



(51) International Patent Classification:

G06F 7/58 (2006.01) **G06F 7/72** (2006.01)
H04L 9/22 (2006.01)

(21) International Application Number:

PCT/US2009/033343

(22) International Filing Date:

6 February 2009 (06.02.2009)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

12/027,658 7 February 2008 (07.02.2008) US

(71) Applicant (for all designated States except US): **HARRIS CORPORATION** [US/US]; 1025 W. NASA Blvd., MS A-11I, Melbourne, Florida 32919 (US).

(72) Inventors: **MICHAELS, Alan J.**; 1584 Sumter Lane, West Melbourne, Florida 32904 (US). **CHESTER, David B.**; 961 Peacock Avenue NE, Palm Bay, Florida 32907 (US).

(74) Agents: **YATSKO, Michael S.** et al.; Harris Corporation, 1025 W. NASA Blvd., MS A-11I, Melbourne, Florida 32919 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

- with international search report (Art. 21(3))
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

(54) Title: RANDOM NUMBER GENERATION USING RANGE TRANSFORMATION

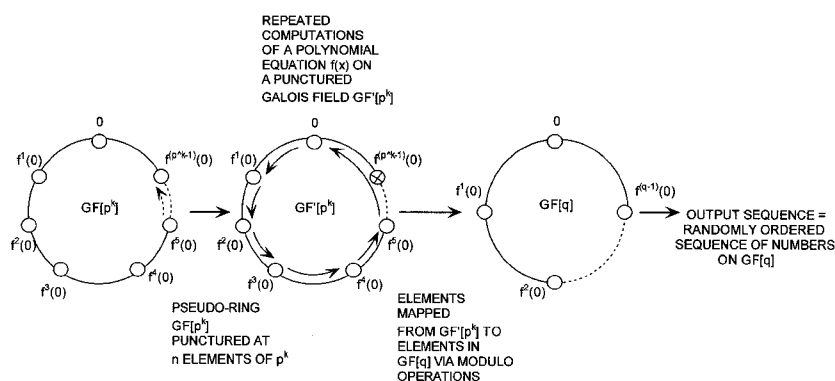


FIG. 2

(57) Abstract: A cryptographic system (CS) is provided. The CS (800) comprises a data stream receiving means (DSRM), a generator (702), a mixed radix converter (MRC) and an encryptor (908). The DSRM (902) is configured to receive a data stream (DS). The generator is configured to selectively generate a random number sequence (RNS) utilizing a punctured ring structure. The MRC (704) is coupled to the generator and configured to perform a mixed radix conversion to convert the RNS from a first number base to a second number base. The encryptor is coupled to the DSRM and MRC. The encryptor is configured to generate an altered data stream by combining the RNS in the second number base with the DS. The punctured ring structure and the MRC are configured in combination to produce an RNS in the second number base which contains a priori defined statistical artifacts after the mixed radix conversion.

RANDOM NUMBER GENERATION USING RANGE TRANSFORMATION

5 The inventive arrangements relate to cryptographic systems having ring generators. More particularly, the inventive arrangements relate to a cryptographic system comprising a ring generator configured for performing a mixed radix conversion absent of unwanted statistical artifacts.

 Many number theoretic based computational systems include ring generators.
10 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
15 field GF[M] is a field that contains only a finite number of elements $\{0, 1, 2, \dots, M-1\}$. 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
20 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
25 of an output sequence and in many applications it is desirable to mask this information. Such applications include, but are not limited to, a cryptographic application.

 In view of the foregoing, there remains a need for a ring generator implementing an arithmetic operation that is computationally efficient in a digital
30 (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 for use in a cryptographic system.

The invention concerns a cryptographic system. The cryptographic system is comprised of a data stream receiving means, a generator, a mixed radix converter and an encryptor. The data stream receiving means is configured to receive an input data stream. The generator is configured to selectively generate a random number sequence utilizing a ring structure which has been punctured. The mixed radix converter is coupled to the generator and 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. The encryptor is coupled to the data stream receiving means and the mixed radix converter. The encryptor is configured to generate a modified data stream by incorporating or combining the random number sequence in the second number base with the input data stream.

According to an aspect of the invention, the first number base is defined by a first Galois field characteristic 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.

5 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.

 According to another aspect of the invention, the ring structure has m
10 element(s) removed therefrom to induce a chosen non-uniform statistical artifact when expressed in a second number base. M is determined based on the characteristics of the two number bases and the mechanics of a combining method. The specific value of M is application dependent.

 According to another aspect of the invention, the encryptor includes at least
15 one of a multiplier, an adder, a digital logic device and a feedback mechanism. In this regard, it should be appreciated that the encryptor is configured to perform a combination method for masking the input data stream. The combination method includes at least one of a standard multiplication operation, a multiplication in a Galois extension field operation, an addition modulo q operation, a subtraction
20 modulo q operation and a bitwise logic operation.

 According to another aspect of the invention, the cryptographic system is further comprised of a truncation device and/or a size converter. The truncation device is coupled to the mixed radix converter. The truncation device is configured to select a truncated portion of the random number sequence in the second number base.
25 The size converter is coupled between the truncation device and the encryptor. The size converter is configured to convert the truncated portion from a size $GF[M]$ to a size n if the input data stream is of a size $GF[n]$ or $GF[n/d]$, where d is an even divisor of n . The input data stream is expressed in the second number base.

 According to yet another aspect of the invention, the cryptographic system is
30 comprised of a modified data stream receiving means. The modified data receiving

means is configured to receive the modified data stream. The cryptographic system is also comprised of a second ring structure and a second mixed radix converter. The second ring structure and a second mixed radix converter are configured in combination to produce a decryption sequence. The cryptographic system is further
5 comprised of a decryptor. The decryptor is electronically connected to the modified data stream receiving means and the second mixed radix converter. The decryptor is configured to generate decrypted data by performing a decryption method utilizing the modified data stream and decryption sequence.

Embodiments will be described with reference to the following drawing
10 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
15 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.

20 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.

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

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

FIG. 8 is a block diagram of a cryptographic system that is useful for understanding the invention.

FIG. 9 is a block diagram of the encryption device of FIG. 8 that is useful for understanding the invention.

FIG. 10 is a block diagram of the decryption device of FIG. 8 that is useful for understanding the invention.

5 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 value or 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]
10 base is converted to a number sequence expressed in a Galois field GF[3] base.

In cryptographic 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
15 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 $\{0, 1, 2, \dots, p-1\}$. 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 cyclic
20 Galois field GF[p] operation must 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[$p_1^{k_1}$] base
25 to a second Galois field GF[$p_2^{k_2}$] 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 $\{0, 1, 2, \dots, 6\}$. Similarly, the number sequence expressed in a Galois field
30 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 $\{0, 1, 2, \dots, 6\}$ 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
- 5 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

- 10 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
- 15 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 system implementing the conventional mixed radix conversion algorithm (described above in
- 20 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
5 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 $GF[2^k]$. As used herein, the term “puncturing” means discarding one or more elements in a Galois field $GF[2^k]$ that
10 exceed an integer multiple of a desired range characteristic. The “puncturing” is performed to maintain a perfectly uniform distribution over a desired number base. Alternatively, the puncturing is performed to induce specific non-uniformities in the statistical output distribution. 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
15 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 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
20 cryptographic system. All arithmetic of the initial sequence generation process is performed in the first number base prior to puncturing.

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
25 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 structure 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 $\{0, 1, 2, \dots, p^k-1\}$. 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 $GF[q]$. 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 $GF[q]$ can be defined by a mathematical Equation (1).

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

where NOC is the number of cycles in a punctured Galois field $GF[p^k - n]$. $p^k - n$ 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 $GF[q]$ 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 $GF[5]$ 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
 5 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 $GF'[10]$ (which is isomorphic to $GF[9]$). As such, the resulting sequence
 10 is defined by the elements $\{0, 1, 2, \dots, 8\}$. 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.

15 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 $\{0, 1, 2, \dots, 6\}$. The elements of the Galois field $GF[7]$ are mapped to elements in a Galois
 20 field $GF[3]$. In order to guarantee a uniform distribution over a structure 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
 25 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] is defined by the previously discussed mathematical Equation (1), repeated below.

$$\text{NOC} = (p^k - n) / q$$

- 5 where NOC is the number of cycles in the Galois field GF[3]. 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

10

- 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).

15

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

20

contains only a finite number of elements $\{0, 1, 2, \dots, 232\}$. 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] 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].

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

$$\text{NOC} = p_1/p_2 \quad (2)$$

where NOC is the number of cycles in the Galois field GF[5]. p_1 is a positive integer number defining a finite field size of a first punctured 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] can be computed as follows: $\text{NOC} = (233^1 - 13)/5 = 44$. Accordingly, there are forty four (44) complete cycles through the Galois field GF[5].

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
5 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
10 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
15 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
20 to eliminate or intentionally induce 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
25 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 computed and 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 a chosen 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 $\{0, 1, 2, \dots, M-1\}$. 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 $GF[M]$, where M is a large multiplicative compilation of mutually prime numbers. If the random number sequence contains five hundred (500) independent p-adic digits and a portion of the random number sequence is selected to include only sixteen (16) of the five hundred (500) digits to alter a data stream, then 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 cryptographic 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 cryptographic 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 cryptographic system
5 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
10 the same is defined by a set of complete cycles in a Galois field $GF[q]$. 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 cryptographic system implementing method 600 by making the deterministic rule defining the output sequence dependant on a non-advertised mutually prime number
15 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 $GF'[M]$.

20 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
25 degree of security to a cryptographic 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
30 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
5 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
10 increasing a security of a cryptographic 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 sequence generation circuit
15 (SGC) 700 that is useful for understanding the invention. As shown in FIG. 7, the SGC 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 undesired statistical
20 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
25 sequence utilizing a ring structure which has been punctured. The ring structure can be a punctured Galois field $GF'[M]$. 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).

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

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 or intentionally induced 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.

5 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 the desired number of elements after the mixed radix conversion.

10 Referring now to FIG. 8, there is illustrated one embodiment of a cryptographic system 800 which could be used to implement the inventive arrangements. Notably, the cryptographic system 800 has an increased security feature as compared to conventional cryptographic systems. In this regard, it should be understood that the cryptographic system 800 includes a means to encrypt a data
15 stream utilizing a random number sequence which is exclusive of any statistical artifacts associated with a mixed radix conversion. In effect, reverse engineering of mathematical patterns present in an encrypted data stream generated by the cryptographic system 800 is more difficult than mathematical patterns present in an encrypted data stream generated by a conventional cryptographic system.

20 Referring again to FIG. 8, the cryptographic system 800 is comprised of a data stream source 802, an encryption device 804 and a decryption device 806. The data stream source 802 can be comprised of hardware and/or software configured to generate a data stream. The data stream can include payload data, such as voice data, video data, user identification data, signature data and/or the like. The data stream
25 can also be a digital data stream. The data stream source 802 is also comprised of hardware and/or software configured to communicate the data stream to the encryption device 804.

 The encryption device 804 is comprised of hardware and/or software configured to generate an encryption sequence. The encryption sequence is a random
30 number sequence which is exclusive of any statistical artifacts associated with a

mixed radix conversion. The encryption device 804 is also comprised of hardware and/or software configured to perform actions to encrypt (or modify) the data stream using the encryption sequence. The encryption device 804 is further comprised of hardware and/or software configured to communicate a modified data stream to the decryption device 806. The encryption device 804 will be described in greater detail below in relation to FIG. 9.

The decryption device 806 is comprised of hardware and/or software configured to generate a decryption sequence. The decryption sequence is a random number sequence expressed in a second number base which is exclusive of any statistical artifacts associated with a mixed radix conversion. The decryption sequence can be the same as the encryption sequence generated by the encryption device 804 or may be different based on the combining method. The decryption device 806 is also comprised of hardware and/or software configured to perform actions to decrypt the received modified data stream. Such decryption actions are well known to persons skilled in the art, and therefore will not be described in great detail herein. The decryption device 806 is also comprised of hardware and/or software configured to communicate the decrypted data to an external device (not shown). The decryption device 806 will be described in greater detail below in relation to FIG. 10.

Referring now to FIG. 9, there is provided a block diagram of the encryption device 802 of FIG. 8. As shown in FIG. 9, the encryption device 802 is comprised of a data stream receiving means (DSRM) 902, a sequence generation circuit (SGC) 700, an optional truncation device 904, an optional size converter 906 and an encryptor 908. Each of the components 902, 904, 906, 908 is well known to persons skilled in the art, and therefore will not be described in great detail herein. However, a brief discussion of the encryption device 802 is provided to assist a reader in understanding the present invention.

Referring again to FIG. 9, the DSRM 902 is configured to receive an input data stream. The DSRM is also configured to communicate the input data stream to the encryptor 908. The SGC 700 is generally configured to generate an encryption

sequence. The encryption sequence is a random number sequence which is exclusive of any statistical artifacts associated with a mixed radix conversion. In this regard, it should be appreciated that the SGC 700 is comprised of a punctured ring generator 702 and a mixed-radix converter 704. The discussion provided above in relation to
5 FIG. 7 is sufficient for understanding the SGC 700.

The SGC 700 is electronically coupled to the optional truncation device 904. However, it should be appreciated that the SGC 700 can alternatively be directly coupled to the encryptor 908. The optional truncation device 904 is configured to select a truncated portion of the encryption sequence generated by the SGC 700. The
10 phrase “truncated portion” as used herein refers to the random numbers that remain after selected random numbers are removed from a random number sequence. The optional truncation device 904 is electronically coupled to the optional size converter 906. The optional size converter 906 is configured to convert the portion of the encryption sequence from a size $GF[M]$ to a size n if the input data stream is of a size
15 $GF[n]$ or $GF[n/d]$, where d is an even divisor of n . The optional size converter 906 is electronically coupled to the encryptor 908.

The encryptor 908 is configured to generate a modified data stream by incorporating or combining the encryption sequence with the input data stream. More particularly, the encryptor 908 is configured to perform a combination method for
20 masking a data stream. The combination method may be a standard multiplication, multiplication within 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 appreciated that the encryptor 908 can include a multiplier, an adder, a digital logic device, a feedback mechanism or a similar combining function device.

25 A person skilled in the art will appreciate that the encryption device 804 illustrates an exemplary architecture of an encryption device implementing the present invention. However, the invention is not limited in this regard and any other encryption device architecture can be used without limitation.

Referring now to FIG. 10, there is illustrated one embodiment of the
30 decryption device 806 of FIG. 8. The decryption device 806 is comprised of a

modified data stream receiving means (MDSRM) 1002, a sequence generation circuit (SGC) 700 and a decryptor 1004. Each of the listed components 1002, 1004 is well known to persons skilled in the art, and therefore will not be described in great detail herein. However, a brief description of the decryption device 806 is provided to assist
5 a reader in understanding the present invention.

Referring again to FIG. 10, the MDSRM 1002 is comprised of hardware and/or software configured to receive a modified data stream from an external device, such as the encryption device 804 (described above in relation to FIG. 8). The MDSRM 1002 is also comprised of hardware and/or software configured to
10 communicate the modified data stream to the decryptor 1004. In this regard, it should be appreciated that the modified data stream receiving means 1002 is electronically connected to the decryptor 1004.

The SGC 700 is generally configured to generate a decryption sequence. The decryption sequence is a random number sequence which is exclusive of any
15 statistical artifacts associated with a mixed radix conversion. In this regard, it should be appreciated that the SGC 700 is comprised of a punctured ring generator 702 and a mixed-radix converter. The discussion provided above in relation to FIG. 7 is sufficient for understanding the SGC 700. The SGC 700 is electronically coupled to the decryptor 1004.

20 The decryptor 1004 is configured to generate decrypted data by performing a decryption method utilizing the modified data stream and the decryption sequence. Decryption methods are well known to persons skilled in the art, and therefore will not be described in great detail herein.

A person skilled in the art will appreciate that the decryption device 806
25 illustrates an exemplary architecture of a decryption device implementing the present invention. However, the invention is not limited in this regard and any other decryption device architecture can be used without limitation.

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
30 hardware and software. A method of puncturing the output elements of a ring

generator 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
5 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.

10 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
15 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 cryptographic system, comprising:
 - a data stream receiving means configured for receiving an input data stream;
 - 5 a generator configured for selectively generating a random number sequence utilizing a ring structure which has been punctured;
 - a mixed radix converter coupled to said generator and configured for performing a mixed radix conversion to convert said random number sequence from a first number base to a second number base;
 - 10 an encryptor coupled to said data stream receiving means and said mixed radix converter, said encryptor configured for generating an modified data stream by combining said random number sequence in said second number base with said input data stream; and
 - wherein said ring structure which has been punctured and said mixed radix
 - 15 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.
2. The cryptographic system according to claim 1, wherein said first number base
- 20 and said second number base are respectively defined by a first Galois field characteristic and a second Galois field characteristic.
3. The cryptographic system according to claim 2, wherein said first Galois field characteristic is mutually prime with respect to said second Galois field characteristic.
- 25 4. The cryptographic system according to claim 2, 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.

5. The cryptographic system according to claim 4, wherein said ring structure which has been punctured comprised n element(s) which have been 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
- 5 mathematical relation between a number of elements in said first Galois field and a number of elements in a second Galois field.
6. The cryptographic system according to claim 5, wherein n is determined based on a remainder value resulting from a quotient of said number of elements in said first
- 10 Galois field divided by said number of elements in said second Galois field.
7. The cryptographic system according to claim 6, wherein said mixed radix conversion produces a plurality of equivalence classes in said second number base, and said n elements which have been removed from said ring structure are selected to
- 15 ensure that each equivalence class has an equal or desired number of elements after said mixed radix conversion.
8. The cryptographic system according to claim 1, wherein said encryptor
- 20 includes at least one of a multiplier, an adder, a digital logic device and a feedback mechanism.
9. The cryptographic system according to claim 1, wherein said input data stream is expressed in said second number base.
- 25 10. The cryptographic system according to claim 1, wherein chosen statistical artifacts with a priori defined statistical distributions are induced into said random number sequence expressed in said second number base.

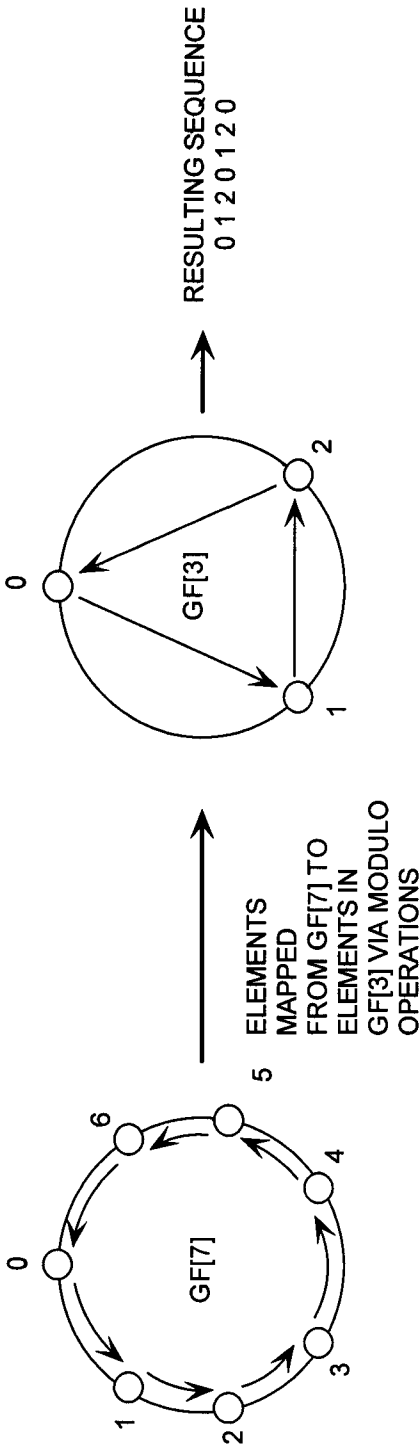


FIG. 1
(PRIOR ART)

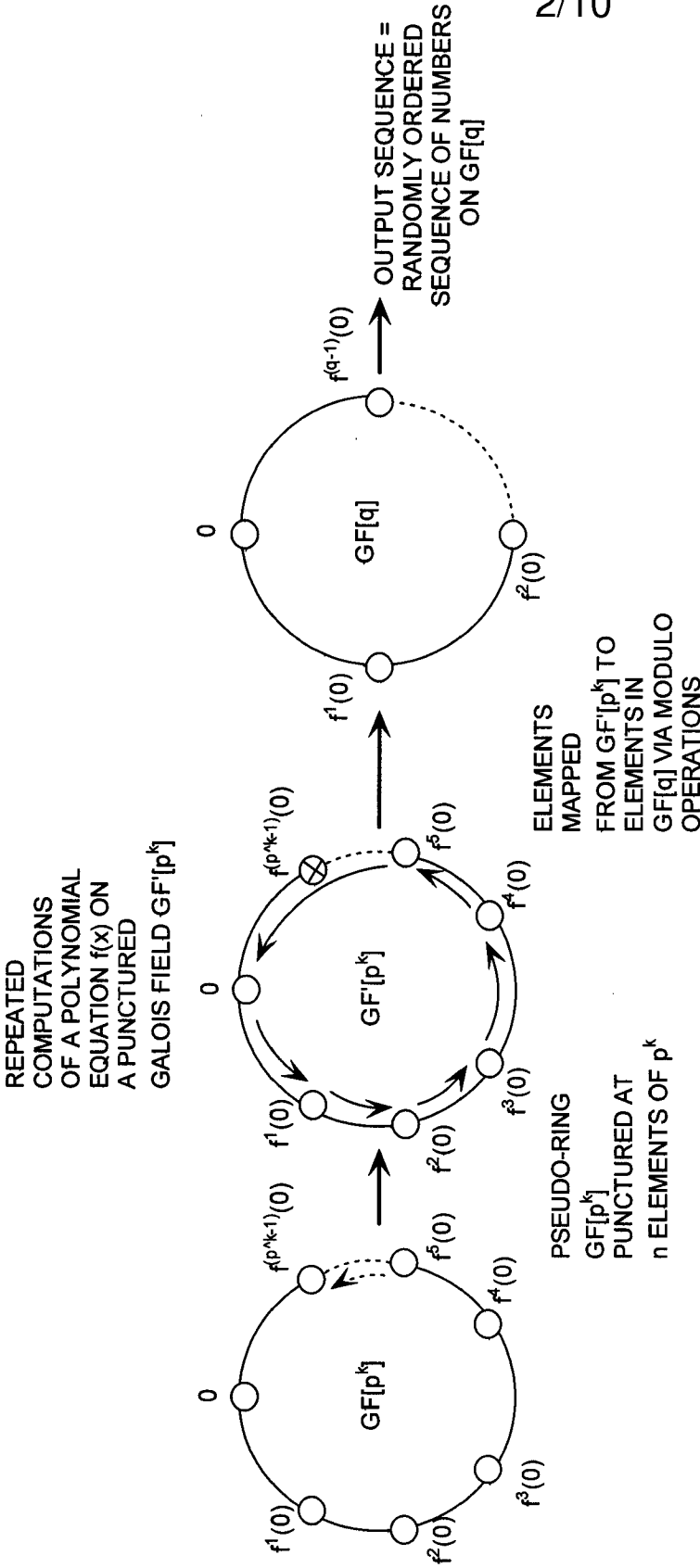


FIG. 2

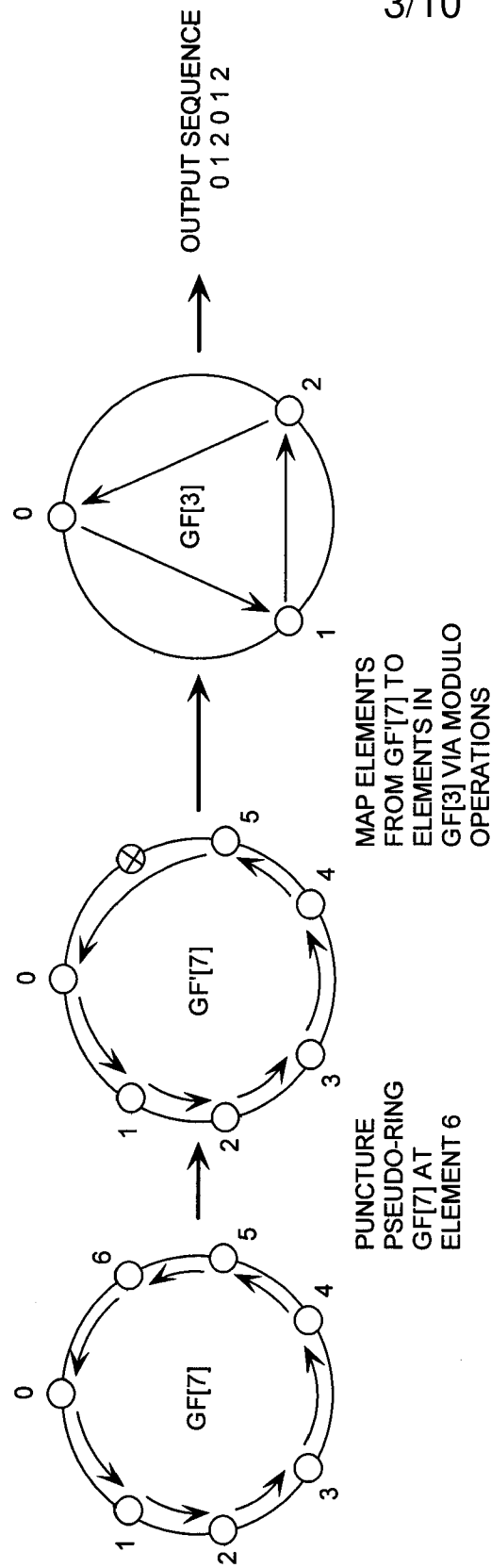


FIG. 3

FIG. 4

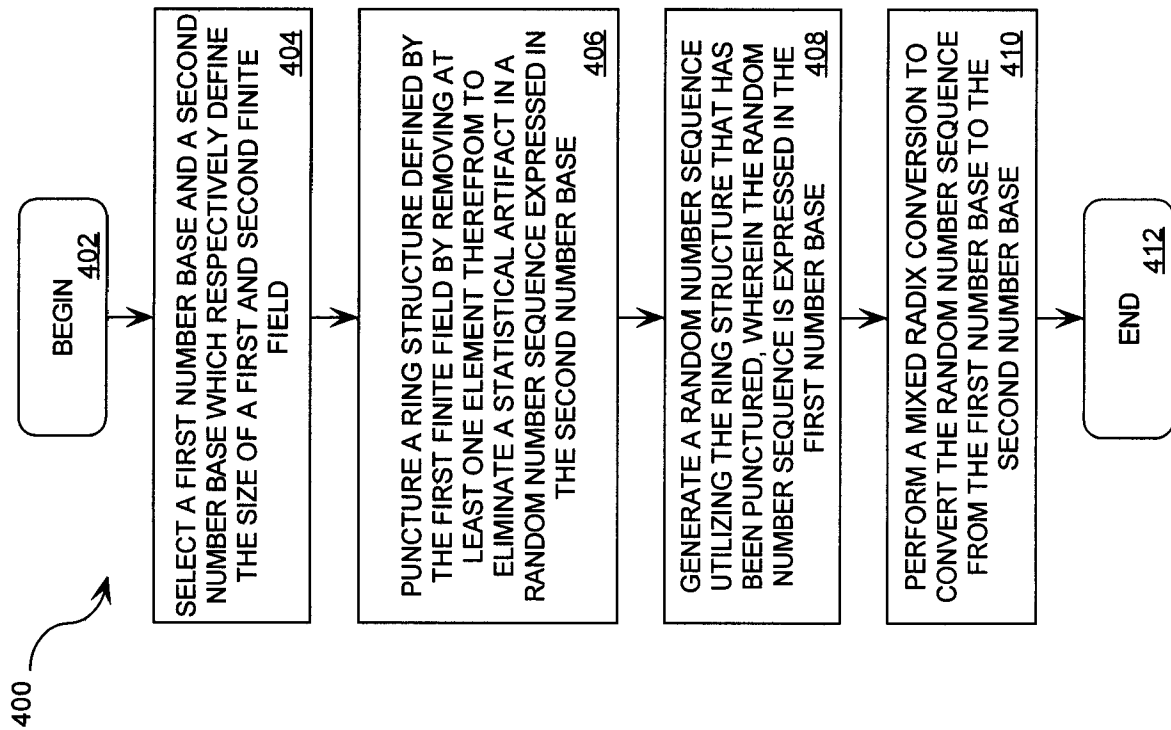
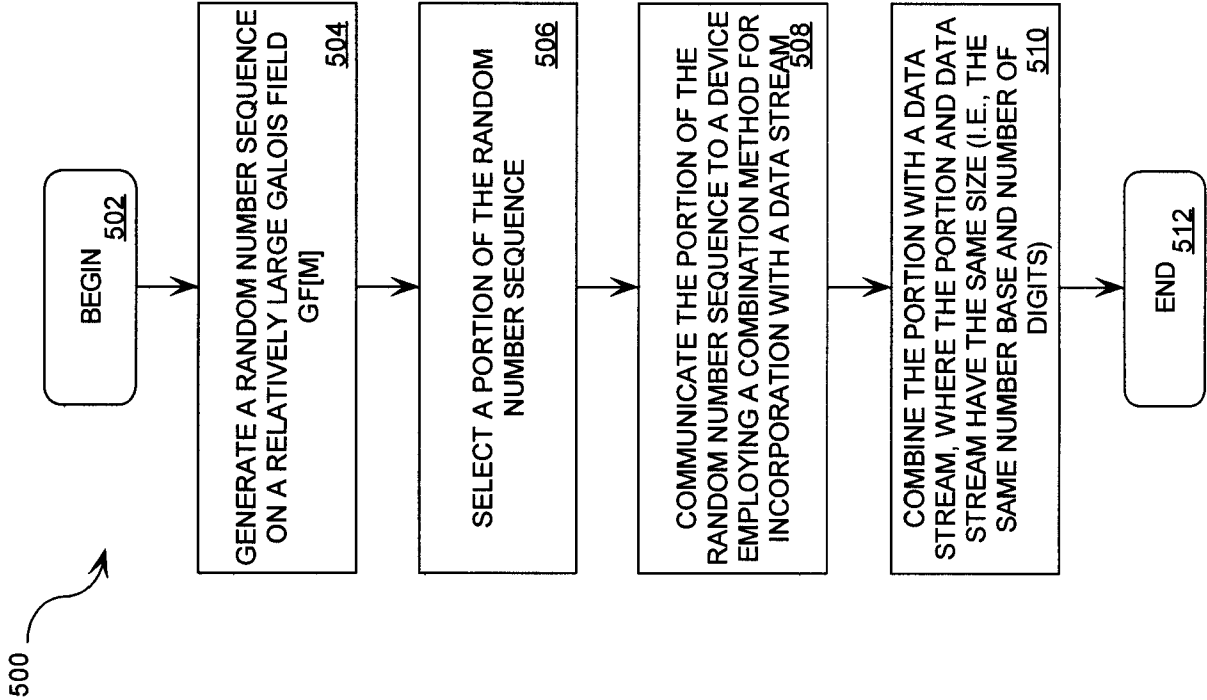


FIG. 5
(PRIOR ART)



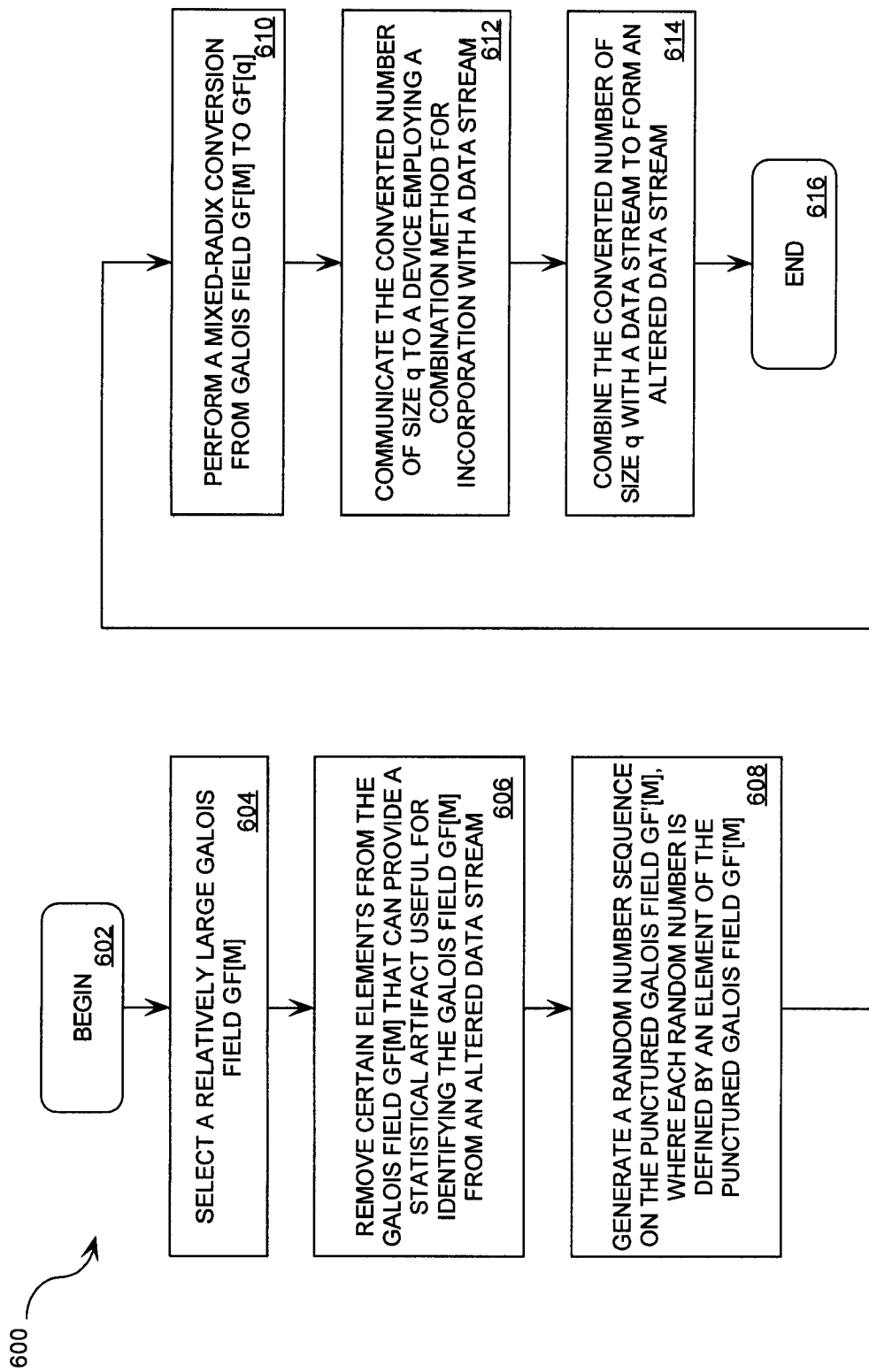


FIG. 6

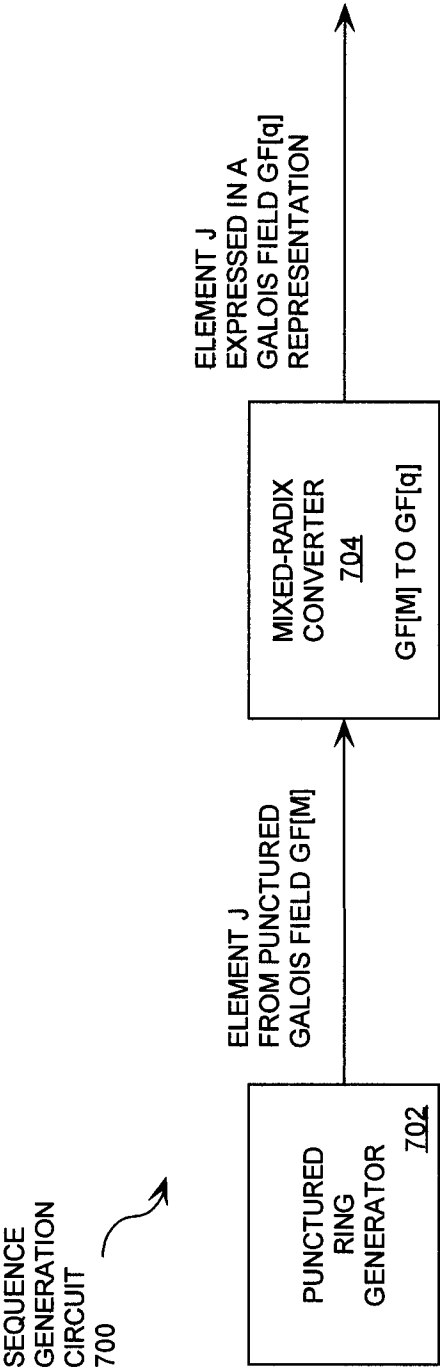


FIG. 7

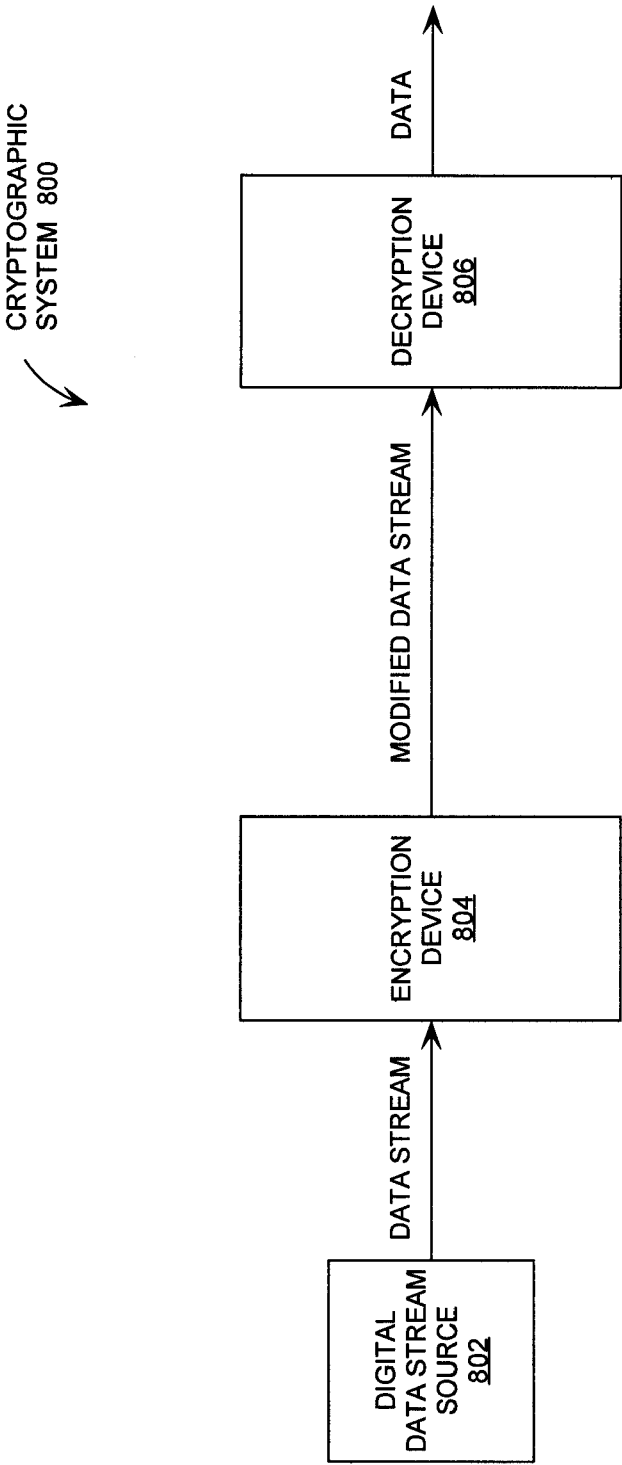


FIG. 8

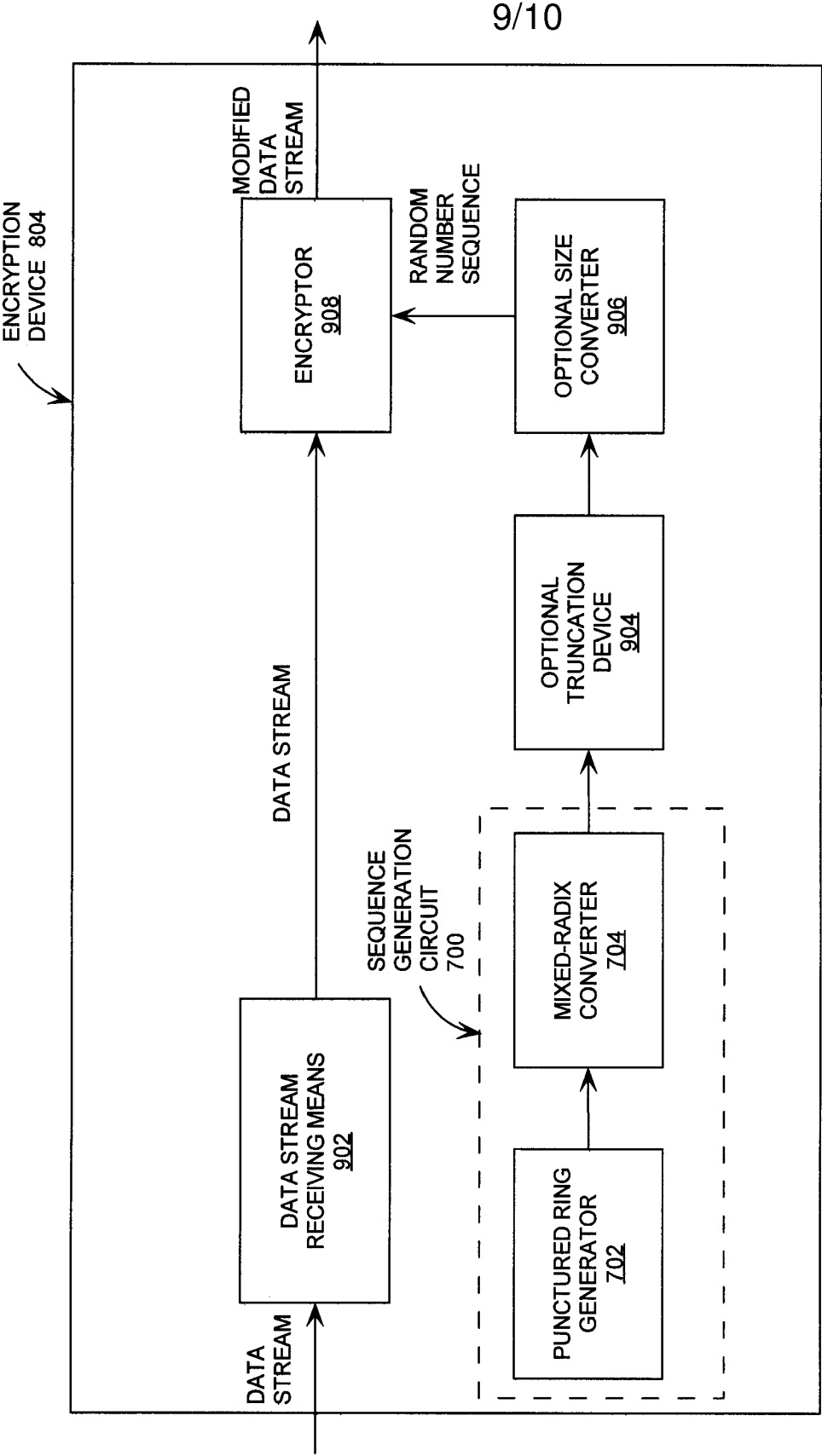


FIG. 9

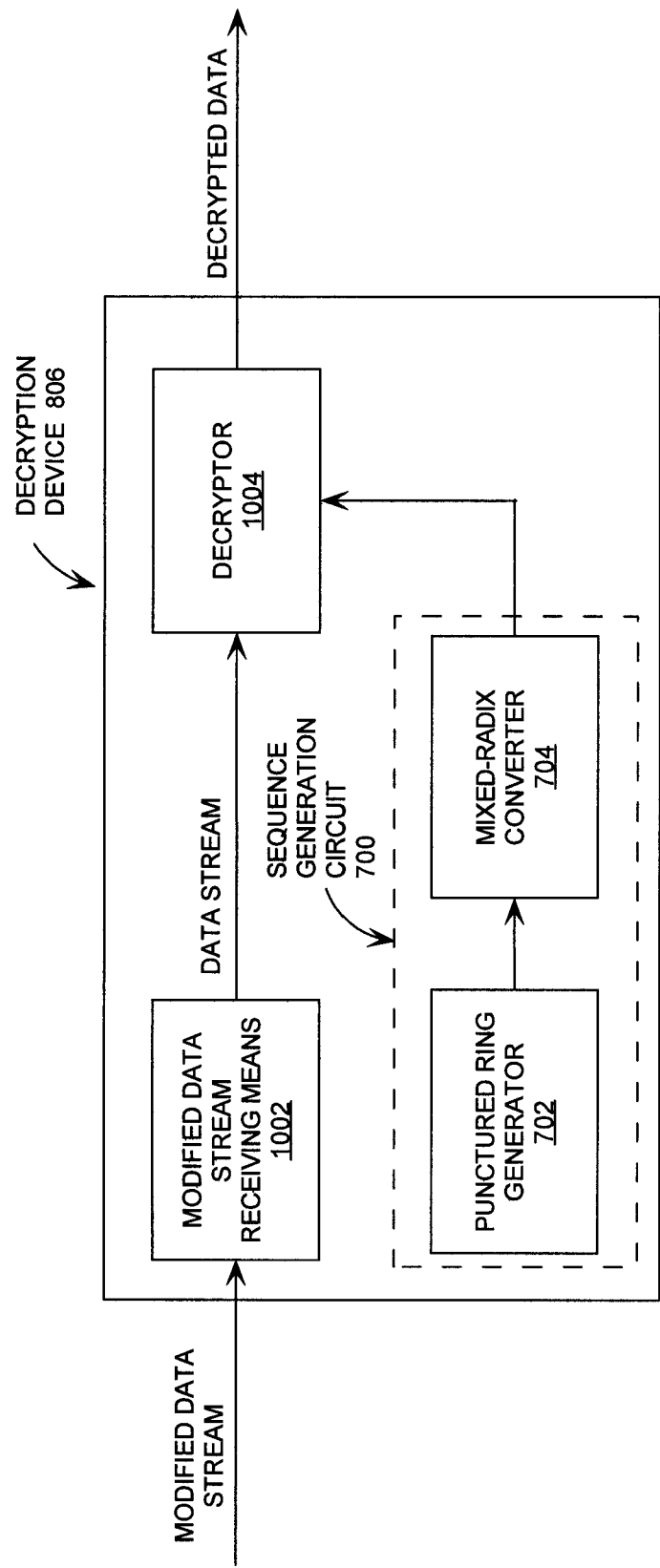


FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2009/033343

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F7/58 H04L9/22
ADD. G06F7/72

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2006/251250 A1 (RUGGIERO DAVIDE [IT] ET AL) 9 November 2006 (2006-11-09) abstract page 6, paragraph 92 - paragraph 101 figure 4	1-10
Y	US 2005/050121 A1 (KLEIN UDO [DE] ET AL) 3 March 2005 (2005-03-03) abstract page 1, paragraph 2 page 1, paragraph 4 - paragraph 9 page 2, paragraph 19 - page 3, paragraph 24 claim 12 figures 1-3	1-10

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *G* document member of the same patent family

Date of the actual completion of the international search

8 June 2009

Date of mailing of the international search report

26/06/2009

Name and mailing address of the ISA/
European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Post, Katharina

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2009/033343

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2005/207574 A1 (PITZ JEANNE K [US] ET AL PITZ JEANNE KRAYER [US] ET AL) 22 September 2005 (2005-09-22) abstract page 1, paragraph 2 - paragraph 7 page 2, paragraph 23 - page 3, paragraph 31 figures 1,7	1-10
P,X	EP 2 000 902 A (HARRIS CORP [US]) 10 December 2008 (2008-12-10) the whole document	1-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2009/033343

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006251250 A1	09-11-2006	NONE	
US 2005050121 A1	03-03-2005	US 2005050122 A1	03-03-2005
US 2005207574 A1	22-09-2005	NONE	
EP 2000902 A	10-12-2008	CA 2633858 A1	07-12-2008
		JP 2008304916 A	18-12-2008
		US 2008307022 A1	11-12-2008