Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2633858 C 2015/08/11

(11)(21) **2 633 858**

(12) **BREVET CANADIEN**
CANADIAN PATENT

(13) **C**

(22) **Date de dépôt/Filing Date:** 2008/06/05

(41) **Mise à la disp. pub./Open to Public Insp.:** 2008/12/07

(45) **Date de délivrance/Issue Date:** 2015/08/11

(30) **Priorité/Priority:** 2007/06/07 (US11/759,277)

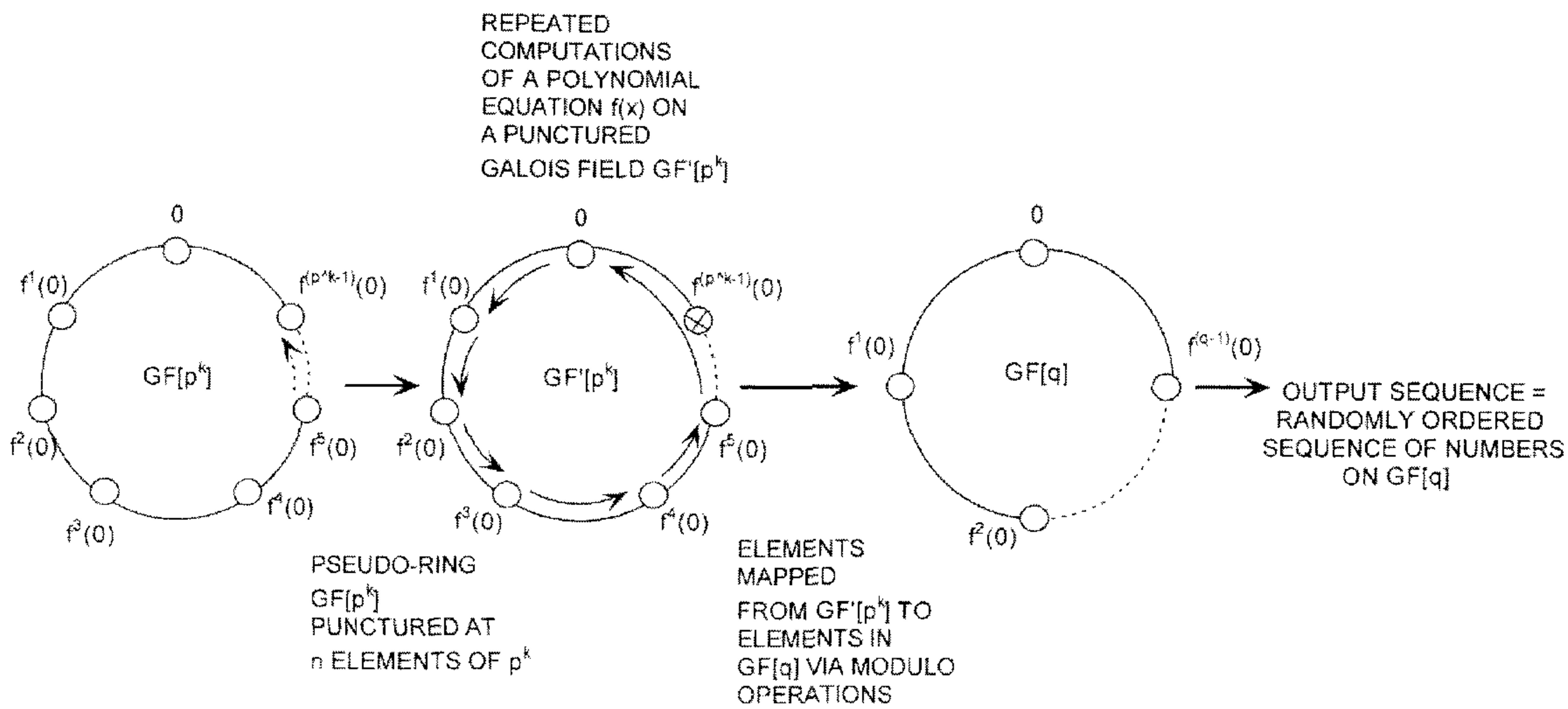
(51) **Cl.Int./Int.Cl.** ***G06F 7/58*** (2006.01), ***G06F 5/00*** (2006.01), ***G06F 7/49*** (2006.01)

(72) **Inventeurs/Inventors:**
MICHAELS, ALAN J., US;
CHESTER, DAVID B., US

(73) **Propriétaire/Owner:**
HARRIS CORPORATION, US

(74) **Agent:** GOUDREAU GAGE DUBUC

(54) **Titre : CONVERSION A RACINES MIXTES AVEC ARTEFACTS STATISTIQUES DEFINIS A PRIORI**
(54) **Title: MIXED RADIX CONVERSION WITH A PRIORI DEFINED STATISTICAL ARTIFACTS**



(57) **Abrégé/Abstract:**

A method is provided for masking a process used in generating a random number sequence. The method includes generating a random number sequence. This step involves selectively generating the random number sequence utilizing a ring structure which has been punctured. The method also includes performing a mixed radix conversion to convert the random number sequence from a first number base to a second number base. The method further includes puncturing the ring structure by removing at least one element therefrom to eliminate a statistical artifact in the random number sequence expressed in the second number base. The first number base and second number base are selected so that they are respectively defined by a first Galois field characteristic and a second Galois field characteristic.

ABSTRACT

A method is provided for masking a process used in generating a random number sequence. The method includes generating a random number sequence. This step involves selectively generating the random number sequence utilizing a ring structure which has been punctured. The method also includes performing a mixed radix conversion to convert the random number sequence from a first number base to a second number base. The method further includes puncturing the ring structure by removing at least one element therefrom to eliminate a statistical artifact in the random number sequence expressed in the second number base. The first number base and second number base are selected so that they are respectively defined by a first Galois field characteristic and a second Galois field characteristic.

MIXED RADIX CONVERSION WITH A PRIORI DEFINED STATISTICAL ARTIFACTS

The inventive arrangements relate to communications systems having ring generators. More particularly, the inventive arrangements relate to a method and system for performing a mixed radix conversion absent of unwanted statistical artifacts.

Many number theoretic based computational systems can include ring generators. A ring generator is a simple structure over a finite field that exhaustively produces possible outputs through repeated mapping. The mapping is some combination of an additive and a multiplicative mapping, with irreducible polynomials being ideal. For example, a ring generator includes repeated computations of an irreducible polynomial $f(x) = 3x^3 + 3x^2 + x$ on the finite Galois field, GF[11]. A finite or Galois field GF[M] is a field that contains only a finite number of elements {0, 1, 2, ..., M-1}. The finite or Galois field GF[M] has a finite field size defined by the Galois characteristic M. M is most often chosen to be either a power of two (2) or an odd prime.

Despite the advantages of such a ring generator, it suffers from certain drawbacks. For example, the odd-sized ring generator's reliance on the Galois characteristic M is computationally inefficient in a digital (binary) domain. Also, lookup table operations performed in the finite or Galois field GF[M] are resource intensive. Moreover, the ring generator's orbits are highly deterministic. As such, knowledge of a mapping and current finite field conditions gives complete knowledge of an output sequence and in many applications it is desirable to mask this information. Such applications include, but are not limited to, a spread spectrum communications application and a cryptography application.

In view of the forgoing, there remains a need for a ring generator implementing an arithmetic operation that is computationally efficient in a digital (binary) domain. There is also a need for a ring generator having an implementation that is less hardware intensive than conventional ring generator implementations. There is further a need for a ring generator having orbits that are more robust in obscuring their deterministic characteristics.

The invention concerns a method for masking a process used in generating a random number sequence. The method includes generating a random number sequence. This step involves selectively generating the random number sequence utilizing a ring structure which has been punctured. The method also includes performing a mixed radix conversion to convert the random number sequence from a first number base to a second number base. The method further includes using the random number sequence to modify a data stream. The term "random number sequence" as used herein refers to a sequence of numerical values that each mimic independent random numbers from a chosen statistical distribution.

According to an aspect of the invention, the method includes puncturing the ring structure by removing at least one element therefrom. This puncturing is performed to eliminate a statistical artifact in the random number sequence expressed in the second number base. The method also includes selecting the punctured elements to induce a chosen statistical artifact in the mixed radix conversion. The method further includes selecting the first number base and the second number base so that they are respectively defined by a first Galois field characteristic and a second Galois field characteristic. The first Galois field characteristic can be selected so that it is mutually prime with respect to the second Galois field characteristic. The second Galois field characteristic is selected to be a finite field size which is smaller than a finite field size of a first Galois field.

According to another aspect of the invention, the puncturing step further comprises eliminating n element(s) from the ring structure. This puncturing is performed to remove at least one statistical artifact in the random number sequence expressed in the second number base. n is determined based on a mathematical relation between a number of elements in the first Galois field and the number of elements in the second Galois field. More particularly, n is determined based on a remainder value resulting from a quotient of the number of elements in the first Galois field divided by the number of elements in the second Galois field.

According to yet another aspect of the invention, the mixed radix conversion produces a plurality of equivalence classes in the second number base. The n elements which are eliminated from the ring structure are selected to ensure that each equivalence class has an equal number of elements after performing the mixed radix conversion.

A system is also provided. The system comprises a generator and a mixed radix converter. The generator is configured to selectively generate a random number sequence utilizing a ring structure which has been punctured. The mixed radix converter is configured to perform a mixed radix conversion. The mixed radix conversion is performed to convert the random number sequence from a first number base to a second number base. The ring structure which has been punctured and the mixed radix converter are configured in combination to produce a random number sequence in the second number base which is exclusive of any statistical artifacts associated with the mixed radix conversion.

According to an aspect of the invention, the system is further comprised of a means for modifying a data stream utilizing the random number sequence. According to another aspect of the invention, the first number base is defined by a first Galois field characterisitc or a compilation of Galois fields of mutually prime characteristic combined via a method similar to the Chinese Remainder Theorem. Similarly, the second number base is defined by a second Galois field characteristic or a compilation of Galois fields of mutually prime characteristic combined via a method similar to the Chinese Remainder Theorem. The first Galois field characteristic is mutually prime with respect to the second Galois field characteristic. The second Galois field characteristic is selected to be a finite field size which is smaller than a finite field size of a first Galois field.

According to another aspect of the invention, the ring structure has n element(s) removed therefrom to eliminate at least one statistical artifact in the random number sequence expressed in the second number base. n is determined based on a mathematical relation between a number of elements in the first Galois field and the number of elements in a second Galois field. More particularly, n is determined based on a remainder value resulting from a quotient of the number of elements in the first Galois field divided by the number of elements in the second Galois field.

According to yet another aspect of the invention, the mixed radix conversion produces a plurality of equivalence classes in the second number base. The n elements which are removed from the ring structure are selected to ensure that each equivalence class has an equal number of elements after the mixed radix conversion.

Embodiments will be described with reference to the following drawing figures, in which like numerals represent like items throughout the figures, and in which:

FIG. 1 is a conceptual diagram of a conventional mixed radix conversion algorithm that is useful for understanding the invention.

FIG. 2 is a conceptual diagram of a method for removing unwanted statistical artifacts in a mixed radix conversion algorithm that is useful for understanding the invention.

FIG. 3 is a schematic illustration of a mixed radix conversion of elements from a Galois field GF[7] to a Galois field GF[3] that is useful for understanding the invention.

FIG. 4 is a flow diagram of a method for masking a process used in generating a random number sequence that is useful for understanding the invention.

FIG. 5 a flow diagram of a conventional method for altering a data stream that is useful for understanding the invention.

FIG. 6 a flow diagram of a method for increasing the security of communications system that is useful for understanding the invention.

FIG. 7 is a block diagram of a system having a punctured ring generator that is useful for understanding the invention.

Referring now to FIG. 1, there is provided a conceptual diagram of a conventional mixed radix conversion algorithm that is useful for understanding the invention. The phrase "mixed radix conversion" as used herein refers to a conversion of a number sequence from a first number base (or radix) to a second number base (or radix). For example, a number sequence expressed in a Galois field GF[7] base is converted to a number sequence expressed in a Galois field GF[3] base.

In communications systems, various algorithms are employed for combining a number sequence with a data stream. This combining process can be performed for encrypting or masking the data stream prior to its transmission over a communications link. Such algorithms can include residue number system (RNS) operations for expressing each number of the number sequence in a Galois field [p] base. A Galois field GF[p] is a field that contains only a finite number of elements {0, 1, 2, ..., p-1}. As such, all arithmetic operations performed in the finite or Galois field result in an element within that field. The finite or Galois field GF[p] has a finite field size defined by the Galois characteristic p. As such, a resulting sequence of a Galois field GF[p] operation can repeat every p^{th} element. These RNS operations are well known to persons skilled in the art, and therefore will not be described in great detail herein.

Notably, there is a statistical non-uniformity in an element distribution resulting from a number sequence conversion from a first Galois field $GF[p_1^{k1}]$ base to a second Galois field $GF[p_2^{k2}]$ base when the two (2) number bases are not evenly divisible. For example, a number sequence expressed in a Galois field GF[7] base is mapped to a number sequence expressed in a Galois field GF[3] base. The random number sequence expressed in a Galois field GF[7] base is defined by the set of elements {0, 1, 2, ..., 6}. Similarly, the number sequence expressed in a Galois field GF[3] base is defined by the set of elements {0, 1, 2}. Mapping the number sequence expressed in a Galois field GF[7] base to a number sequence expressed in the Galois field GF[3] base generally involves segmenting each element {0, 1, 2, ..., 6} by their corresponding equivalence class modulo three (3). Since the Galois field GF[3] is a finite field that contains only a finite number of elements {0, 1, 2}, there is a corresponding equivalence class for the integers zero (0), one (1), and two (2).

The mapping operations of the elements from the Galois field GF[7] to elements in a Galois field GF[3] are listed in the following Table (1).

TABLE 1

Elements From A Galois Field GF[7]:	Mapping Operations:	Equivalent Elements In A Galois Field GF[3]:
0	0 modulo 3	0
1	1 modulo 3	1
2	2 modulo 3	2
3	3 modulo 3	0
4	4 modulo 3	1
5	5 modulo 3	2
6	6 modulo 3	0

As illustrated in Table 1, the mapping operations result in a non-uniform distribution of the elements over the Galois field GF[3]. Specifically, the resulting sequence of the mapping operations is defined as {0 1 2 0 1 2 0}. There are three elements {0, 3, 6} from the Galois field GF[7] in an equivalence class for the integer zero (0). There are two (2) elements {1, 4} from the Galois field GF[7] in an equivalence class for the integer one (1). There are two (2) elements {2, 5} from the Galois field GF[7] in an equivalence class for the integer two (2). The non-uniformity is apparent since different equivalence classes contain different numbers of elements.

By utilizing a statistical analysis, an attacker of a cryptographic or spread spectrum system implementing the conventional mixed radix conversion algorithm (described above in relation to FIG. 1) can more easily identify an original number sequence from a data stream altered by a resulting number sequence of the mapping operations. For example, if one knows the sizes of the two (2) number bases, then the attacker can use the statistical proportion of elements in the various equivalence classes to identify the original number sequence from the altered data stream. As such, it is desirable to remove statistical artifacts from results derived by a mixed radix conversion algorithm so that identifying an original number sequence from an altered data stream is more difficult.

Accordingly, some embodiments of the present invention provide a method for removing unwanted statistical artifacts in a mixed radix conversion. This method generally includes puncturing a Galois field $GF[2^k]$ pseudo-ring. As used herein, the term "puncturing" means discarding one or more elements in a Galois field $GF[2^k]$ that exceed an integer multiple of a desired characteristic. The "puncturing" is performed to maintain a perfectly uniform distribution over a desired number base. The desired number base includes, but is not limited to, prime number bases that are smaller than the Galois field $GF[2^k]$ base. The Galois field $GF[2^k]$ base is preferably mutually prime with respect to the desired number base. The phrase "mutually prime" as used herein refers to two or more integers having no common divisor except one (1). This method can be used in a variety of communications system applications. For example, such a method can be implemented in a cryptographic system. In such a scenario, the method can be used to increase a security feature of a cryptographic system.

The present invention will now be described more fully hereinafter with reference to accompanying drawings, in which illustrative embodiments of the invention are shown. This invention, may however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. For example, the present invention can be embodied as a method, a data processing system, or a computer program product. Accordingly, the present invention can take the form as an entirely hardware embodiment, an entirely software embodiment, or a hardware/software embodiment.

Referring now to FIG. 2, there is provided a conceptual diagram of a method for removing unwanted statistical artifacts in a mixed radix conversion that is useful for understanding the invention. The mixed radix conversion begins with a pseudo-ring defined by a Galois field $GF[p^k]$, where p^k is a number defining a finite field size of the Galois field $GF[p^k]$. According to an embodiment of the invention, p is advantageously selected to have a value other than two (2). Still, the invention is not limited in this regard. As should be understood, the Galois field $GF[p^k]$ is a field that contains only a finite number of elements $\{0, 1, 2, \ldots, p^k-1\}$. In order to guarantee a mapping having a uniform distribution over a Galois field GF[q], at least one element of the Galois field $GF[p^k]$ is discarded. In other words, the Galois field $GF[p^k]$ is punctured at one or more elements so as to have a mapping defined by an integer number of complete cycles in a Galois field GF[q] pseudo-ring. The elements discarded need not be contiguous or chosen in any specific order besides their resulting equivalence class in the second Galois field, GF[q]. Moreover, a larger number of elements than the minimum necessary to remove statistical artifacts may be removed in order to more completely mask the attributes of the conversion.

In this regard, it should be appreciated that the number of cycles in the Galois field GF[q] pseudo-ring can be defined by a mathematical Equation (1).

$$NOC = (p^k-n) / q \qquad (1)$$

where NOC is the number of cycles in a punctured Galois field GF[p^k-n] pseudo-ring. p^k-n is a positive integer defining a finite field size of a punctured Galois field GF[p^k-n]. q is a positive integer defining a finite field size of a Galois field GF[q].

By substituting the values for p^k, n, and q into the mathematical Equation (1), the NOC for the Galois field GF[q] pseudo-ring can be computed. For example, if p^k equals twenty-seven (27), q equals five (5), and the number of punctures n is seven (7), then the NOC for the Galois field GF[5] pseudo-ring equals four (4). In accordance with the embodiment shown in FIG. 2, the Galois field GF[3^3] (or Galois field GF[27]) could be punctured at elements {1, 5, 9, 17, 18, 20, 26}. Alternatively, the same Galois field GF[27] ring could be punctured at elements {0, 1, 2, 3, 4, 5, 6}. Still, the invention is not limited in this regard.

The mixed radix conversion continues with repeated computations of a polynomial equation f(x) modulo p^k on a punctured Galois field GF'[p^k], which contains p^k -n elements. The results of the computations are numbers expressed in a number base defined by the punctured Galois field GF'[p^k] modulo the second number base q. For example, if the punctured Galois field GF'[p^k] is selected as a Galois field GF[10] punctured at element nine (9), then the resulting sequence can have a size GF'[10] (or GF[9]). As such, the resulting sequence is defined by the elements {0, 1, 2, ..., 8}. The elements of this resulting sequence are mapped to elements in a Galois field GF[q].

The following Examples are provided in order to further illustrate the present invention. The scope of the present invention, however, is not to be considered limited in any way thereby.

EXAMPLE 1

Referring now to FIG. 3, a ring generator is selected to include repeated computations of the trivial polynomial equation f(x)=x on a Galois field GF[7]. The Galois field GF[7] is a field that contains only a finite number of elements {0, 1, 2, ..., 6}. The elements of the Galois field GF[7] are mapped to elements in a Galois field GF[3]. In order to guarantee a uniform distribution over a pseudo-ring defined by the Galois field GF[3], the element of the Galois field GF[7] having a value of six (6) is discarded. In other words, the Galois field GF(7) is punctured at element six (6) so as to have a mapping defined by two (i.e., 6/3 = 2) complete cycles in the Galois field GF[3]. It should be noted that an equivalent puncturing operation could be obtained by choosing to puncture GF[7] at element zero (0) or element three (3) instead of element six (6).

In this regard, it should be appreciated that the number of cycles in the Galois field GF[3] pseudo-ring is defined by the previously discussed mathematical Equation (1), repeated below.

$$NOC = (p^k-n) / q$$

where NOC is the number of cycles in the Galois field GF[3] pseudo-ring. Values for the variables are p=7, k=1, n=1, and q=3.

The mappings of the elements in the punctured Galois field GF'[7] to elements in a Galois field GF[3] are listed in the following Table (2).

TABLE 2

Elements From A Punctured Galois Field GF'[7]:	Mapping Operations:	Elements In A Galois Field GF[3]:
0	0 modulo 3	0
1	1 modulo 3	1
2	2 modulo 3	2
3	3 modulo 3	0
4	4 modulo 3	1
5	5 modulo 3	2

As illustrated in Table 3, the mapping operations result in a uniform distribution of the elements over the Galois field GF[3]. Specifically, the resulting sequence of the mapping operations is defined as {0 1 2 0 1 2}. There are two elements {0, 3} from the Galois field GF[7] in an equivalence class for the integer zero (0). There are two (2) elements {1, 4} from the Galois field GF[7] in an equivalence class for the integer one (1). There are two (2) elements {2, 5} from the Galois field GF[7] in an equivalence class for the integer two (2).

EXAMPLE 2

A ring generator is selected to include repeated computations of a polynomial equation f(x) on a Galois field GF[233]. The Galois field GF[233] is a field that contains only a finite number of elements {0, 1, 2, ..., 232}. The elements of the Galois field GF[233] are mapped to elements in a Galois field GF[5]. In order to guarantee a uniform distribution over a Galois field GF[5], thirteen (13) elements of the Galois field GF[233] are discarded. Chosen arbitrarily, the last thirteen (13) elements are discarded via puncturing. In other words, the Galois field GF[233] pseudo-ring is punctured at element two hundred twenty (220) through element two hundred thirty two (232) so as to have a mapping defined by forty-four (i.e., 220/5 = 44) complete cycles in a Galois field GF[5] pseudo-ring.

In this regard, it should be appreciated that the number of cycles in the Galois field GF[5] pseudo-ring is defined by a mathematical Equation (2).

$$NOC = p_1/p_2 \tag{2}$$

where NOC is the number of cycles in the Galois field GF[5] pseudo-ring. p_1 is a positive integer number defining a finite field size of a first Galois field GF[233]. p_2 is a positive integer number defining a finite field size of a second Galois field GF[5].

By substituting the values for p^k, n, and q into the mathematical Equation (1), the NOC for the Galois field GF[5] pseudo-ring can be computed as follows: NOC = $(233^1-13)/5 = 44$. Accordingly, there are forty four (44) complete cycles through the Galois field GF[5] pseudo-ring.

The mappings of the elements of the punctured Galois field GF'[233] to elements in a Galois field GF[5] are listed in the following Table (3).

TABLE 3

Elements From A Punctured Galois Field GF'[233]:	Mapping Operations:	Elements In A Galois Field GF[5]:
0	0 modulo 5	0
1	1 modulo 5	1
2	2 modulo 5	2
3	3 modulo 5	3
4	4 modulo 5	4
5	5 modulo 5	0
....		
215	215 modulo 5	0
216	216 modulo 5	1
217	217 modulo 5	2
218	218 modulo 5	3
219	219 modulo 5	4

As illustrated in Table 3, the mapping operations result in a uniform distribution of the elements over the Galois field GF[5]. Specifically, the resulting sequence of the mapping operations is defined as {0 1 2 3 4 ... 0 1 2 3 4}. There are the same number of elements from the Galois field GF[5] in each of the equivalence classes for the integers zero (0), one (1), two (2), three (3), and four (4).

Referring now to FIG. 4, there is provided a flow diagram of a method 400 for masking a process used in generating a random number sequence. As shown in FIG. 4, the method 400 begins with step 402 and continues with step 404. In step 404, a first number base and second number base are selected. The first number base defines a size of a first finite field. The first finite field can be defined by a first Galois field $GF[p^k]$ or a first Galois field GF[M]. The second number base defines a size of a second finite field. The second finite field can be defined by a second Galois field GF[q]. The first Galois field can be selected so that it is mutually prime with respect to the second Galois field. The second Galois field can be selected so that it has a finite field size smaller than a finite field size of the first Galois field.

After step 404, the method 400 continues with step 406. In step 406, a ring structure is punctured by removing at least one element therefrom. The ring structure is defined by the first finite field or a first Galois field. This puncturing is performed to eliminate a statistical artifact in a random number sequence expressed in the second number base. The statistical artifact can include a statistical artifact of a mixed radix conversion (described below in relation to step 410). This step can further involve removing n elements from the ring structure. n is determined based on a mathematical relation between a number of elements in the first finite field or Galois field and a number of elements in the second finite field or Galois field. More particularly, n is determined based on a remainder value resulting from a quotient of the number of elements in the first finite field or Galois field GF divided by the number of elements in the second finite field or Galois field.

Subsequently, step 408 is performed where a random number sequence is generated. This step can involve selectively generating the random number sequence utilizing the ring structure which has been punctured. It should be appreciated that the random number sequence generated in this step is expressed in the first number base. In step 410, a mixed radix conversion is performed to convert the random number sequence from the first number base to the second number base. It should be understood that the mixed radix conversion produces a plurality of equivalent classes in the second number base. The n elements which are removed from the ring structure are selected to ensure that each equivalence class has an equal number of elements after performing this step. Thereafter, step 412 is performed where the method 400 ends.

A person skilled in the art will appreciate that method 400 is one method for masking a process used in generating a random number sequence. However, the invention is not limited in this regard and any other method for masking a process used in generating a random number sequence can be used without limitation.

Method for Altering A Data Stream

Referring now to FIG. 5, there is provided a flow diagram of a conventional method 500 for altering a data stream that is useful for understanding the invention. As shown in FIG. 5, the method 500 begins with step 502 and continues with step 504. In step 504, a random number sequence is generated. It should be understood that the sequence of random numbers are contained within a relatively large Galois field GF[M]. After generating the random number sequence, step 506 is performed where a portion of the random number sequence is selected.

After step 506, the method 500 continues with step 508. In step 508, the portion of the random number sequence is communicated to a device employing a combination method. Such devices include a multiplier, an adder, a digital logic device, a feedback mechanism, or similar combining function device. Thereafter, the portion of the random number sequence is incorporated or combined with a data stream thereby altering the data stream. In this regard, it should be understood that the portion of the random number sequence and data stream have the same size, i.e., they are expressed in the same number base (or radix) and contain the same number of digits. As such, the method 500 can be modified accordingly. For example, the method 500 can include a conversion step prior to the step 508. The conversion step can involve converting the portion of the random number sequence from a size GF[M] to a size n if the data stream is of a size GF[n] or GF[n/d], where d is an even divisor of n. Subsequently, step 512 is performed where the method 500 ends.

As should be understood, a relatively large Galois field GF[M] provides a certain degree of security to the conventional method 500. In this regard, it should be appreciated that the Galois field GF[M] is a field that contains only a finite number of elements {0, 1, 2, ..., M-1}. As such, an output sequence can repeat every M^{th} element. This repetitive behavior can produce correlations thereby making a decoding of an altered data stream relatively easy when M is small. Consequently, it is desirable to select a relatively large Galois field GF[M].

It should also be appreciated that selecting a truncated portion of the random number sequence also provides a certain degree of security to the conventional method 500. For example, a random number sequence is generated on a Galois field GF[M]. The random number sequence contains five hundred (500) independent p-adic digits. A portion of the random number sequence is selected to include only sixteen (16) of the five hundred (500) digits. By using only sixteen (16) digits of the random number sequence to alter a data stream, it becomes more difficult to determine the deterministic rule employed for generating the random number sequence. Still, it is desirable to further increase the security of the method.

Referring now to FIG. 6, there is provided a method 600 for increasing the security of a communications system that is useful for understanding the invention. As shown in FIG. 6, the method 600 begins with step 602 and continues with step 604. In step 604, a relatively large Galois field GF[M] is selected. As should be understood, a large Galois field can minimize the likelihood that an attacker of a communications system can determine the Galois field GF[M] employed for generating an original random number sequence from an altered data stream. In effect, the large Galois field GF[M] can provide a certain degree of security to a communications system implementing method 600.

Thereafter, step 606 is performed where certain elements are removed from the Galois field GF[M]. The elements are selected as elements that can provide a statistical artifact useful for identifying the Galois field GF[M] from an altered data stream. For example, the elements are selected so that a mixed radix conversion of the same is defined by a set of complete cycles in a Galois field GF[q] pseudo-ring. As a result, this step assures that a subsequent mixed radix conversion will be absent of unwanted statistical artifacts. In effect, this step provides an increased degree of security to a communications system implementing method 600 by making the deterministic rule defining the output sequence dependant on a non-advertised mutually prime number base.

Subsequently, the method 600 continues with step 608. In step 608, a random number sequence is generated on the punctured Galois field GF'[M]. Each random number of the sequence is defined by an element of the punctured Galois field GF'[M].

In step 610, a mixed-radix conversion is performed from a Galois field GF[M] to a Galois field GF[q]. This step involves selecting a portion of the random number sequence. This step also involves converting the selected portion of the random number sequence from a punctured Galois field GF'[M] to the resulting output number base represented by the Galois field GF[q]. This step provides an even higher degree of security to a communications system implementing method 600. In this regard, it should be appreciated that it becomes more difficult to determine the Galois field GF[M] and the underlying random number sequence when a mixed-radix conversion is used prior to altering a data stream.

After step 610, step 612 is performed where the resulting value from step 610 mapped on the Galois field GF[q] is communicated to a device employing a combination method for masking a data stream. The combination method may be standard multiplication, multiplication in a Galois extension field, addition modulo q, subtraction modulo q, bitwise logic operations, or any other standard combination method. In this regard, it should be understood that the Galois field GF[q] output and input data stream need not have the same size if proper combination techniques are used. In step 614, the resulting value from step 610 is combined with a data stream to form an altered data stream. Thereafter, step 616 is performed where the method 600 ends.

A person skilled in the art will appreciate that method 600 is one method for increasing a security of a communications system. However, the invention is not limited in this regard and any other method implementing the present invention can be used without limitation.

Hardware Implementation

Referring now to FIG. 7, there is provided a system 700 that is useful for understanding the invention. As shown in FIG. 7, the system 700 is comprised of a punctured ring generator 702 and a mixed radix converter 704. It should be understood that the punctured ring generator 702 and the mixed radix converter 704 are configured in combination to produce a random number sequence in a second number base which is exclusive of any statistical artifacts associated with a mixed radix conversion.

As shown in FIG. 7, the punctured ring generator 702 is comprised of hardware and software configured to generate a random number sequence expressed in a first number base. The punctured ring generator 702 is also comprised of hardware and software configured to selectively generate the random number sequence utilizing a ring structure which has been punctured. The ring structure can be a punctured Galois field GF'[M] pseudo-ring. Each of the random numbers can each be defined by or as an element from the punctured Galois field GF'[M]. The ring structure has at least one element removed therefrom to eliminate a statistical artifact in a random number expressed in a second number base. The punctured ring generator 702 is further comprised of hardware and software configured to communicate random numbers to the mixed radix converter 704.

The mixed radix converter 704 is comprised of hardware and software configured to perform mixed radix conversion. The mixed radix conversion involves performing arithmetic operations to convert a random number J from a first number base to a second number base. According to an aspect of the invention, the first number base is defined by a first Galois field GF[M]. Similarly, the second number base is defined by a second Galois field GF[q]. The first Galois field GF[M] can be mutually prime with respect to the second Galois field GF[q]. The second Galois field GF[q] has a finite field size smaller than the finite field size of the first Galois field GF[M].

The arithmetic operations can involve performing modulo operations. Modulo operations are well known to those skilled in the art, and therefore will not be described in great detail herein. However, it should be appreciated that modulo operations can generally be defined by a mathematical Equation (2).

$$R = J \text{ modulo } (q) \tag{2}$$

where R is a remainder derived from a modulo operation. J is a random number input to the mixed radix converter 704. q is a modulus having a value selected to be a positive integer defining a finite field size of a Galois field GF[q]. It should be noted that the range of values for J are {0, 1, 2, . . ., M} and the range of values for R are {0, 1, 2, . . ., q-1}.

The mapping operations can also involve lookup table operations. In such a scenario, the mixed radix converter 704 can query a data store (not shown) for information necessary to map a random number J modulo q. The mixed radix converter 704 is also comprised of hardware and software configured to communicate a random number J expressed in a Galois field GF[q] base to an external device (not shown).

According to an aspect of the invention, the ring structure has n elements removed therefrom. By removing the n elements from the ring structure, at least one statistical artifact is eliminated in the random number sequence expressed in the second number base. It should be understood that n is determined based on a mathematical relation between a number of elements in the first Galois field and a number of elements in a second Galois field. More particularly, n is determined based on a remainder value from a quotient of the number of elements in the first Galois field divided by the number of elements in the second Galois field.

According to another aspect of the invention, the mixed radix conversion produces a plurality of equivalence classes in the second number base. The n elements which are removed from the ring structure are selected to ensure that each equivalence class has an equal number of elements after the mixed radix conversion.

A person skilled in the art will appreciate that the system 700 is one architecture of a system implementing the present invention. However, the invention is not limited in this regard and any other system architecture implementing the present invention can be used without limitation. For example, the system can further be comprised of a means for modifying a digital data stream utilizing the random number sequence.

In light of the foregoing description of the invention, it should be recognized that the present invention can be realized in hardware, software, or a combination of hardware and software. A method of generating an arbitrary permutation ordering of bits according to the present invention can be realized in a centralized fashion in one processing system, or in a distributed fashion where different elements are spread across several interconnected processing systems. Any kind of computer system, or other apparatus adapted for carrying out the methods described herein, is suited. A typical combination of hardware and software could be a general purpose computer processor, with a computer program that, when being loaded and executed, controls the computer processor such that it carries out the methods described herein. Of course, an application specific integrated circuit (ASIC), and/or an FPGA could also be used to achieve a similar result.

The present invention can also be embedded in a computer program product, which comprises all the features enabling the implementation of the methods described herein, and which, when loaded in a computer system, is able to carry out these methods. Computer program or application in the present context means any expression, in any language, code or notation, of a set of instructions intended to cause a system having an information processing capability to perform a particular function either directly or after either or both of the following a) conversion to another language, code or notation; b) reproduction in a different material form. Additionally, the description above is intended by way of example only and is not intended to limit the present invention in any way, except as set forth in the following claims.

CLAIMS

1. A method for masking a process used in generating a random number sequence, comprising:

generating, by at least one electronic circuit, a random number sequence;

performing, by said electronic circuit, a mixed radix conversion to convert said random number sequence from a first number base to a second number base; and

combining, by said electronic circuit, said random number sequence expressed in said second number base with a sequence of symbols defining information to be stored in a storage device or transmitted over a communications link;

wherein said generating step further comprises selectively generating said random number sequence utilizing a ring structure that has been punctured.

2. The method according to claim 1, wherein said ring structure is punctured by removing at least one element therefrom to eliminate a statistical artifact in said random number sequence expressed in said second number base.

3. The method according to claim 2, wherein said at least one element is selected to induce a chosen statistical artifact in said mixed radix conversion step.

4. The method according to claim 2, wherein said first number base and said second number base are selected so that they are respectively defined by a first Galois field characteristic and a second Galois field characteristic.

5. The method according to claim 4, wherein said first Galois field characteristic is selected so that it is mutually prime with respect to said second Galois field characteristic.

6. The method according to claim 4, wherein said second Galois field characteristic is selected to be a finite field size which is smaller as compared to a finite field size of a first Galois field.

7. The method according to claim 6, wherein said puncturing step further comprises eliminating n element(s) from said ring structure to remove at least one statistical artifact in said random number sequence expressed in said second number base, wherein n is determined based on a mathematical relation between a number of elements in said first Galois field and a number of elements in a second Galois field.

8. The method according to claim 7, wherein n is determined based on a remainder value resulting from a quotient of said number of elements in said first Galois field divided by said number of elements in said second Galois field.

9. The method according to claim 7, wherein said mixed radix conversion produces a plurality of equivalence classes in said second number base, and said n elements which are eliminated from said ring structure are selected to ensure that each equivalence class has an equal number of elements after said performing a mixed radix conversion step.

10. A system, comprising:

a generator configured for selectively generating a random number sequence utilizing a ring structure which has been punctured;

a mixed radix converter configured for performing a mixed radix conversion to convert said random number sequence from a first number base to a second number base; and

wherein said ring structure which has been punctured and said mixed radix converter are configured in combination to produce a random number sequence in said second number base which is exclusive of any statistical artifacts associated with said mixed radix conversion.

11. The system according to claim 10, further comprising a means for modifying a data stream utilizing said random number sequence expressed in said second number base.

12. The system according to claim 10, wherein said first number base and said second number base are respectively defined by a first Galois field characteristic and a second Galois field characteristic.

13. The system according to claim 12, wherein said first Galois field characteristic is mutually prime with respect to said second Galois field characteristic.

14. The system according to claim 12, wherein said second Galois field characteristic is selected as a finite field size which is smaller as compared to a finite field size of a first Galois field.

15. The system according to claim 14, wherein said ring structure has n element(s) removed therefrom to eliminate at least one statistical artifact in said random number sequence expressed in said second number base, wherein n is determined based on a mathematical relation between a number of elements in said first Galois field and a number of elements in a second Galois field.

16. The system according to claim 15, wherein n is determined based on a remainder value resulting from a quotient of said number of elements in said first Galois field divided by said number of elements in said second Galois field.

17. The system according to claim 16, wherein said mixed radix conversion produces a plurality of equivalence classes in said second number base, and said n elements which are removed from said ring structure are selected to ensure that each equivalence class has an equal number of elements after said mixed radix conversion.

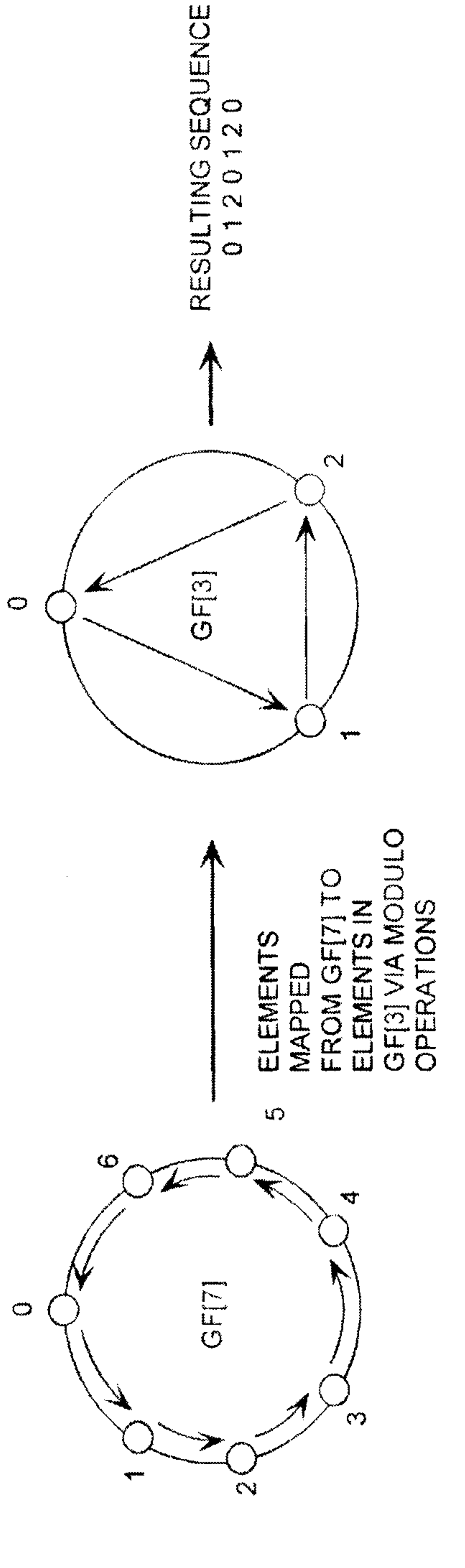


FIG. 1
(PRIOR ART)

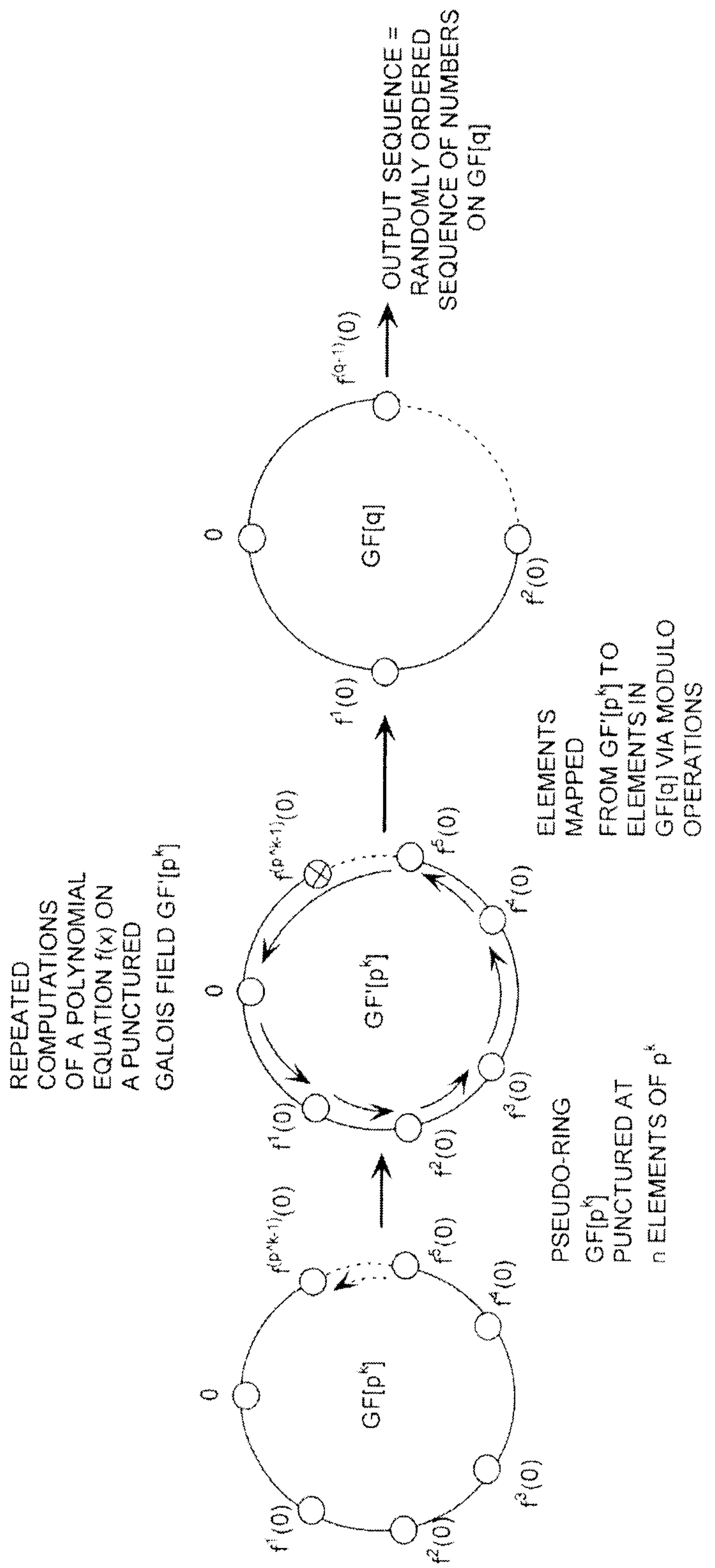

GF[p^k]
0
f^1(0)
f^2(0)
f^3(0)
f^4(0)
f^5(0)
f^(p^k-1)(0)
PSEUDO-RING GF[p^k] PUNCTURED AT n ELEMENTS OF p^k
REPEATED COMPUTATIONS OF A POLYNOMIAL EQUATION f(x) ON A PUNCTURED GALOIS FIELD GF'[p^k]
GF'[p^k]
ELEMENTS MAPPED FROM GF'[p^k] TO ELEMENTS IN GF[q] VIA MODULO OPERATIONS
GF[q]
f^(q-1)(0)
OUTPUT SEQUENCE = RANDOMLY ORDERED SEQUENCE OF NUMBERS ON GF[q]

FIG. 2

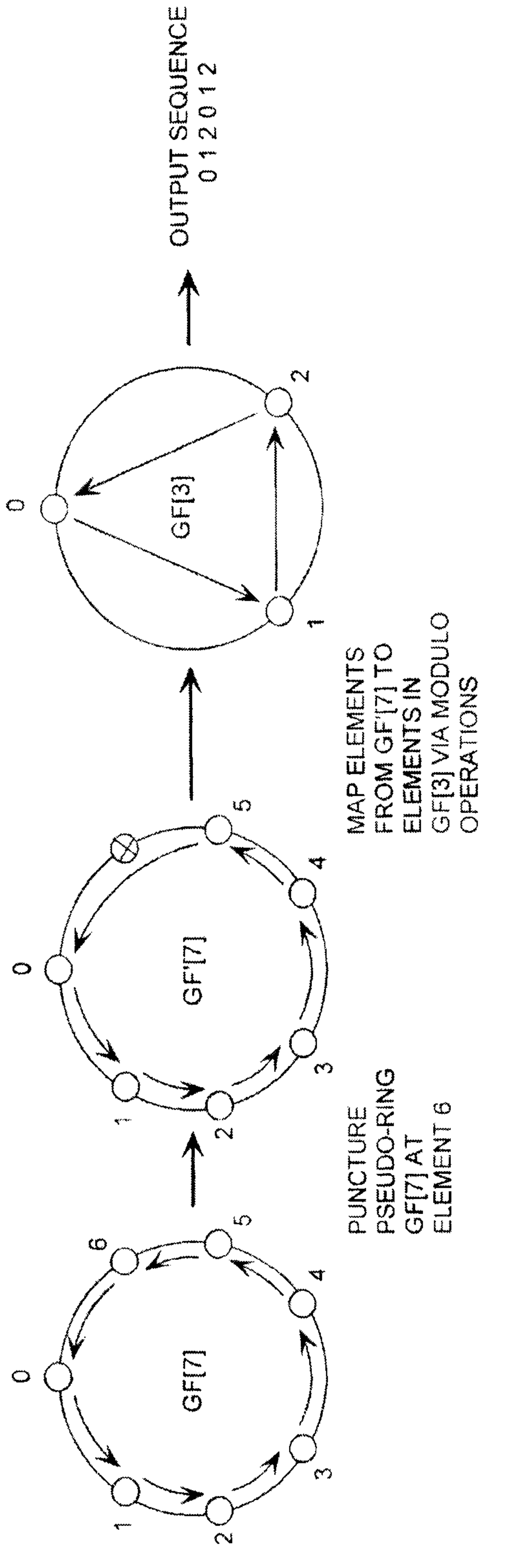

GF[7]
0
1
2
3
4
5
6
PUNCTURE
PSEUDO-RING
GF[7] AT
ELEMENT 6
GF'[7]
0
1
2
3
4
5
MAP ELEMENTS
FROM GF'[7] TO
ELEMENTS IN
GF[3] VIA MODULO
OPERATIONS
GF[3]
0
1
2
OUTPUT SEQUENCE
0 1 2 0 1 2

FIG. 3

FIG. 4

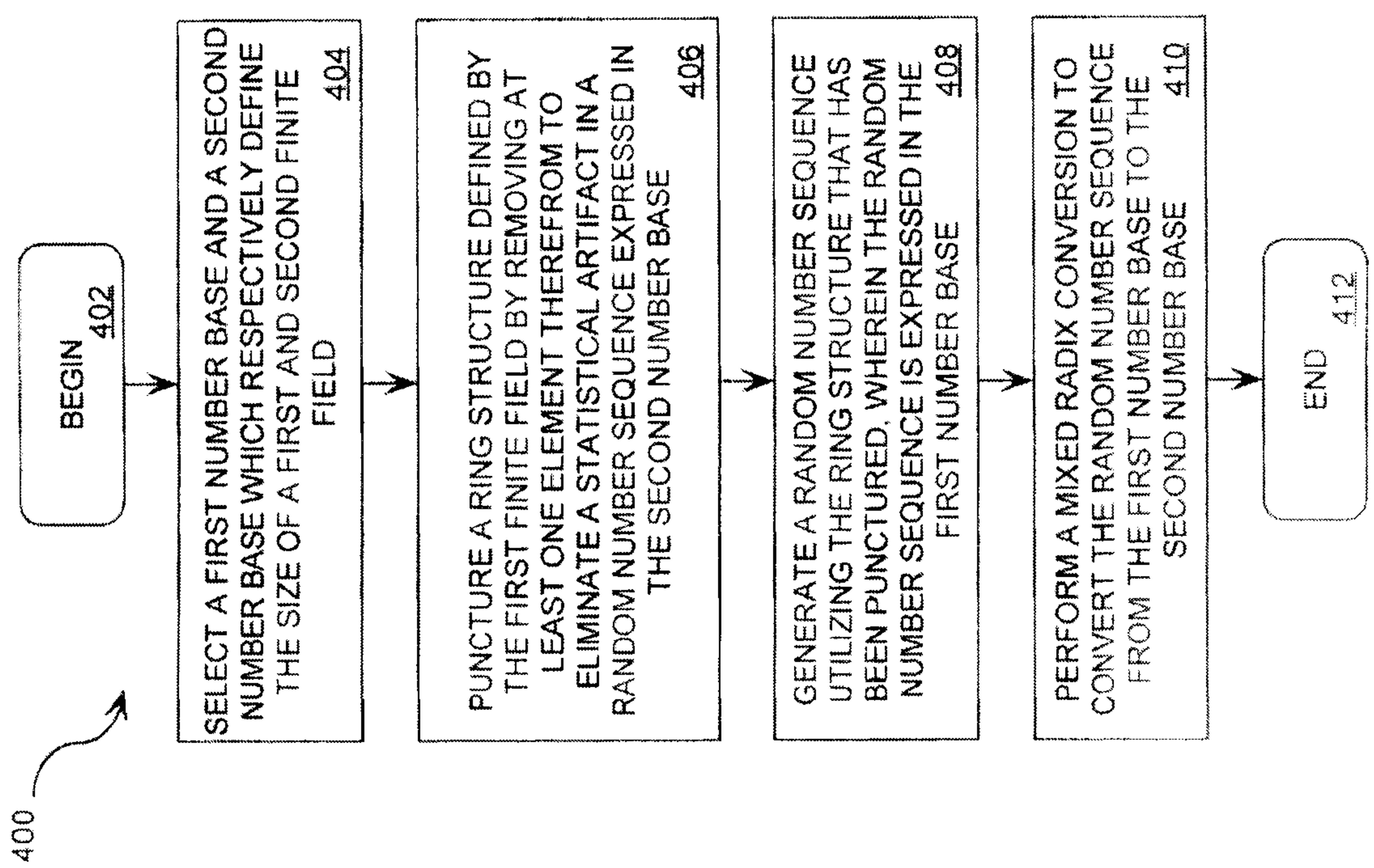
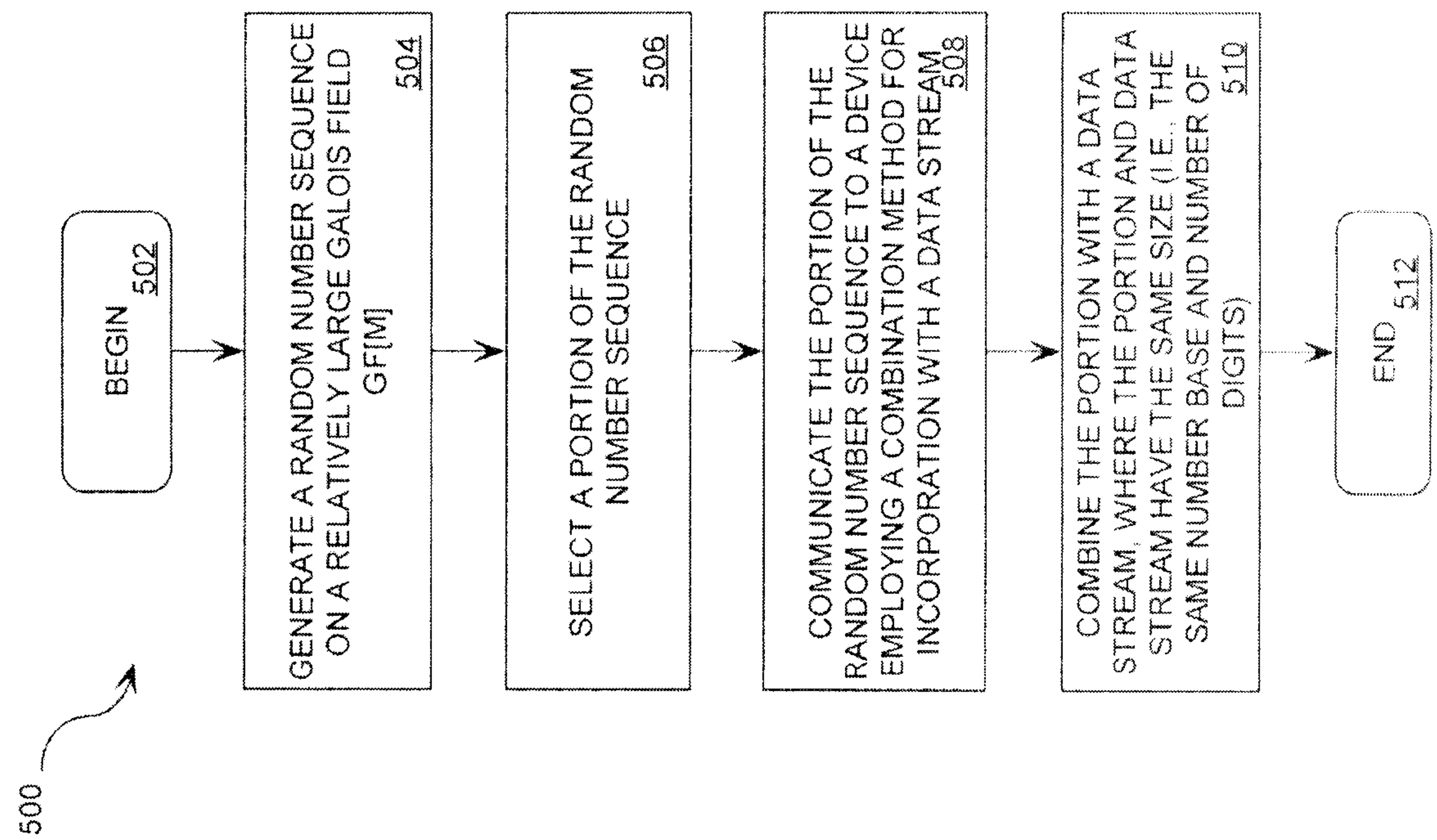

400
BEGIN 402
SELECT A FIRST NUMBER BASE AND A SECOND NUMBER BASE WHICH RESPECTIVELY DEFINE THE SIZE OF A FIRST AND SECOND FINITE FIELD 404
PUNCTURE A RING STRUCTURE DEFINED BY THE FIRST FINITE FIELD BY REMOVING AT LEAST ONE ELEMENT THEREFROM TO ELIMINATE A STATISTICAL ARTIFACT IN A RANDOM NUMBER SEQUENCE EXPRESSED IN THE SECOND NUMBER BASE 406
GENERATE A RANDOM NUMBER SEQUENCE UTILIZING THE RING STRUCTURE THAT HAS BEEN PUNCTURED, WHEREIN THE RANDOM NUMBER SEQUENCE IS EXPRESSED IN THE FIRST NUMBER BASE 408
PERFORM A MIXED RADIX CONVERSION TO CONVERT THE RANDOM NUMBER SEQUENCE FROM THE FIRST NUMBER BASE TO THE SECOND NUMBER BASE 410
END 412

FIG. 5
(PRIOR ART)



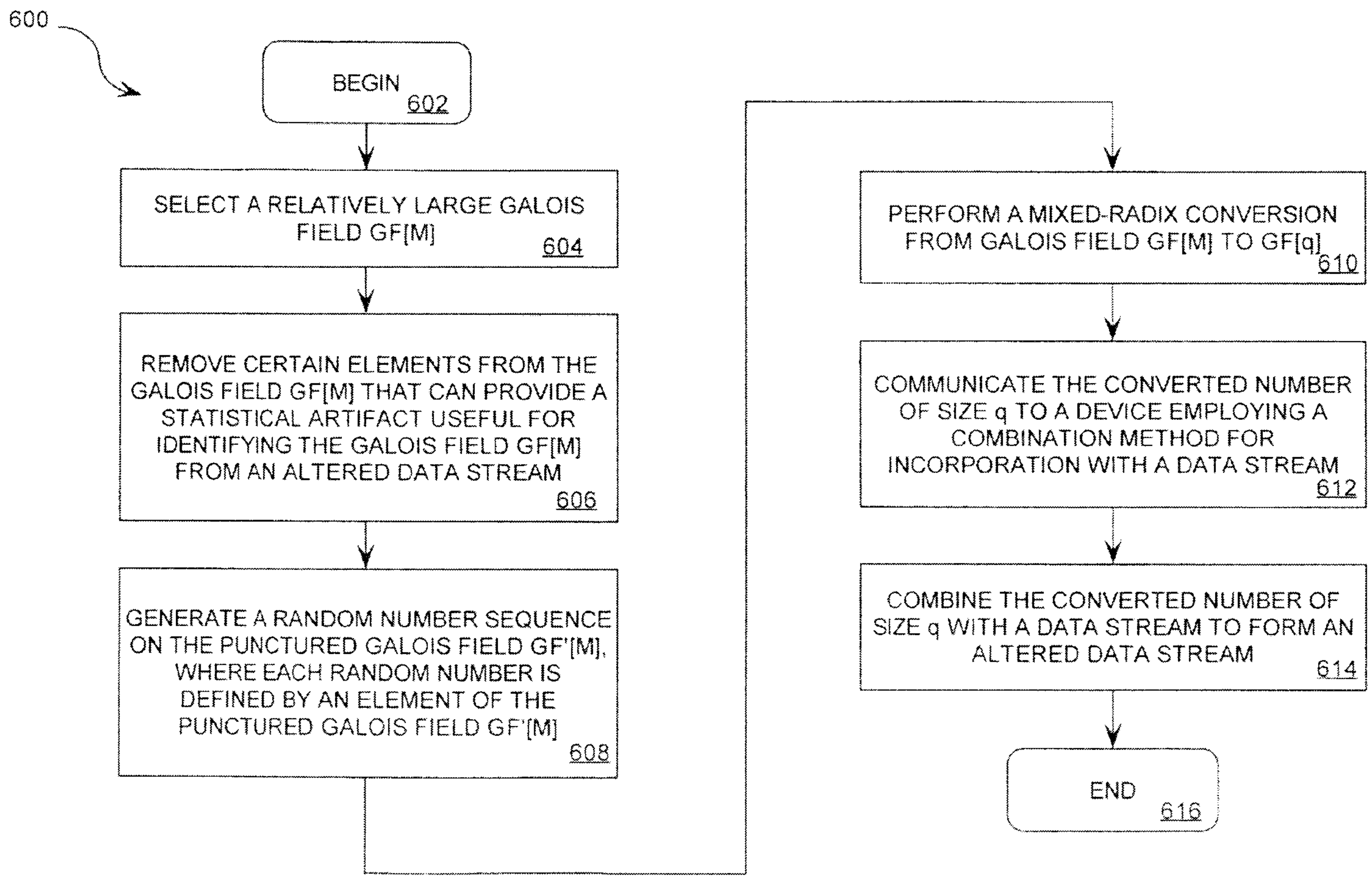

600
BEGIN
602
SELECT A RELATIVELY LARGE GALOIS FIELD GF[M]
604
REMOVE CERTAIN ELEMENTS FROM THE GALOIS FIELD GF[M] THAT CAN PROVIDE A STATISTICAL ARTIFACT USEFUL FOR IDENTIFYING THE GALOIS FIELD GF[M] FROM AN ALTERED DATA STREAM
606
GENERATE A RANDOM NUMBER SEQUENCE ON THE PUNCTURED GALOIS FIELD GF'[M], WHERE EACH RANDOM NUMBER IS DEFINED BY AN ELEMENT OF THE PUNCTURED GALOIS FIELD GF'[M]
608
PERFORM A MIXED-RADIX CONVERSION FROM GALOIS FIELD GF[M] TO GF[q]
610
COMMUNICATE THE CONVERTED NUMBER OF SIZE q TO A DEVICE EMPLOYING A COMBINATION METHOD FOR INCORPORATION WITH A DATA STREAM
612
COMBINE THE CONVERTED NUMBER OF SIZE q WITH A DATA STREAM TO FORM AN ALTERED DATA STREAM
614
END
616

FIG. 6

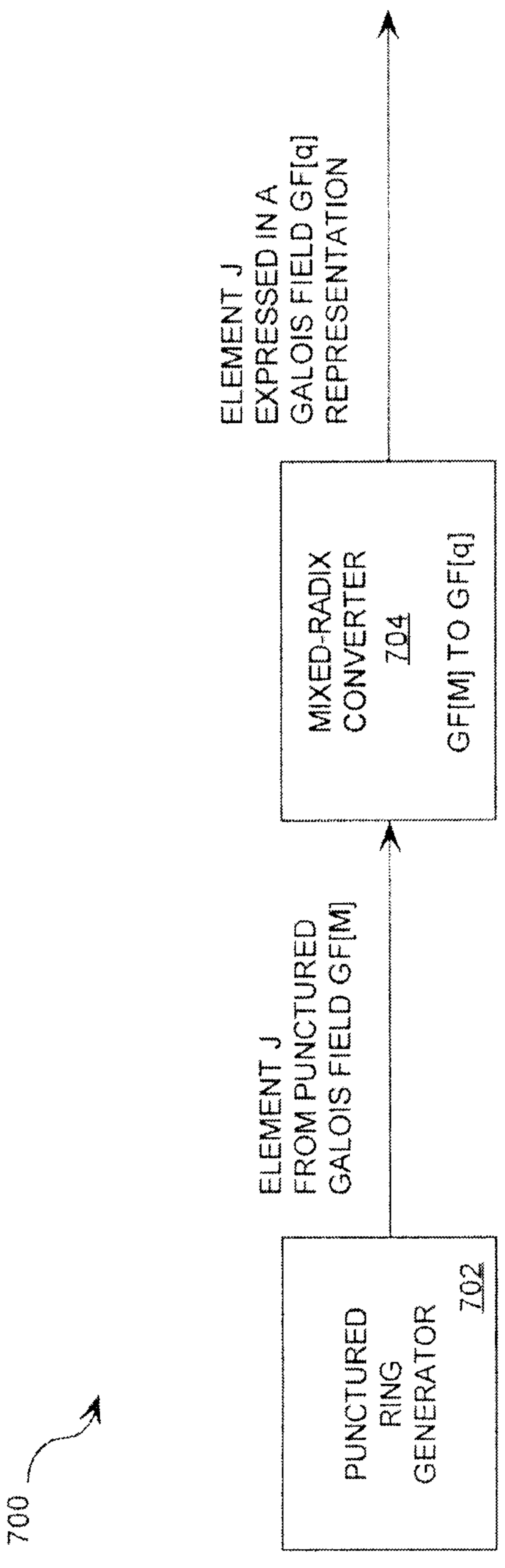
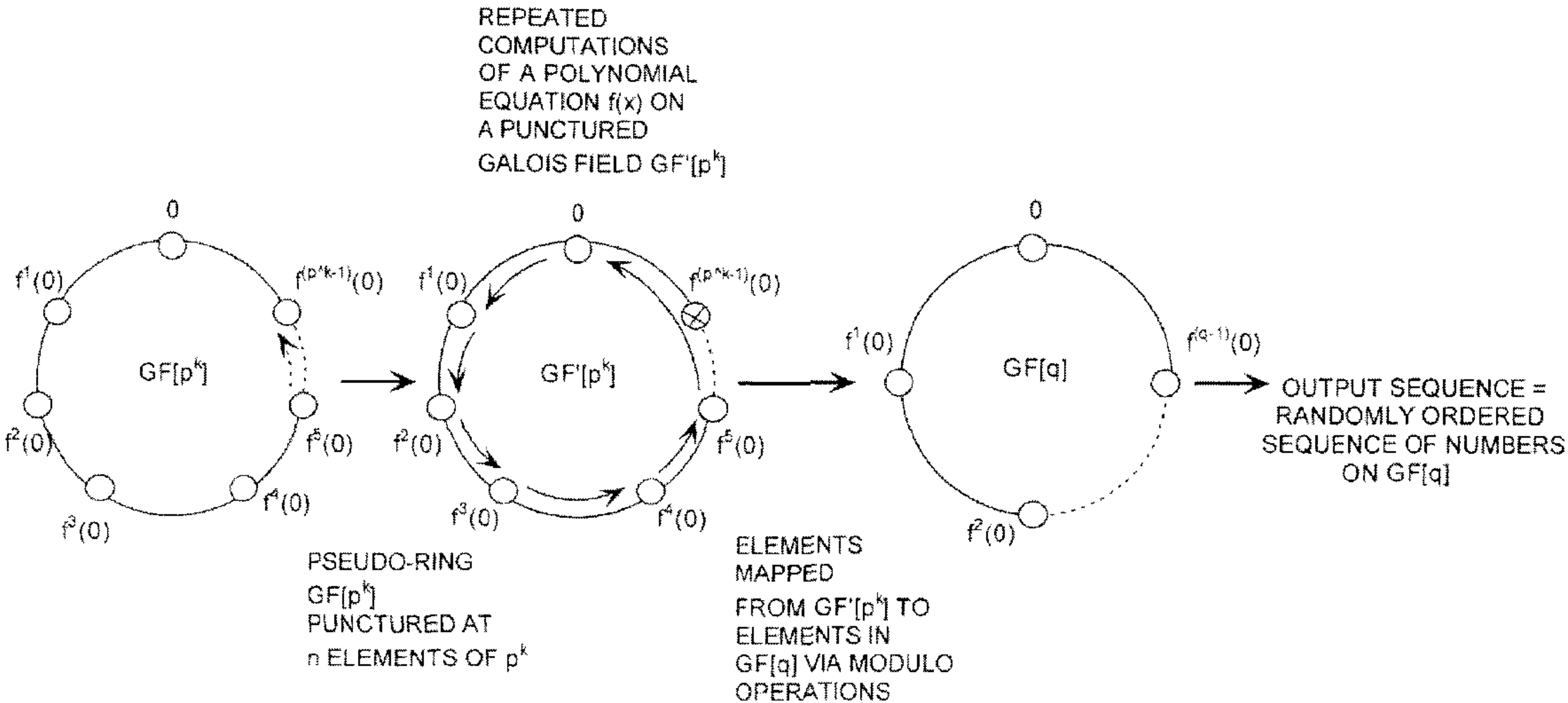

700
PUNCTURED
RING
GENERATOR
702
ELEMENT J
FROM PUNCTURED
GALOIS FIELD GF[M]
MIXED-RADIX
CONVERTER
704
GF[M] TO GF[q]
ELEMENT J
EXPRESSED IN A
GALOIS FIELD GF[q]
REPRESENTATION

FIG. 7



REPEATED COMPUTATIONS OF A POLYNOMIAL EQUATION f(x) ON A PUNCTURED GALOIS FIELD GF'[p^k]
0
f^1(0)
f^(p^k-1)(0)
GF[p^k]
f^2(0)
f^5(0)
f^3(0)
f^4(0)
0
f^1(0)
f^(p^k-1)(0)
GF'[p^k]
f^2(0)
f^5(0)
f^3(0)
f^4(0)
0
f^1(0)
f^(q-1)(0)
GF[q]
f^2(0)
OUTPUT SEQUENCE = RANDOMLY ORDERED SEQUENCE OF NUMBERS ON GF[q]
PSEUDO-RING GF[p^k] PUNCTURED AT n ELEMENTS OF p^k
ELEMENTS MAPPED FROM GF'[p^k] TO ELEMENTS IN GF[q] VIA MODULO OPERATIONS