for this purpose. These recovery identifiers can be used as just described to control modification of their corresponding data. So configured, in this illustrative example, 10 bits of roll group F 74B, 10 bits of fixed group A 75A, and 10 bits of fixed group B 75B have their bits ordered and inverted as a function of the bits of roll group E 74A while 10 bits of roll group H 74D, 10 bits of fixed group C 75C, and 10 bits of fixed group D 75D are similarly ordered/inverted as a function of the bits of roll group G 74C.

[0064] If desired, these joint messages 80A and 80B can be sent in a concatenated manner. By another approach, however, these joint messages can be separated by at least a minimal amount of silence (achieved, for example, by not transmitting during this period of time). For example, 75 milliseconds or so of blank time can be used for this purpose. So configured, a receiver that receives a second joint message prior to this period of blank time expiring can conclude that one or both of the received messages is somehow in error and should be avoided.

[0065] As noted above, in some cases it may be useful to transmit an additional amount of data or information than that specifically provided above. For example, it may be useful to transmit additional data that represents a particular instruction, status information, or the like. Such additional information can be readily accommodated by the teachings set forth above. To illustrate, and referring now to FIG. 12, 32 bits of such additional data can be subdivided into four corresponding data groups I and J 122A and 122B and K and L 122C and 122D where each such data group has eight bits.

[0066] Referring now to FIG. 13, the second portion 82 of each joint message 80 can now comprise 54 bits. By one approach, this can comprise 8 bits for a repeated presentation of the same rolling code group E or G as comprises the recovery identifier, 10 bits each for rolling code group F or H, fixed group A or C, and fixed group B or D, as well as 8 bits each for data group I or K and data group J or L as are described above. These various bits are again combined into data triplets using a group selection pattern such as that illustrated in FIG. 13. And, once again, the recovery identifier comprised of the roll group presented in the first portion 81 of the joint message 80 is used to select from a lookup table(s) the particular bit order and inversion patterns to employ with respect to these data triplets. In this case, and referring now to FIG. 14, the lookup table 141 can include specific bit order patterns that apply in different ways depending upon whether the data triplet includes the supplemental data.

[0067] In some cases, it may be necessary or appropriate to transmit even a larger quantity of data than can be accommodated by the processes and techniques described above. In such a case, if desired, additional supplemental joint messages can be used to present such supplemental data. With reference to FIG. 15, 32 bit value data elements 151 can be parsed using an application defined algorithm 152 of choice as corresponds to the data itself (or as may be otherwise provided or selected) into four ternary bit pairs 153 and three data groups of N bits each 154A – 154C.

[0068] Referring now to FIG. 16, the recovery indicator can be reused from a previous related joint message and the second portion 82 of the joint message 80 can contain 3 to the Nth power bits as necessary to accommodate the full data payload. The three data groups A – C are then used to form corresponding data triplets. And, as before, the recovery identifier is used to extract from a corresponding lookup table (such as the lookup table 171 presented in

FIG. 17) the particular bit order pattern and bit inversion pattern to employ with respect to the transmission of these data triplets.

[0069] Those skilled in the art will appreciate that the above-described processes are readily enabled using any of a wide variety of available and/or readily configured platforms, including partially or wholly programmable platforms as are known in the art or dedicated purpose platforms as may be desired for some applications. Referring now to FIG. 18, an illustrative approach to such a platform will now be provided.

[0070] In this illustrative embodiment, the apparatus 180 (which may comprise, for example, a wireless remote control transmitter) comprises a processor 181 that couples to a transmitter 182 (such as a wireless transmitter) of choice. Both of these components then also operably couple to a first memory 183, a second memory 184, a first lookup table 185, and a second lookup table 186. The first memory 183 can have a fixed value stored therein. This fixed value can comprise, for example, information that substantially uniquely identifies this particular apparatus 180. This first memory 183 may also, if desired, have a plurality of different fixed values contained therein. This would permit storing, for example, remote control signals that are not specific (i.e., unique) to the apparatus 180 itself.

[0071] The second memory 184 can have the aforementioned encrypted rolling code stored therein. By one approach, the processor 181 is configured and arranged to calculate the encrypted rolling code when needed and to temporarily buffer that value in the second memory 184 pending actual use of that information. By another approach, the encrypted rolling code information can be pre-provisioned using a derivation and storage approach of choice.

[0072] The lookup tables 185 and 186 are the lookup tables described above. For example, the first lookup table 185 can comprise the lookup table that correlates a first plurality of different encrypted rolling code values with corresponding differing data bit order patterns. Similarly, the second lookup table 186 can comprise the lookup table that correlates a second plurality of different encrypted rolling code values with corresponding different data inversion patterns.

[0073] The processor 181 itself is configured and arranged (via, for example, appropriate programming) to carry out selected teachings as have been presented above. So configured,

for example, the processor 181 can be configured and arranged to use the encrypted rolling code to select ones of the particular data bit order patterns and data inversion patterns for the transmitter 182 to use as transmission characteristics when transmitting the fixed value and at least portions of the encrypted rolling code. In particular, if desired, the processor can use a first part of the encrypted rolling code to select a data bit order pattern and a data inversion pattern to use when transmitting a first part of the encrypted rolling code and the fixed value and a second, different part of the encrypted rolling code to select a data bit order pattern and a data inversion pattern to use when transmitting a second, different part of the encrypted rolling code and the fixed value.

[0074] Those skilled in the art will recognize and understand that such an apparatus 180 may be comprised of a plurality of physically distinct elements as is suggested by the illustration shown in FIG. 18. It is also possible, however, to view this illustration as comprising a logical view, in which case one or more of these elements can be enabled and realized via a shared platform and/or a more-widely-distributed platform. It will also be understood that such a shared platform may comprise a wholly or at least partially programmable platform as are known in the art.

[0075] So configured, those skilled in the art will recognize and appreciate that these teachings offer great flexibility and opportunity with respect to further protecting information during a wireless transmission of that information. These teachings have particular relevance to transmissions of rolling codes and offer particular advantages when also used in conjunction with the transmission of fixed information in addition to rolling code information. The particular transmission characteristics presented are largely compatible for use with a wide variety of wireless modulation techniques. Those skilled in the art will also appreciate that these teachings are highly compatible for use with binary-based representations of ternary data formats.

[0076] Those skilled in the art will recognize that a wide variety of modifications, alterations, and combinations can be made with respect to the above described embodiments without departing from the spirit and scope of the invention, and that such modifications, alterations, and combinations are to be viewed as being within the ambit of the inventive concept.

The claims defining the invention are as follows:

1. A method comprising:

providing an encrypted rolling code;

providing a plurality of differing data bit order patterns;

providing a plurality of differing data inversion patterns;

selecting a particular one of each of the data bit order patterns and the data inversion patterns to provide selected patterns;

transmitting at least a part of the encrypted rolling code using the selected patterns as transmission characteristics,

wherein selecting a particular one of each of the data bit order patterns and the data inversion patterns to provide selected patterns comprises using the rolling code to select the particular data bit order pattern and data inversion pattern to provide the selected patterns.

2. The method of claim 1 wherein the encrypted rolling code comprises a plurality of bit pairs.

3. The method of claim 1 wherein the differing data bit order patterns each comprise a pattern for exactly three bits.

4. The method of claim 1 wherein the differing data inversion patterns each comprise a pattern for exactly three bits.

5. The method of claim 1 wherein:

providing a plurality of differing data bit order patterns comprises providing at least six different bit order patterns; and

providing a plurality of differing data inversion patterns comprises providing at least eight different data inversion patterns.

6. The method of claim 1 wherein using the encrypted rolling code to select the particular data bit order pattern and data inversion pattern to provide the selected patterns comprises using a predetermined portion of the encrypted rolling code to

select the particular data bit order pattern and data inversion pattern to provide the selected patterns.

7. The method of claim 6 wherein using a predetermined portion of the encrypted rolling code to select the particular data bit order pattern and data inversion pattern to provide the selected patterns comprises using a predetermined four bit pairs of the encrypted rolling code to select the particular data bit order pattern and data inversion pattern to provide the selected patterns.

8. The method of claim 6 wherein using a predetermined portion of the encrypted rolling code to select the particular data bit order pattern and data inversion pattern to provide the selected patterns further comprises:

using a first predetermined portion of the encrypted rolling code to select a first particular data bit order pattern and a first data inversion pattern to provide first selected patterns; and

using a second predetermined portion of the encrypted rolling code to select a second particular data bit order pattern and a second data inversion pattern to provide second selected patterns;

wherein the first and second predetermined portions of the encrypted rolling code are discrete from one another.

9. The method of claim 1 further comprising:

providing a fixed code;

and wherein transmitting at least a part of the encrypted rolling code using the selected patterns as transmission characteristics further comprises transmitting at least a part of the encrypted rolling code and the fixed code using the selected patterns as transmission characteristics.

10. A method to facilitate transmitting a remote control message comprising:

providing a fixed message having at least a first and second part;

providing an encrypted rolling code having at least a first, second, third, and fourth part;

providing a plurality of differing data bit order patterns;

providing a plurality of differing data inversion patterns;

using the first part of the encrypted rolling code to select a particular one of each of the data bit order patterns and the data inversion patterns to provide first selected patterns;

using the second part of the encrypted rolling code to select a particular one of each of the data bit order patterns and the data inversion patterns to provide second selected patterns;

transmitting:

the first part of the fixed message and the third part of the encrypted rolling code using the first selected patterns as transmission characteristics;

the second part of the fixed message and the fourth part of the encrypted rolling code using the second selected patterns as transmission characteristics.

11. The method of claim 10 wherein transmitting further comprises:

transmitting the first and second parts of the encrypted rolling code without using either the first or second selected patterns as transmission characteristics to thereby provide recovery identifiers to be used when recovering at a receiver the first and second parts of the fixed message and the third and fourth parts of the encrypted rolling code.

12. The method of claim 11 wherein the first and second parts of the encrypted rolling code each comprise four bit pairs.

13. The method of claim 12 wherein

using the first part of the encrypted rolling code to select a particular one of each of the data bit order patterns and the data inversion patterns to provide first selected patterns comprises using two bit pairs of the four bit pairs as comprise the first part of the encrypted rolling code and a first lookup table to correlate the two bit pairs to a corresponding data bit order pattern and using a different two bit pairs of the four bit pairs as comprise the first part of the

encrypted rolling code and a second lookup table to correlate the different two bit pairs to a corresponding data inversion pattern;

using the second part of the encrypted rolling code to select a particular one of each of the data bit order patterns and the data inversion patterns to provide second selected patterns comprises using two bit pairs of the four bit pairs as comprise the second part of the encrypted rolling code and the first lookup table to correlate the two bit pairs to a corresponding data bit order pattern and using a different two bit pairs of the four bit pairs as comprise the second part of the encrypted rolling code and the second lookup table to correlate the different two bit pairs to a corresponding data inversion pattern.

14. The method of claim 13 wherein transmitting comprises transmitting using Manchester encoding.

15. The method of claim 14 wherein transmitting further comprises:

transmitting the second part of the fixed message and the fourth part of the encrypted rolling code using the second selected patterns as transmission characteristics only after not transmitting for at least a predetermined period of time following transmission of the first part of the fixed message and the third part of the encrypted rolling code using the first selected patterns as transmission characteristics.

16. The method of claim 15 wherein the predetermined period of time comprises about 75 milliseconds.

17. The method of claim 10 wherein the fixed message comprises a value that is substantially unique to a given transmitter and therefore serves to identify the given transmitter.

18. The method of claim 17 further comprising:

providing a data payload that is not substantially unique to the given transmitter; and wherein transmitting:

the first part of the fixed message and the third part of the encrypted rolling code using the first selected patterns as transmission characteristics;

the second part of the fixed message and the fourth part of the encrypted rolling code using the second selected patterns as transmission characteristics;

further comprises:

transmitting:

the first part of the fixed message, the third part of the encrypted rolling code, and a first part of the data payload using the first selected patterns as transmission characteristics;

the second part of the fixed message, the fourth part of the encrypted rolling code, and a second part of the data payload using the second selected patterns as transmission characteristics.

19. The method of claim 18 wherein the data payload comprises a movable barrier operator remote control signal.

20. The method of claim 19 wherein transmitting further comprises transmitting a remaining part of the data payload using one of the selected patterns as transmission characteristics.

21. An apparatus comprising:

a first memory having a fixed value stored therein;

a second memory having an encrypted rolling code stored therein;

a first lookup table that correlates a first plurality of different encrypted rolling code values with corresponding differing data bit order patterns;

a second lookup table that correlates a second plurality of different encrypted rolling code values with corresponding differing data inversion patterns;

a processor that is operably coupled to the first and second memory and the first and second lookup table and that is configured and arranged to use the encrypted rolling code to select ones of the particular data bit order patterns and data inversion patterns to provide selected patterns;

a transmitter operably coupled to the first and second memory and to the processor and being configured and arranged to transmit at least a part of the encrypted rolling code and the fixed value using the selected patterns as transmission characteristics.

22. The apparatus of claim 21 wherein the apparatus comprises a movable barrier operator wireless remote control.

23. The apparatus of claim 21 wherein the processor is further configured and arranged to use:

a first part of the encrypted rolling code to select a data bit order pattern and a data inversion pattern to use when transmitting a first part of the encrypted rolling code and the fixed value; and

a second, different part of the encrypted rolling code to select a data bit order pattern and a data inversion pattern to use when transmitting a second, different part of the encrypted rolling code and the fixed value.

24. The apparatus of claim 21 wherein the fixed value comprises at least one of:

a substantially unique identifier for the apparatus;

a remote control signal that is not specific to the apparatus.

25. The apparatus of claim 25 wherein the fixed value comprises both of the substantially unique identifier for the apparatus and the remote control signal that is not specific to the apparatus.

26. A method comprising:

at a wireless remote control transmitter:

providing data to be transmitted, wherein the data comprises, at least in part, at least portions of an encrypted rolling code wherein the data follows with a particular data bit order pattern and a particular data inversion pattern as a function of a given portion of the rolling code;

transmitting the data in combination with the given portion of the encrypted rolling code wherein the given portion of the encrypted rolling code is not transmitted with any of its bits reordered or inverted as a function of the given

portion of the encrypted rolling code such that a receiver that receives the data can properly recover the at least portions of the encrypted rolling code as a function of the given portion of the encrypted rolling code.

27. The method of claim 26 further comprising:

storing the data in a memory prior to transmitting the data.

28. The method of claim 26 wherein providing data to be transmitted comprises providing data to be transmitted wherein the data comprises, at least in part:

a first data portion comprising a first portion of the encrypted rolling code wherein the first data portion comports with a first data bit order pattern and a first data inversion pattern as a function of a first given portion of the encrypted rolling code;

a second data portion comprising a second, different portion of the encrypted rolling code wherein the second data portion comports with a second data bit order pattern and a second data inversion pattern as a function of a second given portion of the encrypted rolling code.

29. The method of claim 28 wherein transmitting the data comprises:

transmitting the first data portion in combination with the first given portion of the encrypted rolling code wherein the first given portion of the encrypted rolling code is not transmitted with any of its bits reordered or inverted as a function of the first given portion of the encrypted rolling code such that a receiver that receives the first data portion can properly recover the first portion of the encrypted rolling code as a function of the first given portion of the encrypted rolling code;

transmitting the second data portion in combination with the second given portion of the encrypted rolling code wherein the second given portion of the encrypted rolling code is not transmitted with any of its bits reordered or inverted as a function of the second given portion of the encrypted rolling code such that a receiver that receives the second data portion can properly recover the second portion of the encrypted rolling code as a function of the second given portion of the encrypted rolling code.

30. The method of claim 29 wherein transmitting further comprises not transmitting for a predetermined period of time in between transmitting the first data portion and the second data portion.

31. The method of claim 30 wherein the predetermined period of time comprises about 75 milliseconds.

32. A method substantially as herein described with reference to an embodiment as shown in Figs. 1, 2 and 4 to 18 of the accompanying drawings.

33. An apparatus substantially as herein described with reference to an embodiment as shown in Figs. 1, 2 and 4 to 18 of the accompanying drawings.

34. A method to facilitate transmitting a remote control message, said method substantially as herein described with reference to an embodiment as shown in Figs. 1, 2 and 4 to 18 of the accompanying drawings.

2007203558 31 Jul 2007

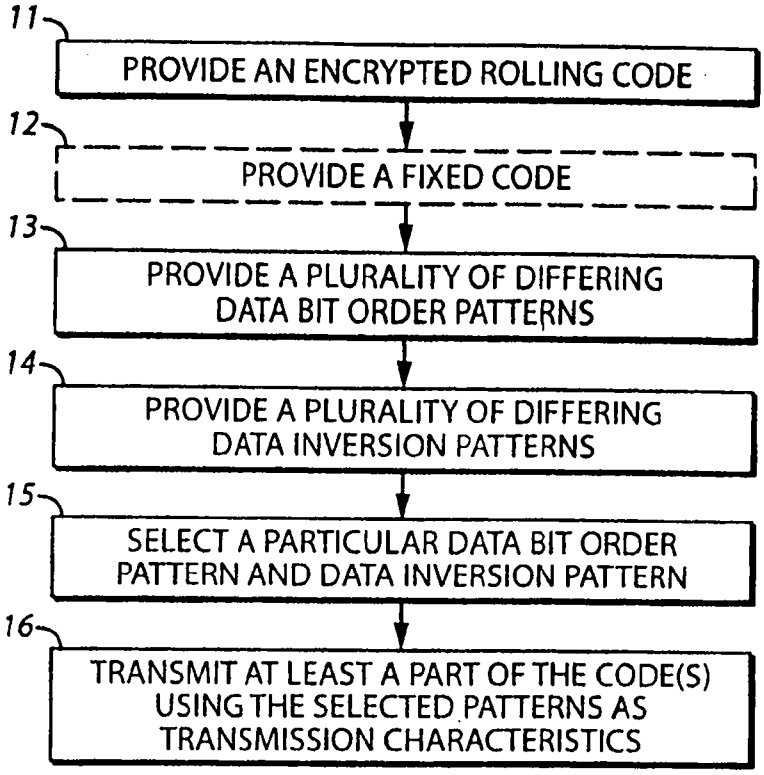

FIG. 1

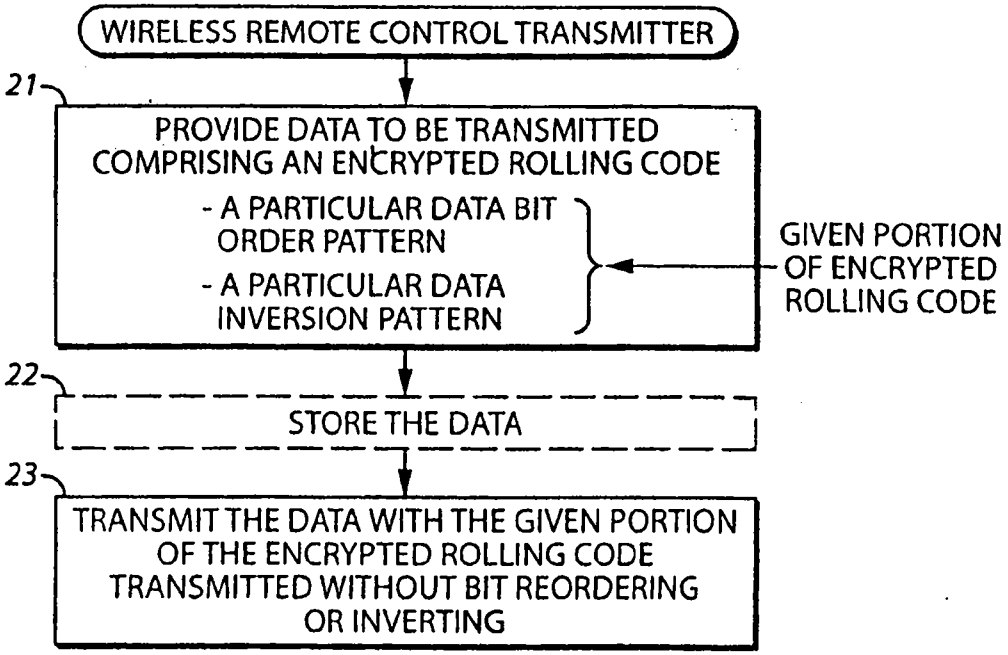

FIG. 2

2007203558 31 Jul 2007

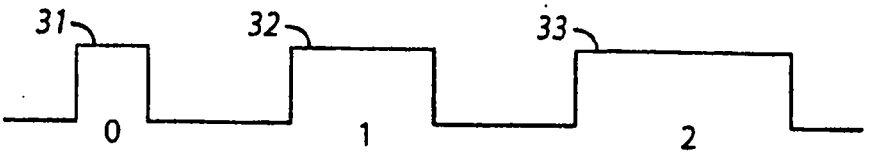

FIG. 3
(Prior Art)

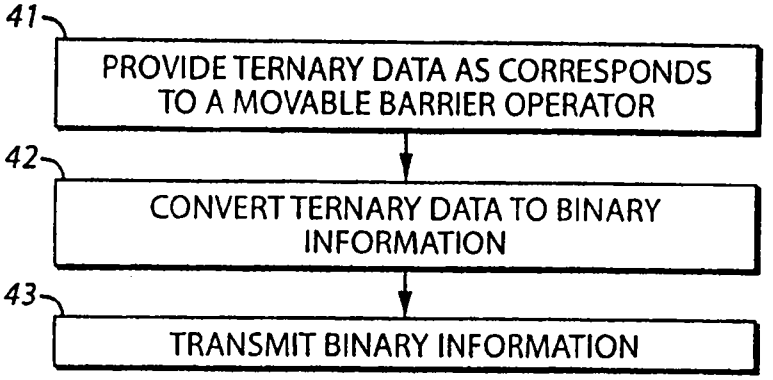

FIG. 4

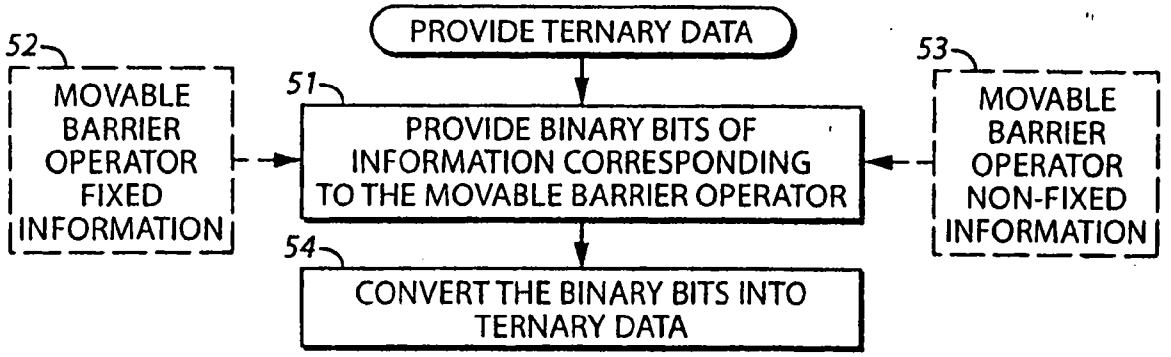

FIG. 5

61

TERNARY DATA	BINARY BIT PAIRS
0	00
1	01
2	10
ILLEGAL	11

FIG. 6

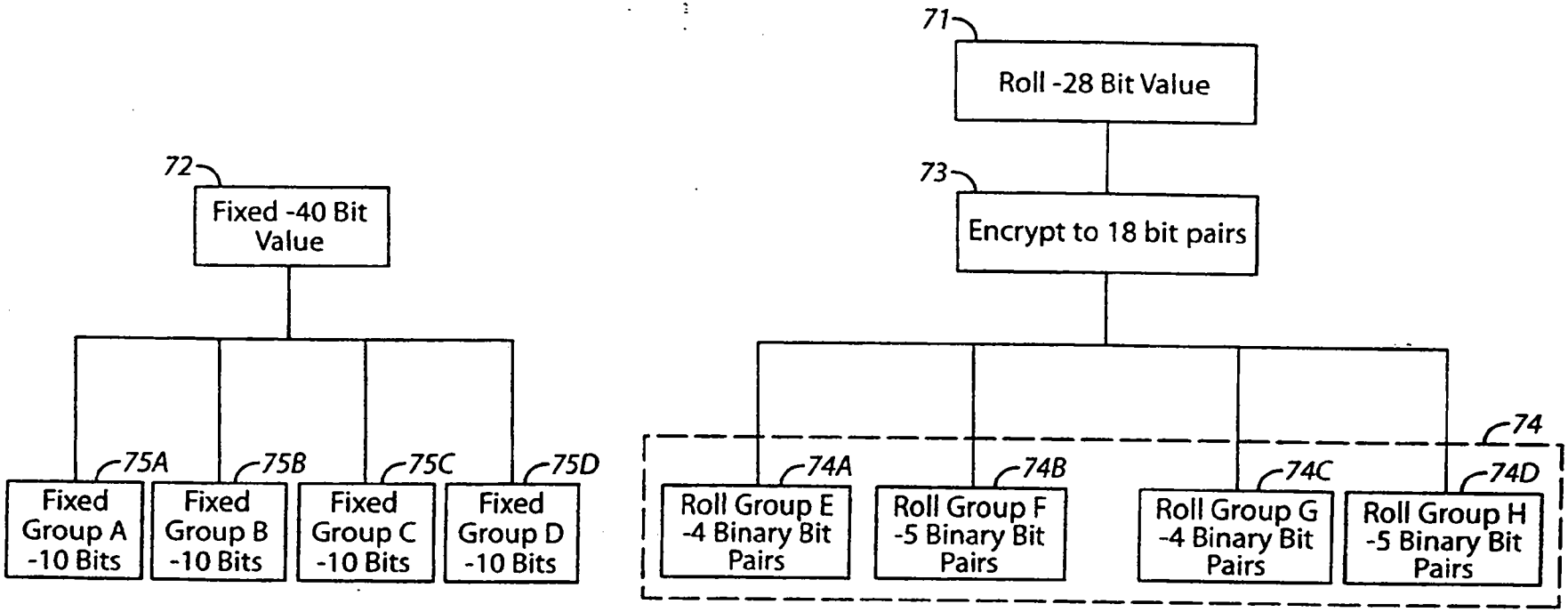
71
Roll -28 Bit Value
72
Fixed -40 Bit Value
73
Encrypt to 18 bit pairs
75A
75B
75C
75D
Fixed Group A -10 Bits
Fixed Group B -10 Bits
Fixed Group C -10 Bits
Fixed Group D -10 Bits
74
74A
74B
74C
74D
Roll Group E -4 Binary Bit Pairs
Roll Group F -5 Binary Bit Pairs
Roll Group G -4 Binary Bit Pairs
Roll Group H -5 Binary Bit Pairs

FIG. 7

2007203558 31 Jul 2007

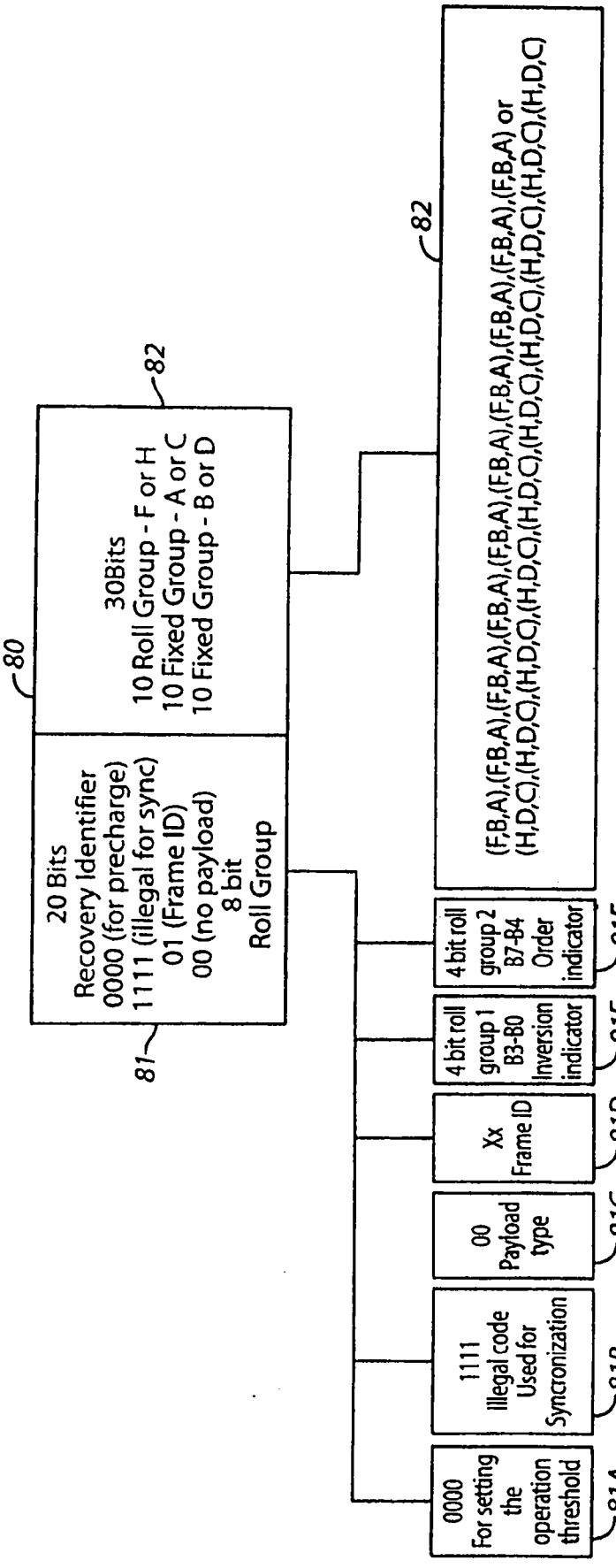

FIG. 8

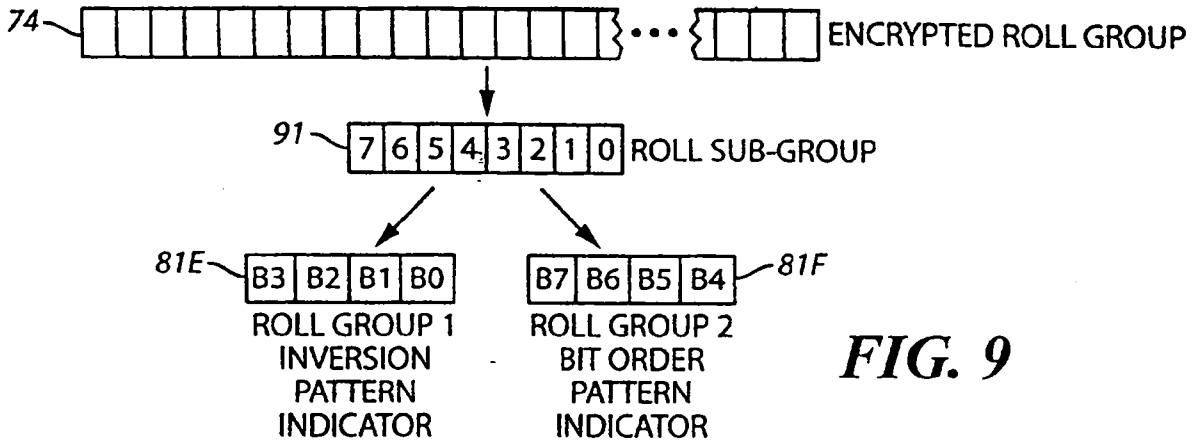

FIG. 9

101

B7	B6	B5	B4	Order of bits	B3	B2	B1	B0	Inversion Pattern
0	0	0	0	F/H,B/D,A/C	0	0	0	0	Normal Normal Normal
0	0	0	1	F/H,A/C,B/D	0	0	0	1	Normal Normal Invert
0	0	1	0	A/C,B/D,F/H	0	0	1	0	Normal Invert Normal
0	1	0	0	A/C,F/H,B/D	0	1	0	0	Normal Invert Invert
0	1	0	1	B/D,F/H,A/C	0	1	0	1	Invert Normal Normal
0	1	1	0	B/D,A/C,F/H	0	1	1	0	Invert Normal Invert
1	0	0	0	F/H,A/C,B/D	1	0	0	0	Invert Invert Normal
1	0	0	1	A/C,F/H,B/D	1	0	0	1	Invert Invert Invert
1	0	1	0	B/D,A/C,F/H	1	0	1	0	Invert Invert Invert

FIG. 10

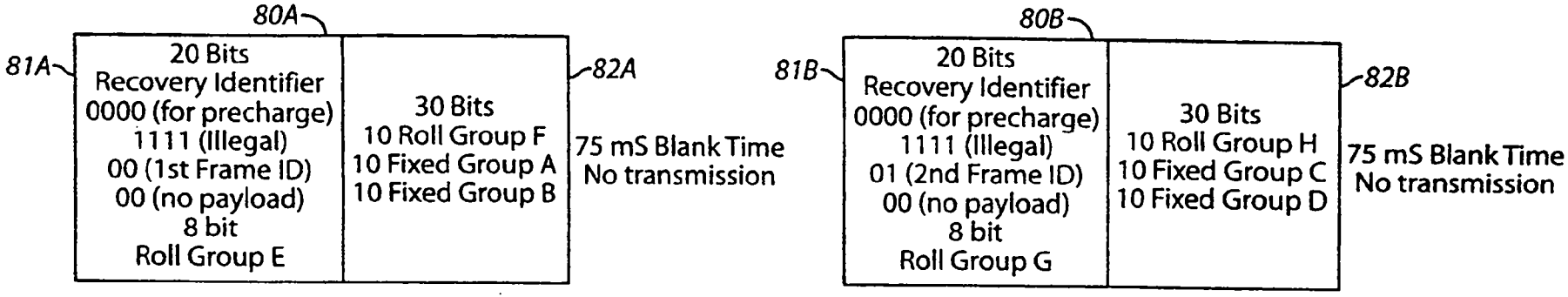
80A
81A
20 Bits
Recovery Identifier
0000 (for precharge)
1111 (Illegal)
00 (1st Frame ID)
00 (no payload)
8 bit
Roll Group E
30 Bits
10 Roll Group F
10 Fixed Group A
10 Fixed Group B
82A
75 mS Blank Time
No transmission
80B
81B
20 Bits
Recovery Identifier
0000 (for precharge)
1111 (Illegal)
01 (2nd Frame ID)
00 (no payload)
8 bit
Roll Group G
30 Bits
10 Roll Group H
10 Fixed Group C
10 Fixed Group D
82B
75 mS Blank Time
No transmission

FIG. 11

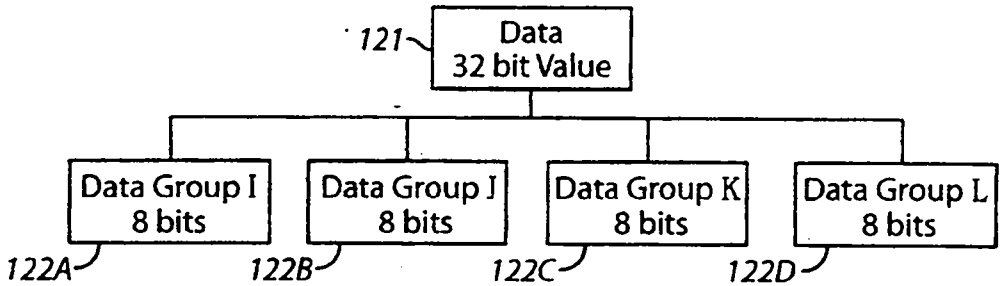
121
Data
32 bit Value
Data Group I
8 bits
Data Group J
8 bits
Data Group K
8 bits
Data Group L
8 bits
122A
122B
122C
122D

FIG. 12

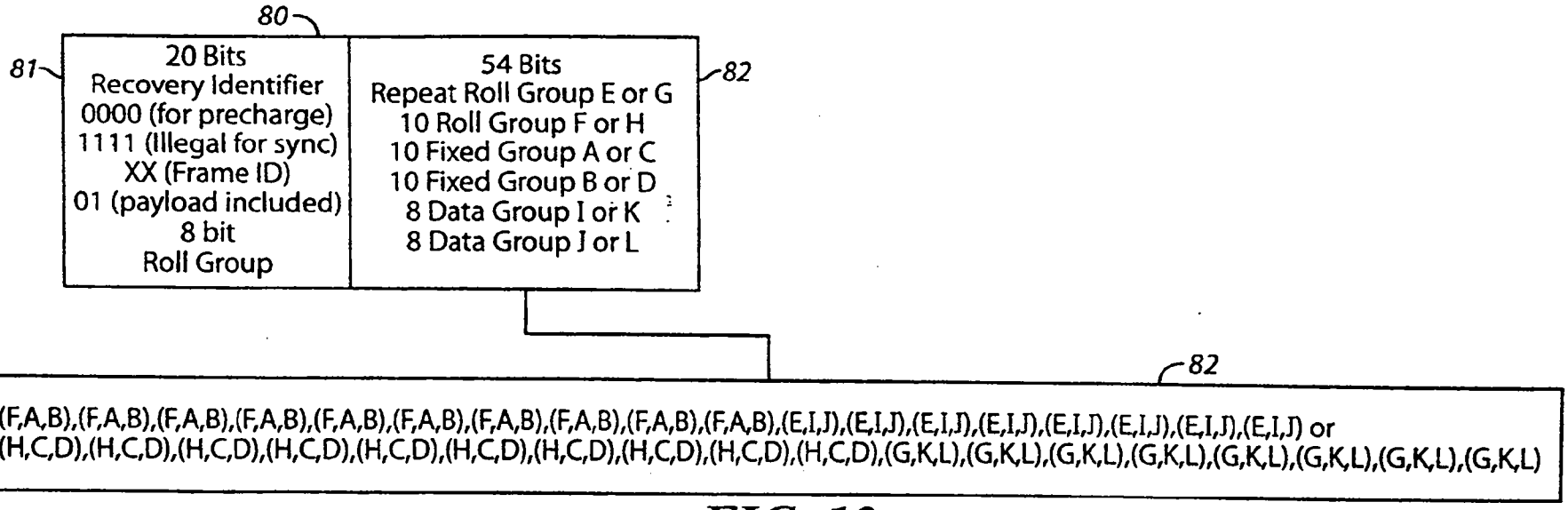

FIG. 13

141

B7	B6	B5	B4	Order of bits	B3	B2	B1	B0	Inversion Pattern
0	0	0	0	F/H/E/G,B/D/J/L,A/C/I,K	0	0	0	0	Normal Normal Normal
0	0	0	1	F/H/E/G,A/C/I/K,B/D/J/L	0	0	0	1	Normal Normal Invert
0	0	1	0	A/C/I/K,B/D/J/L,F/H/E/G	0	0	1	0	Normal Invert Normal
0	1	0	0	A/C/I/K,F/H/E/G,B/D/J/L	0	1	0	0	Normal Invert Invert
0	1	0	1	B/D/J/L,F/H/E/G,A/C/I/K	0	1	0	1	Invert Normal Normal
0	1	1	0	B/D/J/L,A/C/I/K,F/H/E/G	0	1	1	0	Invert Normal Invert
1	0	0	0	F/H/E/G,A/C/I/K,B/D/J/L	1	0	0	0	Invert Invert Normal
1	0	0	1	A/C/I/K,F/H/E/G,B/D/J/L	1	0	0	1	Invert Invert Invert
1	0	1	0	B/D/J/L,A/C/I/K,F/H/E/G	1	0	1	0	Invert Invert Invert

FIG. 14

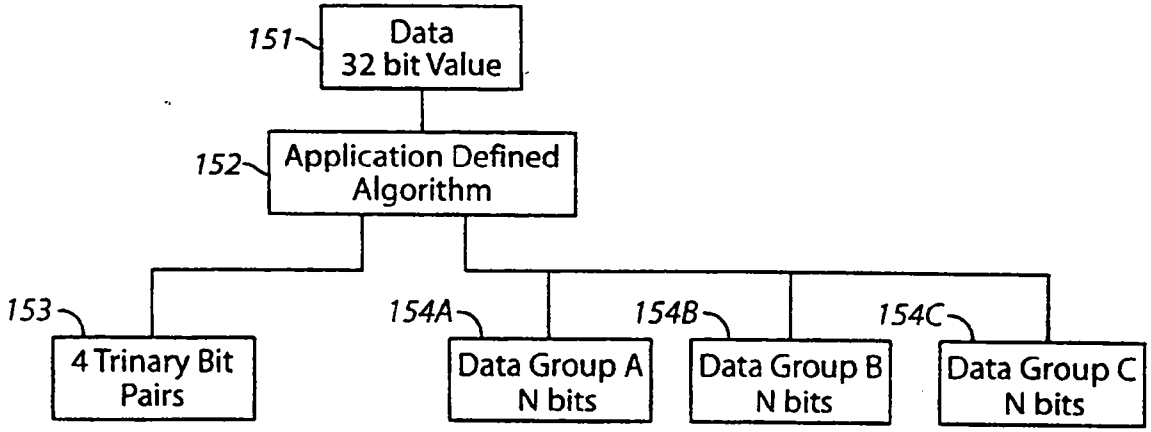
151
Data
32 bit Value
152
Application Defined
Algorithm
153
4 Trinary Bit
Pairs
154A
Data Group A
N bits
154B
Data Group B
N bits
154C
Data Group C
N bits

FIG. 15

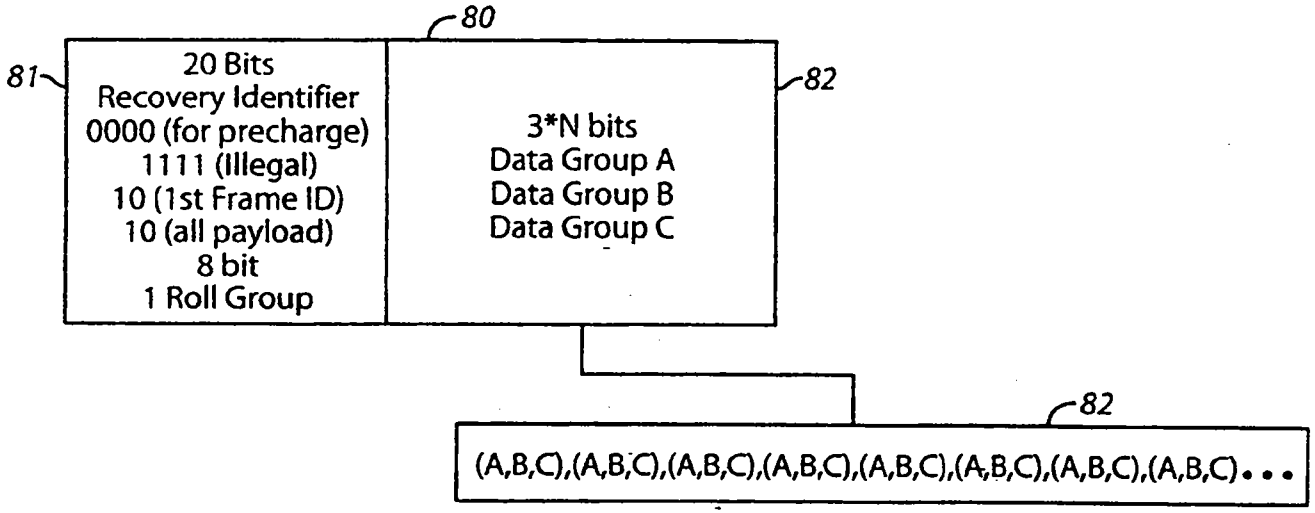
80
81
20 Bits
Recovery Identifier
0000 (for precharge)
1111 (Illegal)
10 (1st Frame ID)
10 (all payload)
8 bit
1 Roll Group
82
3*N bits
Data Group A
Data Group B
Data Group C
82
(A,B,C),(A,B,C),(A,B,C),(A,B,C),(A,B,C),(A,B,C),(A,B,C),(A,B,C)...

FIG. 16

171

B7	B6	B5	B4	Order of bits	B3	B2	B1	B0	Inversion Pattern
0	0	0	0	ABC	0	0	0	0	Normal Normal Normal
0	0	0	1	ACB	0	0	0	1	Normal Normal Invert
0	0	1	0	CBA	0	0	1	0	Normal Invert Normal
0	1	0	0	CAB	0	1	0	0	Normal Invert Invert
0	1	0	1	BAC	0	1	0	1	Invert Normal Normal
0	1	1	0	BCA	0	1	1	0	Invert Normal Invert
1	0	0	0	ACB	1	0	0	0	Invert Invert Normal
1	0	0	1	CAB	1	0	0	1	Invert Invert Invert
1	0	1	0	BCA	1	0	1	0	Invert Invert Invert

FIG. 17

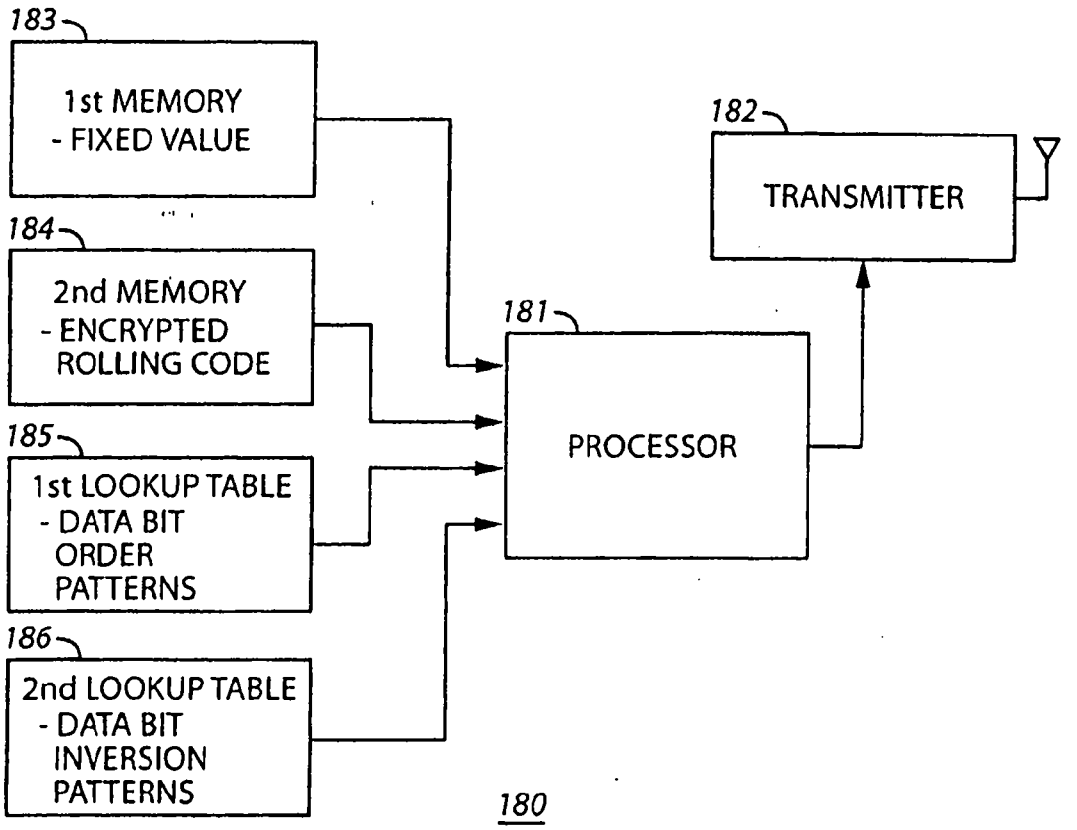

FIG. 18