(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 November 2001 (08.11.2001)

PCT

(10) International Publication Number
WO 01/84767 A1

(51) International Patent Classification⁷: H04L 9/00, 9/32, 17/02

(21) International Application Number: PCT/US01/13504

(22) International Filing Date: 26 April 2001 (26.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/562,336 1 May 2000 (01.05.2000) US

(71) Applicant: **XTEC, INCORPORATED** [US/US]; 5775 Blue Lagoon Drive, Miami, FL 33126 (US).

(72) Inventors: **FERNANDEZ, Alberto, J.**; 16005 S.W. 109th Street, Miami, FL 33196 (US). **BORMEY, Carlos, D.**; 1319 S.W. 141st Avenue, Miami, FL 33184 (US). **NEGRIN, Ismael, E.**; 5678 S.W. 130th Avenue, Miami, FL 33183 (US).

(74) Agent: **PRIEST, Peter, H.**; Priest & Goldstein, PLLC, 529 Dogwood Drive, Chapel Hill, NC 27516 (US).

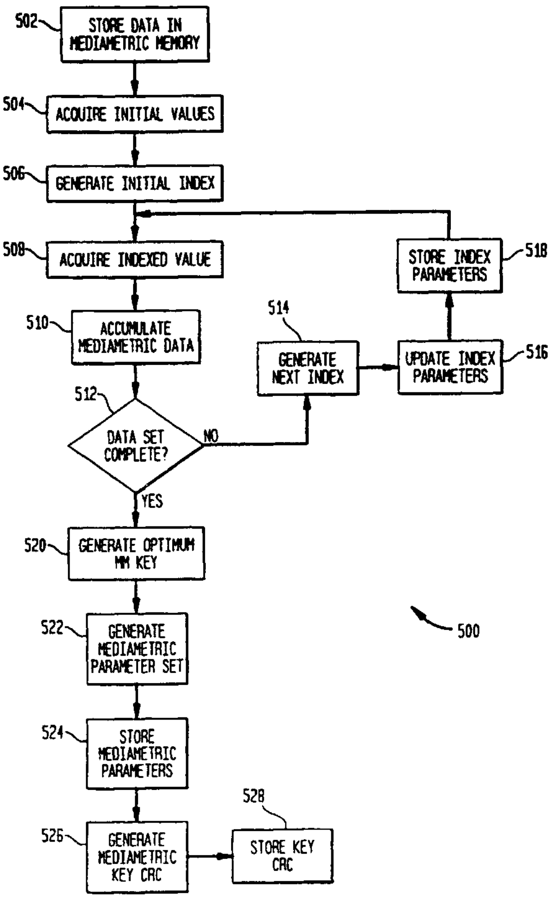
(81) Designated States *(national)*: AU, CA, JP, KR.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHODS AND APPARATUS FOR MEDIAMETRIC DATA CRYPTOPROCESSING



(57) **Abstract:** A data storage device having mediametric properties used as a source of data for keys used in cryptoprocessing. The device may suitably include a memory array such as an EPROM or EEPROM comprising a plurality of memory cells, each cell containing a level of trapped charges. The levels of trapped charges are difficult or impossible to set to a predefined value, but may be read precisely once they are established. Moreover, the levels of cells are difficult or impossible to read unless provisions are made to allow them to be read. These factors establish the levels of trapped charges as secure and unpredictable sources of data. When it is desired to generate cryptoprocessing keys, the levels of trapped charges are read from selected cells (510), and may suitably be converted to numerical data for convenience in processing. The data thus retrieved is used to produce cryptoprocessing keys (520), which are then used for cryptoprocessing of data. The exact levels of charges in a memory array such as an EPROM or EEPROM is random, making this data suitable for easy and convenient generation of random numbers. When a random number is desired, data is written to selected cells of the memory array in order to establish random charge levels in the cells. The data is then retrieved from the selected cells and processed in order to yield a random number.

METHODS AND APPARATUS FOR MEDIAMETRIC DATA CRYPTOPROCESSING

Field of the Invention

The present invention relates generally to improvements to cryptoprocessing of information. More particularly, the invention relates to using physical properties of the media used to record the information as a source of data for use in the generation of encryption keys.

Background of the Invention

Storage of financial and other information in solid-state devices such as smart cards is growing more and more prevalent. Large quantities of data representing customer or merchant information, transaction histories, or stored value may be placed on a card and given to the customer. The information may be completely self-contained on the card, allowing the information to be read directly from the card. This approach is different from the use of magnetic cards, which typically contain only an account number or other identifying information, which is used as an index to retrieve the customer information from a database. A smart card typically stores data in solid-state memory such as an EPROM or EEPROM. The card is placed in a card writer which provides information to the card in a numerical format and transfers the information through ports provided on the card. The card includes a microcomputer, which receives the information from the reader, processes the information, and stores the information in the memory. Similarly, whenever it is desired to use the information stored on the card, the microcomputer retrieves the information from memory, processes the information, and transfers the information through the ports to an external device such as a card reader. Because high-capacity memory devices are widely available, it is possible to store large quantities of data on such a card, making it versatile and convenient.

After information is written to the smart card, it can be given to a customer so that the customer can present the card for reading and writing of data as needed. For example, a cash card may be loaded with information representing cash credits. The card is given to the customer and presented to a merchant or bank whenever a debit is to be made. Upon presentation of the card, the merchant or bank places the card in a reader/writer, reads the balance on the card, makes an appropriate subtraction, and writes the new balance to the card. The debit can be made without a need to retrieve any information other than the information on the card itself.

If a smart card is to be given to a customer, security is vital. A customer in possession of a smart card has long-term, unsupervised access to the card, and has the opportunity to attack the card at leisure in order to attempt to store unauthorized information on the card or to recover secret information from the card. It is possible for a skilled attacker to retrieve numerical information from a smart card through probing of the internal components of the device, or through other unauthorized means. If card security is provided only through numerical means, such as numerical authenticators or cryptoprocessing keys, it is possible to retrieve the information from the card and to obtain information intended to be secret, or to create a counterfeit card which contains information duplicated from a legitimate card.

Mediametric techniques offer considerable advantages in providing data security. These mediametric techniques provide security through the use of data related to physical characteristics of the storage media. Solid state media possess characteristics which are impossible to duplicate precisely, but which can be precisely measured. These include, for example, variations in the remnant charge of EEPROM's, or variations in Row/Column addressing circuits. These and other characteristics have been used for authentication. A numerical representation, or fingerprint, of authenticating characteristics is created and stored. When the card is presented, the authenticating characteristics are measured, and a fingerprint is created and compared against the original fingerprint. Such techniques are described in detail in Fernandez U.S. Patent No. 5,644,636, which is assigned to the assignee of the present invention and incorporated in its entirety herein by reference.

One advantage of such mediametric techniques is that some solid-state devices possess characteristics which will be altered by any tampering with the device. This may be true even when tampering with the device will succeed in revealing the numerical data stored in the device.

For example, it is possible to disassemble an EPROM or EEPROM memory and determine the numerical contents of memory cells through the use of a probe. However, it is not possible to read the precise levels of charges through such probing, as the use of the probe will alter the levels of the charges. It is possible for a memory to supply charge level data if suitable ports are supplied for the purpose, but if no external access to the ports is given, determination of the charge levels is difficult or impossible.

In systems of the prior art, mediametric techniques have been used for authentication and not to secure secret data. A prior-art mediametric card can be made secure against counterfeiting. For example, after a card is to be programmed with data, a "fingerprint" is generated, consisting of numerical representations of levels of trapped charges in selected memory cells. The fingerprint is then provided to an external device and stored. When the card is to be used again, the fingerprint is read from the card and compared against the stored fingerprint before the card is accepted as authentic.

Such techniques do not provide for security of secret data stored on the card. In techniques of the prior art, data to be securely stored may be encrypted using numerical encryption techniques. If the encryption keys are stored in the memory in numerical form, they are vulnerable to unauthorized recovery. An attacker may simply probe the memory to extract numerical information from any desired location within the memory, in a search for the keys. Once the keys are identified, the attacker can simply decrypt the data.

There exists, therefore, a need in the art for techniques for securing of secret data which provide enhanced resistance to attack.

Summary of the Invention

To this end, as discussed in greater detail below, a mediametric technique is provided to advantageously enhance resistance to attack of smart card data. In one respect, a data storage device according to the present invention may suitably be embodied as a smart card. The smart card includes a memory array such as that of an EPROM or EEPROM, which can be read by a microcontroller residing on the card. The memory array comprises a plurality of memory cells, each of which is characterized by a charge level. Each cell contains a representation of a binary digit in the form of a level of charge, which may be a "high" level of charge for a binary "1" and a "low" level of charge for a binary zero. The "high" and "low" levels of charge differ widely, making it easy to distinguish between a "1" and a "0". Programming a cell involves placing a high or low level of charge in the cell, depending on whether a "1" or a "0" is desired. It is not possible to set the level of charge precisely, but once the level of charge has been established it may be precisely measured.

The microcontroller can read the levels of charge, but in order for this information to be accessible outside the smart card, the microcontroller must pass it outside the card. Therefore, if the microcontroller is designed or programmed to protect this information, it can be used inside the smart card, but cannot be obtained or known outside the internal workings of the smart card. This is because any attempt to open the memory array and read the memory contents will disrupt the levels of charge within the memory cells. The binary representations of data can be read in this way, but the act of reading will disrupt the charge levels.

It is therefore possible for the microcontroller to generate an internal encryption key, or alternatively a seed for an encryption key, using data representing charge levels of selected cells of the EEPROM. The encryption key generated from this data can be held within the microcontroller, without ever being released outside the microcontroller. Alternatively, the key may simply be generated when needed and erased after each use. The key provides very good security against compromise, because any attempt to obtain the charge levels will fail.

In order to secure data for storage on a smart card according to the present invention, the data is encrypted using any of a number of standard encryption techniques. The particular technique employed is a matter of design choice, and does not affect the operation of the present invention. The encrypted data is written to the smart card. The encryption key used to encrypt the data, referred to here as the external key, is also provided to the smart card, preferably by providing the key to the microcontroller. After being provided to the smart card, the external key is itself encrypted, using an internal key generated according to the techniques of the present invention.

The internal key is generated using charge level data from the EEPROM. The microcontroller retrieves charge level data from selected cells within the EEPROM. This charge level data is converted from analog to digital form in order to be operated on by the microcontroller. The charge level data need not be stored in numerical form, but can simply be retrieved from the EEPROM whenever it is needed. This secures the charge level data from being discovered, and therefore prevents discovery of the internal key.

Once the charge level data has been retrieved, the microcontroller uses it to encrypt or decrypt the external key. This may be done by using the charge level data to generate an internal key, or alternatively to generate a seed for an internal key. Once the internal key has been generated, it is then used for cryptoprocessing of the external key. After the external key has been provided to the microcontroller and encrypted, it can then be stored in the EEPROM. When data is to be stored on the smart card, the external key can be retrieved, decrypted using the internal key, and used to encrypt the data for storage on the card. Once the data is stored, it is secure. It is encrypted using the external key, but the external key is stored on the card in encrypted format. The internal key cannot be retrieved in order to encrypt the external key, because the internal key is not stored in numerical form. Instead, it is simply obtained whenever needed by examining the physical properties of the EEPROM cells, and these properties cannot be known outside the card.

A more complete understanding of the present invention, as well as further features and advantages of the invention, will be apparent from the following Detailed Description and the accompanying drawings.

Brief Description of the Drawings

Fig. 1 illustrates an exemplary memory cell used in a data storage device according to the present invention;

Fig. 2 is a graphical representation of differing charge levels prevailing in a memory array employed in a data storage device according to the present invention;

Fig. 3 illustrates a first data storage device according to the present invention including an EEPROM array, where parallel access is provided to the array;

Fig. 4 illustrates a second data storage device according to the present invention including an EEPROM array, where parallel access is provided to the array;

Fig. 5 illustrates a method of initialization in preparation for generation of a mediametric cryptoprocessing key according to the present invention;

Fig. 6 illustrates a method of mediametric key generation according to the present invention;

Fig. 7 illustrates a method of mediametric key cryptoprocessing according to the present invention; and

Fig. 8 illustrates a method of generating a random number using mediametric properties of a device.

Detailed Description

Fig. 1 illustrates a memory cell 100 which may be advantageously employed according to the teachings of the present invention. The memory cell 100 may comprise a transistor integrated on a p-type substrate 102. The transistor comprises a source (S) 104 and a drain (D) 106 which are fabricated using well known techniques by the diffusion of N+ impurities on the substrate 102. The transistor includes a field oxide layer 108 that overlays the source 104 and the drain 106, and a floating gate 110 fabricated from a first layer of polysilicon that overlays the oxide layer 108. The transistor further comprises a gate 112 fabricated from a second layer of polysilicon that overlays the floating gate 110. Data may be programmed in the memory cell 100 for purposes of data storage according to the well known technique of floating-gate charge injection. For example, a potential which is typically greater than 12 volts is applied to the drain 106 to create a strong electric field that energizes electrons to jump from the drain 106 region to the floating gate 110 region. The electrons attracted to the floating gate 110 become trapped in the floating gate 110 when the potential is removed from the drain 106. When charges are trapped in the floating gate 110, the threshold of the memory cell 100 changes from a relatively low value, which is associated with the memory cell 100 when no charge or a small charge is present and is called an erased condition, to a higher value, which indicates that programming of the memory cell 100 has occurred. If a low voltage potential for programming a logic level low or "0" in the memory cell 100 is applied to the gate 112, then electrons are not attracted to the floating gate 110, and thus the floating gate 110 remains uncharged. On the other hand, if a high voltage potential for programming a logic level high or "1" is applied to the gate 112, then a large number of electrons will be attracted to the floating gate 18, thereby charging the floating gate 110.

It is well known to one of skill in the art that typical voltages for programming high and low logic levels depend upon the type and design of the semiconductor memory device being used. The level of charges that will be trapped in the memory cell 100 as a result of programming depends upon the characteristics of the semiconductor material and the geometry of the structures in the memory cell 100. For instance, variations in doping levels and dopant purities and the thickness of doped regions of a semiconductor substrate will cause inherent random variations in the level of charges that are trapped in a memory cell when a specific voltage level is applied for a specified amount of time during programming. These inherent random variations make reproduction or duplication of the same relative level of trapped charges in a second memory cell for purposes of obtaining an identical level of trapped charge in the second memory cell very difficult, if not impossible. The level of charges which will be trapped in a memory cell also depends on environmental conditions, such as temperature and the presence of stray static charges, existing at the time that the memory cell is programmed. In addition, the previous level of trapped charges for the memory cell and the total number of write cycles applied to the memory cell, known as the history of the memory cell, contribute to the level of charges trapped in the memory cell. Therefore, with each programming event the pattern of the trapped charges in memory cells of a memory array will vary in a manner which cannot be reproduced, even when the same memory cell is programmed with the identical data.

In an application such as a smart card, it is possible to embed an array of memory cells such as the memory cell 100 into the card, and design the array with one or more ports by which the charge levels of the memory cells may be read by a device such as a microcontroller or microprocessor which is also embedded in the card. If the array and the card are designed such that no external access is allowed to the memory array, the charge level data will be very difficult or almost impossible to intercept. The binary contents of the memory cells such as the cell 100 can be intercepted from outside, because the digital representations of binary data have relatively wide tolerances. However, an attack which attempts to obtain the precise charge levels other than through the port will disrupt the charge levels, such that the attacker will be unable to recover the correct data. The present invention utilizes the inherent, unique and irreproducible variations in the level of trapped charges of each programmed memory cell such as the cell 100 to provide a substantial amount of unpredictable data, which remains stable between write cycles of each of the cells, but which is nearly immune from unauthorized access. This data can be used to generate encryption keys which are used exclusively by the smart card and which are not known outside the smart card.

Fig. 2 is a graphical representation of differing charge levels prevailing in a memory array 200 which may be suitably employed in a data storage device according to the present invention. Charges are at either high or low states, but the high states are not identical to one another, and the low states are not identical to one another. Charge levels 202 and 204, for example, are both in a high state, but they are not identical. Similarly, charge levels 206 and 208 are both in a low state, but are not identical. In writing data to the array 200, it is a simple matter to set each memory cell at a charge level corresponding to a high or a low state, but it is not possible to specify the exact charge level of the memory cell. However, it is easy to read the charge level of each memory cell with great precision, provided that suitable connections are provided for this purpose.

Fig. 3 illustrates a data storage device 300 providing data security according to the principles of the present invention. The device 300 includes a memory array 302, which is here shown as an EEPROM comprising an array of memory cells similar to the cell 100 of Fig. 1. The array 302 is embodied here as an EEPROM because such devices typically include additional mechanisms, such as analog input and output lines for erasing or rewriting data to memory cells of memory arrays, that are useful for explaining the techniques and advantages of the present invention. A memory chip utilizing non-volatile floating-gate EEPROM cell technology has been developed by Information Storage Devices ™, and such a device may be used to practice the invention. However, it is to be understood that the memory array 302 may be any suitable device which comprises memory cells which are structurally and operationally similar to that of the memory cell 100 of FIG. 1, described above, and that most semiconductor memory devices may be adapted for use with this invention.

The storage device 300 also includes a microcontroller 304, which includes a microprocessor 306, RAM 308 and ROM 310. The microcontroller 304 also includes a data port 311 to allow transfer of data between the data storage device 300 and an external device. The data port 311 is connected to the microprocessor 306 and may suitably be a data bus.

It is also necessary to allow the microcontroller 304 to communicate with the memory array 302. An address bus 312 and data bus 314 enable transfer of numerical data between the microcontroller 304 and the array 302. In addition, first and second analog outputs 316 and 318 of the array 302 are used to provide access to charge level data of memory cells in the memory array 302, for use by the microcontroller 304.

In order to provide data security, the storage device 300 employs the charge level data describing charge levels of selected memory cells in the array 302. The first and second analog outputs 316 and 318 are used as inputs to first and second operational amplifiers 320 and 322. The outputs of the operational amplifiers 320 and 322 are provided as inputs of a differential amplifier 324. The output of the differential amplifier 324 is provided to an analog to digital (A/D) converter 326, which converts the analog data to digital data which can be processed by the microcontroller 304. The A/D converter 326 provides data to the microcontroller 304 by means of a data line 328. The microcontroller 302 is controlled so that it accepts data from the A/D converter by means of the application of a control signal or signals on a strobe line 330.

Whenever an internal key is needed for use by the microcontroller 304, the microcontroller 304 directs the memory array 302 to provide charge level data from selected cells. This data is provided through the analog outputs 316 and 318, conditioned by the operational amplifiers 320 and 322 and the differential amplifier 324, and converted to digital form by the A/D converter 326. The digital data representing the charge level data is then processed by the microcontroller 304. The microcontroller 304 uses this data to generate the internal key, which may then be used to encrypt an external key provided from outside the data storage device 300. The microcontroller 304 can then store the encrypted external key in the array 302. The external key, or any other data which is desired to be stored after retrieval of the charge data from which the internal key is generated, must be stored in memory cells other than the memory cells whose charge level data is used to generate the internal key. This is because the charge level in a cell changes whenever data is written to the cell. If data is written to the cell, therefore, the charge level of the cell will not be usable for reconstruction of the internal key.

It is possible to implement the various components of the storage device 300 on a single integrated circuit. This helps to provide security, as all connections except for the data port 311 would then be inside the integrated circuit.

Fig. 4 illustrates an alternative data storage device 400 according to the present invention, illustrating the use of mediametric data security techniques with serial memories. The device 400 employs a serial memory array 402. The memory array 402 may suitably be a serial EPROM or EEPROM. The memory array 402 is connected to a microcontroller 404, which includes a microprocessor 406, RAM 408 and ROM 410. The microcontroller 404 also includes a data port 411 to allow transfer of data between the data storage device 400 and an external device. The data port 411 is connected to the microprocessor 406 and may suitably be a data bus. The memory array 402 communicates with the microcontroller 404 using a clock line 412 and a data line 414. Each of the array 402 and the microcontroller 404 passes data to the other by placing data on the data line 414 one bit at a time and sending a clock input along the clock line for each bit. The memory array 402 also provides an analog output 416, which is used to provide charge level data to the microcontroller 404. The analog output is connected to an operational amplifier 418, which receives and processes mediametric data from the array 402, the mediametric data being charge level readings for levels of trapped charge in cells of the array 402. The operational amplifier 418 produces an output which is then used as an input to a sample and hold circuit 420 and a differential amplifier 422. The sample and hold circuit 420 passes its input to the differential amplifier 422 upon receiving a latch signal produced by the microcontroller 404. The output of the differential amplifier 422 is received by an analog to digital (A/D) converter 424, which converts the analog data representing charge levels of cells of array 402 into digital representations. The analog to digital converter 424 passes each digital representation to the microcontroller 404 upon receiving a strobe signal produced by the microcontroller 404. The data storage device 400 allows the microcontroller 404 to receive mediametric data relating to charge levels of memory cells in the memory array 402 and to use this data to generate cryptographic keys in a similar fashion to that discussed above for the microcontroller 304.

It is possible to implement the various components of the storage device 400 on a single integrated circuit. This single circuit implementation helps to provide security, as all connections except for the data port 411 would then be inside the integrated circuit.

Fig. 5 illustrates a method 500 of mediametric initialization in preparation for encryption, according to the present invention. At step 502, data is stored in a memory array having mediametric characteristics. The memory array possesses physical characteristics which are difficult or impossible to duplicate, but which can be precisely measured. The memory array may be an array such as the array 302 of Fig. 3, the array 402 of Fig. 4, or any other suitable memory array, wherein the mediametric characteristics are levels of charges trapped in the memory cells. Storage and retrieval of data to and from the memory array, and processing of data, is preferably accomplished by a data processing device such as the microcontroller 304 of Fig. 3, the microcontroller 404 of Fig. 4, or any other suitable data processing device. Storing the data establishes a set of mediametric data in the memory array, by setting a new charge level in each cell. At step 504, initial values are acquired. Next, a data set is collected. At step 506, an initial index is generated. This is an index pointing to a memory cell from which mediametric data, such as the level of trapped charges in the memory cell, is to be obtained. Next, at step 508, the mediametric value of the memory cell specified in the index is acquired. That is, the charge level or similar data is read and the mediametric data is suitably converted to a digital representation for easy storage and processing by a digital processor. At step 510, the mediametric value is accumulated. That is, it is stored, either individually or through summing or other processing with other mediametric values that have previously been recovered. Next at step 512, a determination is made as to whether the desired data set is complete. If the data set is not complete, the process continues to step 514, and a new index is generated in order to acquire data from an additional memory cell. Next, the process proceeds to step 516, and the set of index parameters, comprising all indices which have been generated, is updated. Next, at step 518, the set of index parameters is stored, and the process returns to step 508.

If the data set is complete, the process continues to step 520 and an optimum mediametric key is generated. Next, at step 522, a mediametric parameter set is generated. Next, at step 524, the mediametric parameter set is stored. Next, at step 526, a cyclic redundancy code (CRC) for the mediametric key is generated. Next, at step 528, the mediametric key CRC is stored.

Fig. 6 illustrates a method 600 of mediametric key generation according to the present invention. At step 602, initial values are acquired. The initial values are mediametric data obtained from a device. The device may suitably be a storage device such as the serial memory array 402 of Fig. 4 or the parallel memory array 302 of Fig. 3, and the mediametric data may suitably be definitions of levels of trapped charges within the memory array. Storage and retrieval of data to and from the memory array, and processing of data, is preferably accomplished by a data processing device such as the microcontroller 304 of Fig. 3, the microcontroller 404 of Fig. 4, or any other suitable data processing device. At step 604, an initial index is generated. This is a location within the array from which mediametric data is to be retrieved. Next, at step 606, the mediametric value at the array location indicated by the index is retrieved. Next, at step 608, the retrieved value is accumulated with all other previously retrieved values. Next, at step 610, a determination is made as to whether the data set is complete. If the data set is not complete, the process proceeds to step 611 and the previously stored index parameters are retrieved. Next, at step 612, the next index is generated. The process then returns to step 606. If the data set is complete, the process continues to step 614 and the accumulated mediametric parameters are retrieved. Next, the process proceeds to step 616 and a key is generated using the accumulated mediametric parameters. Next, at step 618, the cyclic redundancy code associated with the key is retrieved. This is the cyclic redundancy code generated for the key during the process 500 of Fig. 5. Next, at step 620, the key is verified using the cyclic redundancy code. If the key passes the verification, the process proceeds to step 622 and the key is stored in a volatile memory, preferably within the data processing device. If the key does not pass verification, the process proceeds to step 624 and an error counter is incremented. Next, at step 626, the error counter is compared to a predetermined limit. If the limit is exceeded, the process proceeds to step 628 and an error is reported. If the error limit is not exceeded, the process returns to step 602 and a new attempt is made to generate a key.

Fig. 7 illustrates a method 700 of data encryption using a mediametric key such as the key generated by the method 600 of Fig. 6. At step 702, a mediametric key is generated. This may be done by performing the initialization method 500 of Fig. 5 and the key generation method 600 of Fig. 6. Next, at step 704, the mediametric key is stored in a volatile memory, preferably within the data processing device. Next, at step 706, data is retrieved from an outside source. Next, at step 708, the data is cryptoprocessed using the mediametric key generated at step 702. Next, at step 710, the cryptoprocessed data is output. For example, if the data has been encrypted, it may be output to a memory array for storage. An optional step 712 may follow of erasing the mediametric key from the volatile memory.

In addition to generating a mediametric key for use in cryptoprocessing, it is possible to use mediametric properties to generate useful data. For example, it may be very useful to be able to produce a truly random number. Genuinely random numbers are difficult to generate, especially with limited processing resources such as may be used in a smart card. The use of mediametric properties simplifies random number generation. Charge levels in a memory array are randomly distributed, providing a conveniently accessible source of random data. If charge level data is obtained from a sequence of cells, the charge level data can be used to construct a random number.

Fig. 8 illustrates a method 800 of random number generation according to the present invention. At step 802, data is written to a memory array. The memory array may suitably be an EPROM or EEPROM such as the memory array 302 of Fig. 3, or the memory array 402 of Fig. 4. Writing the data to the array establishes a random pattern of charge levels in the cells of the memory array. At step 804, a desired length of a random number is established. At step 806, a sequence of cells is established from which charge level data is to be obtained. The number of cells in the sequence is sufficient to yield a number of the desired length. At step 808, memory charge level data is retrieved from each cell in the sequence. At step 810, the charge level data is converted to digital representations for processing. At step 812, the representations of the charge level data are processed to produce a random number.

While the present invention is disclosed in the context of a presently preferred embodiment, it will be recognized that a wide variety of implementations may be employed by persons of ordinary skill in the art consistent with the above discussion and the claims which follow below.

We claim:

1. A secure data storage system, comprising:

a memory possessing mediametric properties; and

a processor adapted to receive data relating to mediametric properties of the memory and use the mediametric properties as data to generate an encryption key to encrypt data for storage in the memory.

2. The data storage system of claim 1 and further including a conversion circuit to provide a numerical representation of the mediametric properties of the memory for easy use by the processor.

3. The data storage system wherein the memory comprises a memory array including a plurality of memory cells, each of the memory cells being programmable through the application of a voltage which serves to trap charges within the memory cell, the mediametric properties of the memory being the level of trapped charges within each cell.

4. The data storage system of claim 3 wherein the memory array includes an analog output to enable reading the levels of trapped charges, and wherein the conversion circuit includes an analog to digital converter to convert the levels of trapped charges to a digital representation.

5. The data storage system of claim 4 wherein the memory array is a parallel memory array.

6. The data storage system of claim 4 wherein the memory array is a serial memory array.

7. The data storage system of claim 4 wherein the memory array, the conversion circuit and the processor are contained in a single integrated circuit.

8. The data storage system of claim 7 wherein the integrated circuit includes a data port to provide external access to the processor.

9. The data storage system of claim 8 wherein the integrated circuit is embedded within a smart card.

9. The data storage system of claim 8 wherein the mediametric properties are used to generate an internal key used for cryptoprocessing solely within the data storage system, and wherein the data cryptoprocessed by the internal key includes an external key to be used for cryptoprocessing of data supplied to the data storage system.

10. A method of secure data storage, comprising the steps of:

retrieving mediametric data relating to the mediametric properties from the device;

processing the mediametric data to create a mediametric cryptoprocessing key for cryptoprocessing of data stored in the device; and cryptoprocessing data for storage in the device using the mediametric key.

11. The method of claim 10 wherein the device is a memory array comprising a plurality of memory cells and the mediametric data comprises levels of trapped charges in each of the memory cells.

12. The method of claim 11 wherein the mediametric data is converted to digital form for processing.

13. The method of claim 12 wherein the step of retrieving the mediametric data is preceded by the steps of establishing a desired key length and selecting cells from which mediametric data is to be retrieved and the step of retrieving the data comprises sequentially retrieving that data from each of the selected cells and accumulating the data until data has been retrieved from each of the selected cells.

14. The method of claim 13 wherein the key is verified using a cyclic redundancy code.

15. The method of claim 14 wherein the step of selecting cells from which the mediametric data is to be retrieved is followed by the step of writing numerical data to the selected cells in order to establish new random mediametric data for key generation.

16. A method of random number generation comprising:

retrieving mediametric data from selected cells of a memory array;

converting the mediametric data to numerical representations; and

processing the numerical representations to produce the random number.

FIG. 1

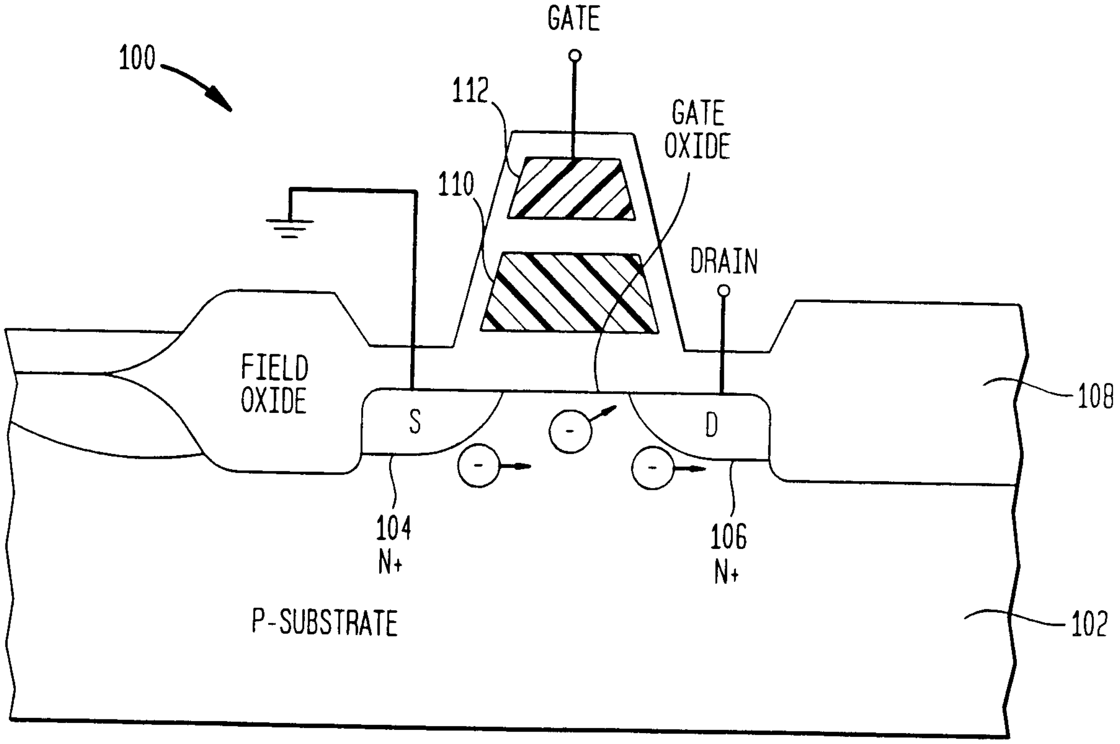

GATE
100
112
GATE
OXIDE
110
DRAIN
FIELD
OXIDE
S
D
108
104
N+
106
N+
P-SUBSTRATE
102

FIG. 2

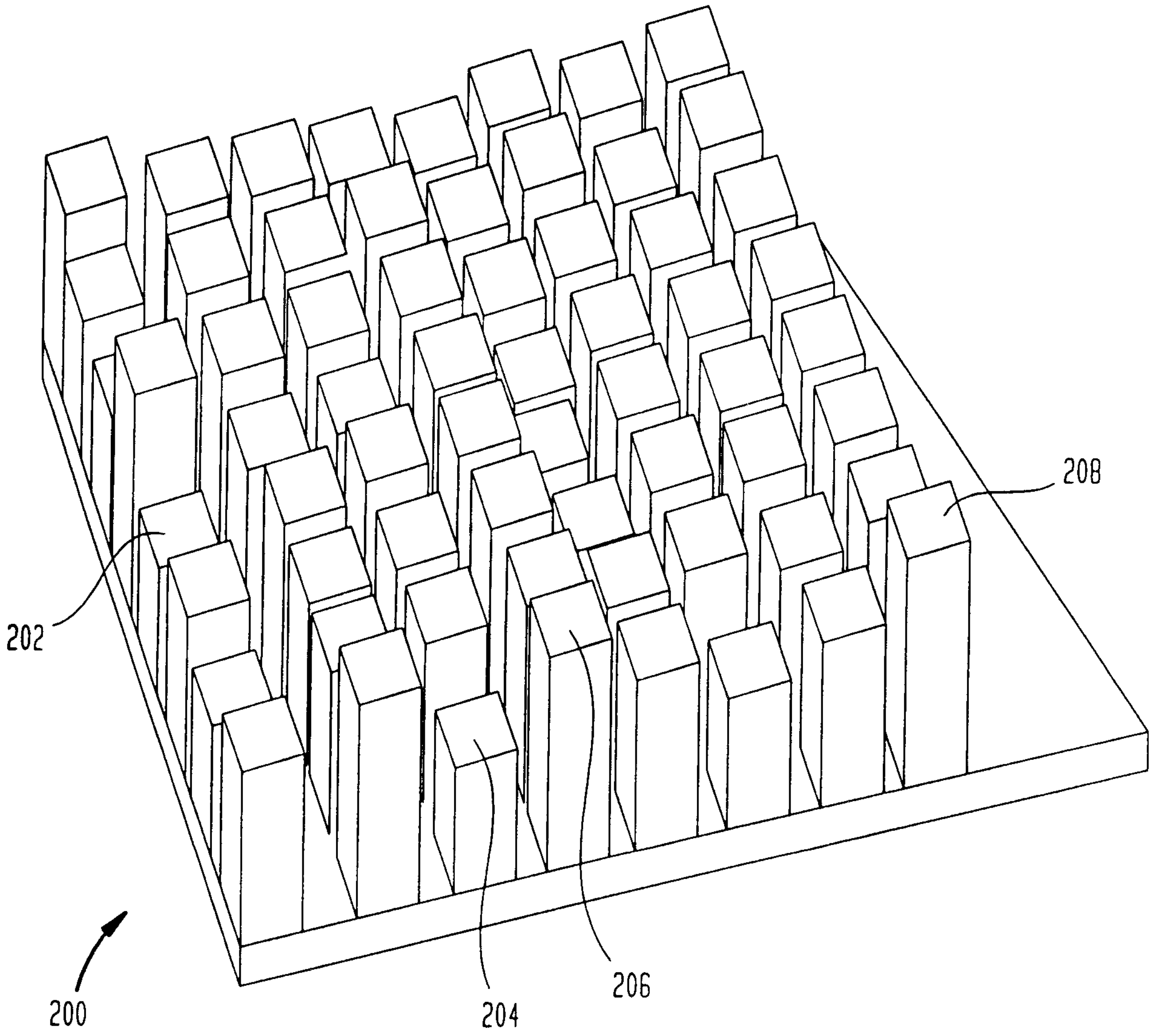


FIG. 3

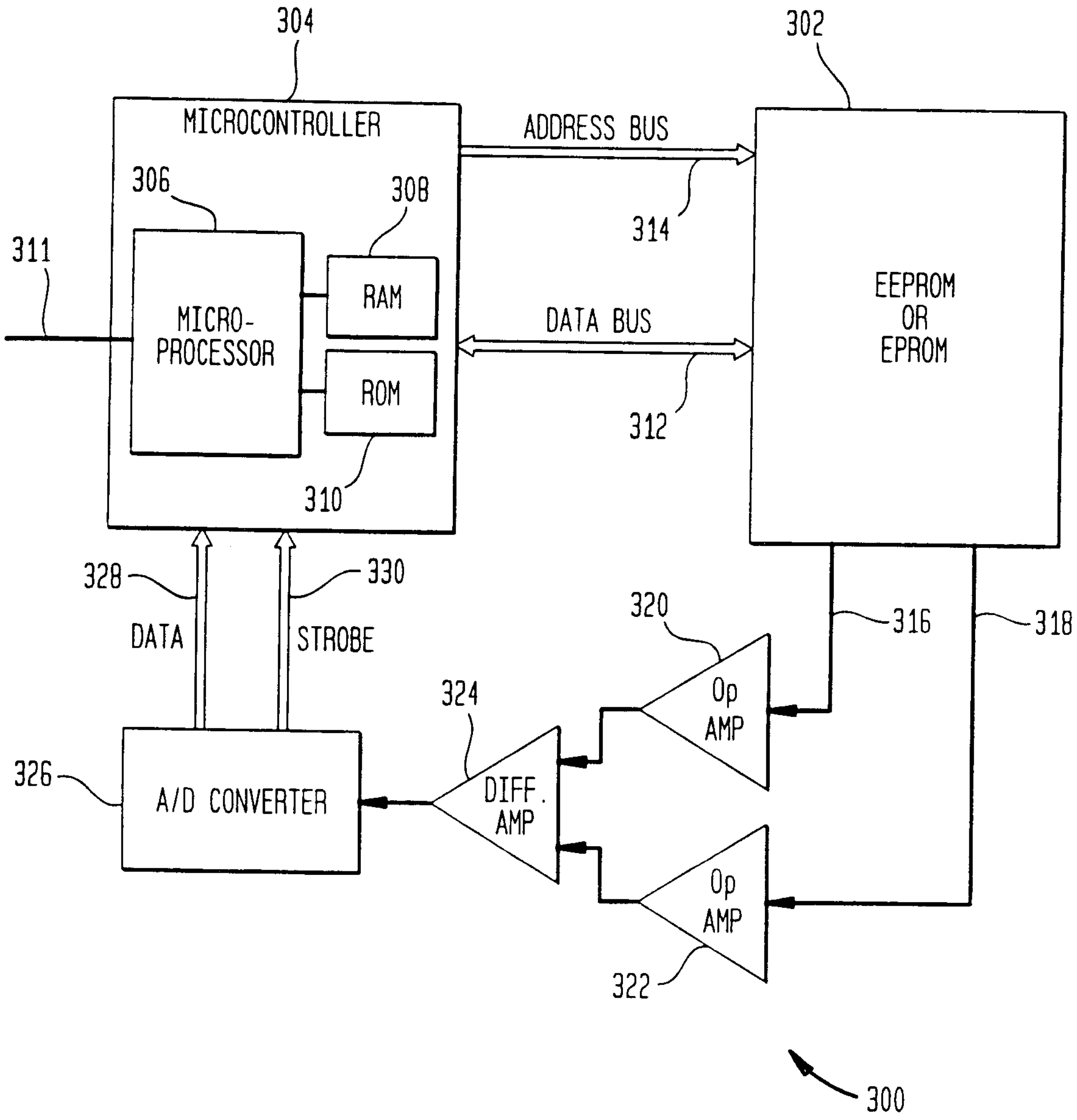
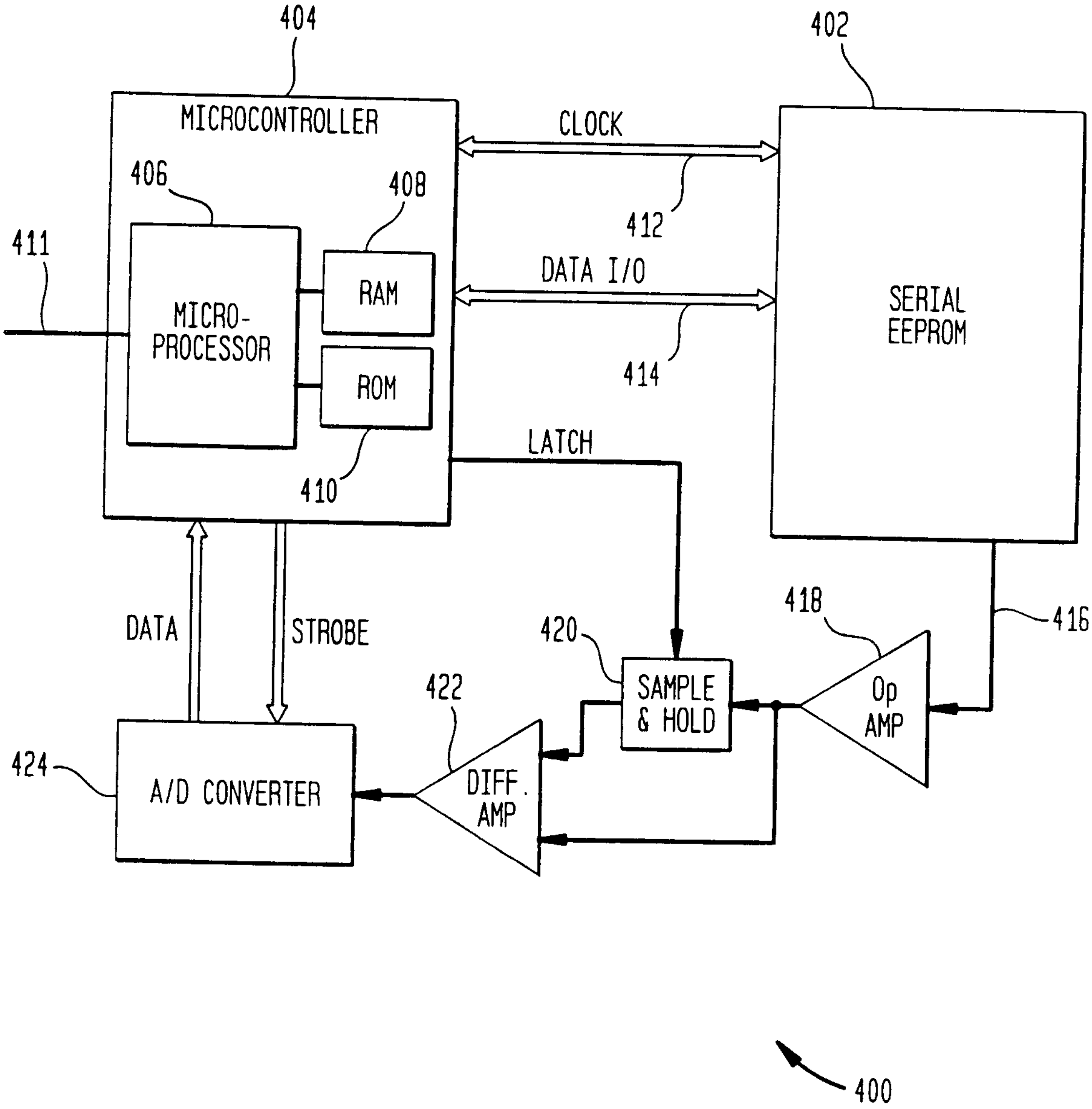

304
MICROCONTROLLER
302
ADDRESS BUS
306
308
314
311
MICRO-
PROCESSOR
RAM
ROM
DATA BUS
EEPROM
OR
EPROM
312
310
328
330
DATA
STROBE
320
316
318
324
Op
AMP
326
A/D CONVERTER
DIFF.
AMP
Op
AMP
322
300

FIG. 4


404
MICROCONTROLLER
406
408
411
MICRO-
PROCESSOR
RAM
ROM
410
402
CLOCK
412
DATA I/O
414
SERIAL
EEPROM
LATCH
DATA
STROBE
420
418
416
SAMPLE
& HOLD
Op
AMP
422
DIFF.
AMP
424
A/D CONVERTER
400

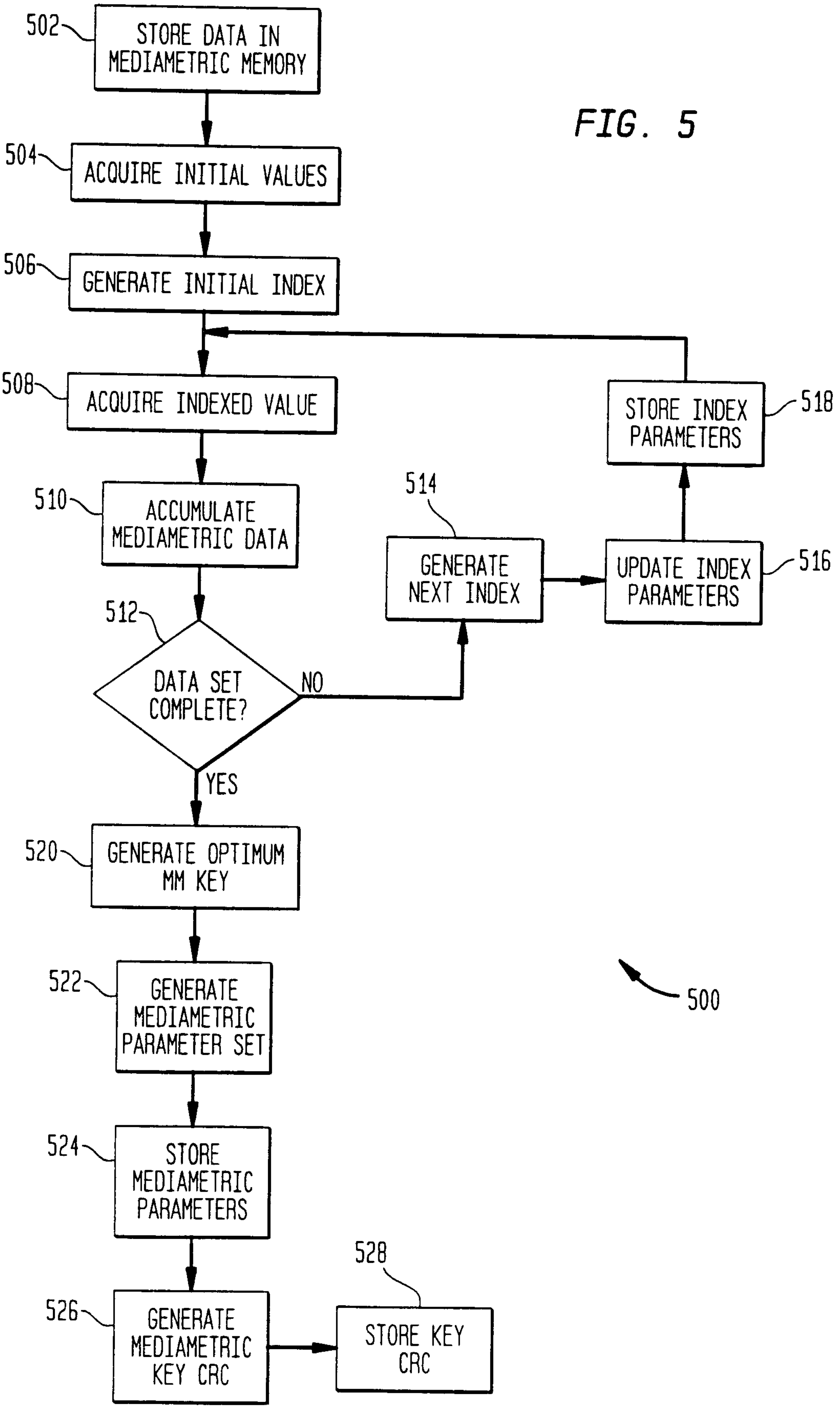

502
STORE DATA IN MEDIAMETRIC MEMORY
504
ACQUIRE INITIAL VALUES
506
GENERATE INITIAL INDEX
508
ACQUIRE INDEXED VALUE
510
ACCUMULATE MEDIAMETRIC DATA
512
DATA SET COMPLETE?
NO
YES
514
GENERATE NEXT INDEX
516
UPDATE INDEX PARAMETERS
518
STORE INDEX PARAMETERS
520
GENERATE OPTIMUM MM KEY
522
GENERATE MEDIAMETRIC PARAMETER SET
524
STORE MEDIAMETRIC PARAMETERS
526
GENERATE MEDIAMETRIC KEY CRC
528
STORE KEY CRC
500

FIG. 5

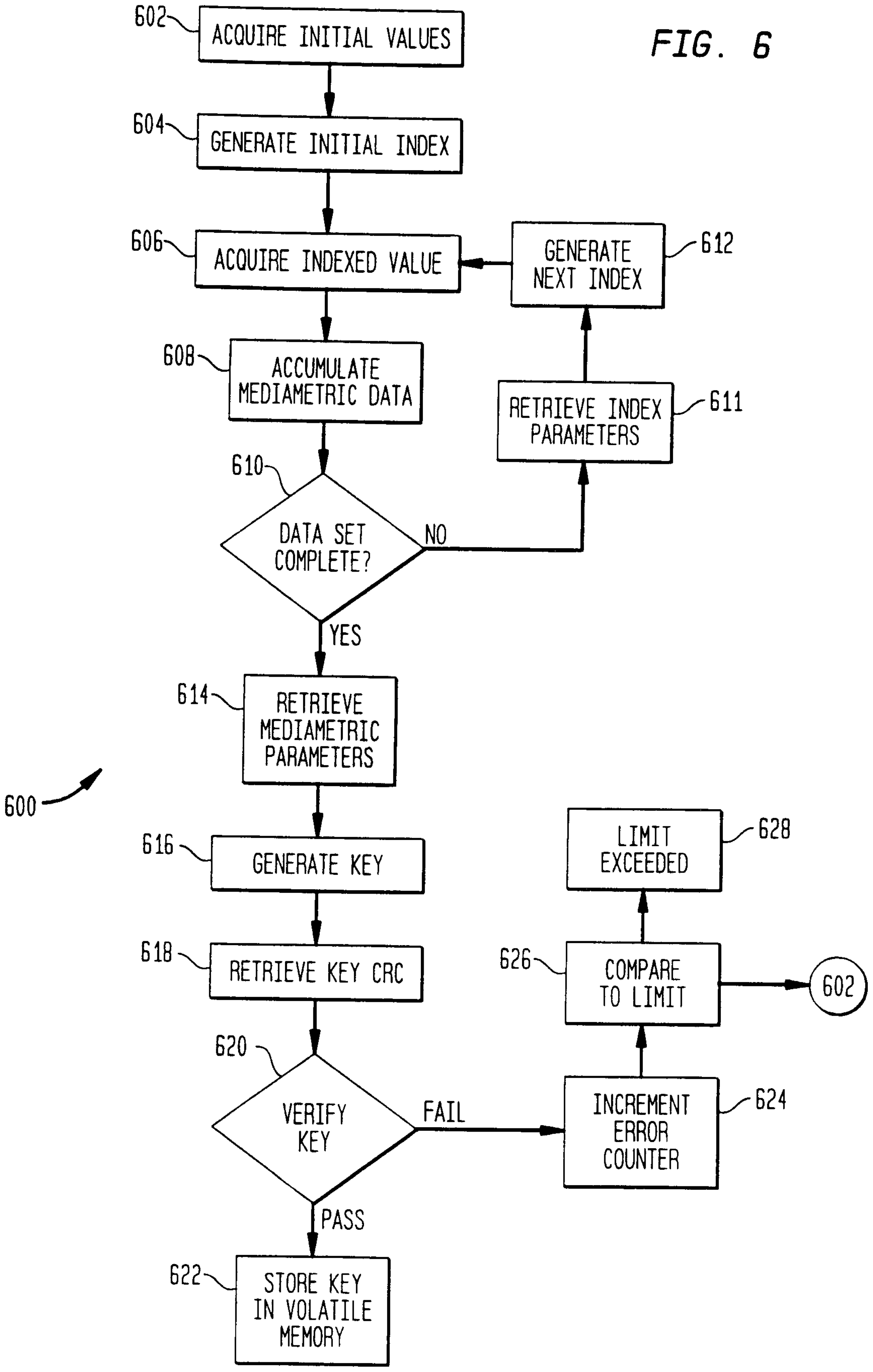

602
ACQUIRE INITIAL VALUES
604
GENERATE INITIAL INDEX
606
ACQUIRE INDEXED VALUE
612
GENERATE NEXT INDEX
608
ACCUMULATE MEDIAMETRIC DATA
611
RETRIEVE INDEX PARAMETERS
610
DATA SET COMPLETE?
NO
YES
614
RETRIEVE MEDIAMETRIC PARAMETERS
600
628
LIMIT EXCEEDED
616
GENERATE KEY
618
RETRIEVE KEY CRC
626
COMPARE TO LIMIT
602
620
VERIFY KEY
FAIL
624
INCREMENT ERROR COUNTER
PASS
622
STORE KEY IN VOLATILE MEMORY

FIG. 6

FIG. 7

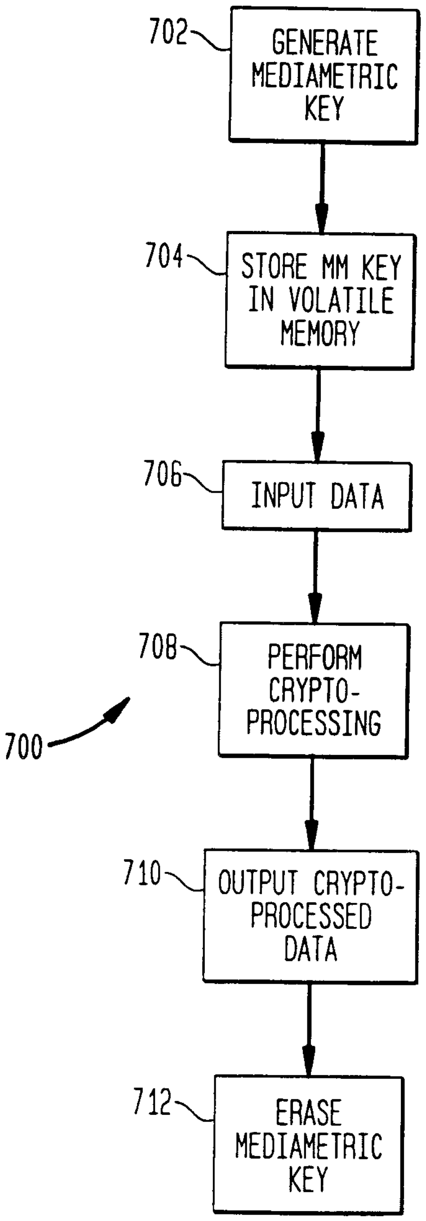

702
GENERATE MEDIAMETRIC KEY
704
STORE MM KEY IN VOLATILE MEMORY
706
INPUT DATA
708
PERFORM CRYPTO-PROCESSING
700
710
OUTPUT CRYPTO-PROCESSED DATA
712
ERASE MEDIAMETRIC KEY

FIG. 8

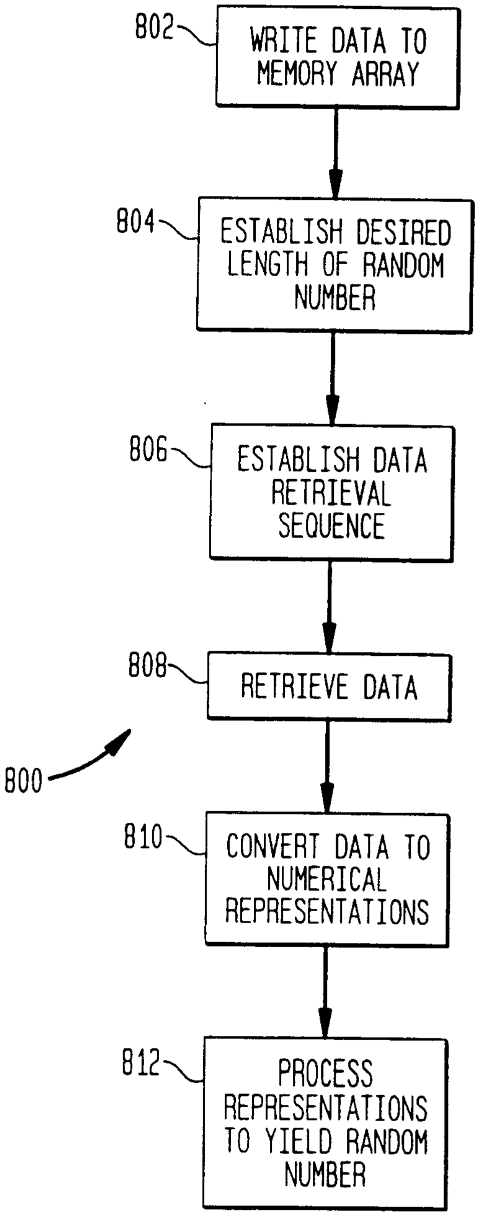
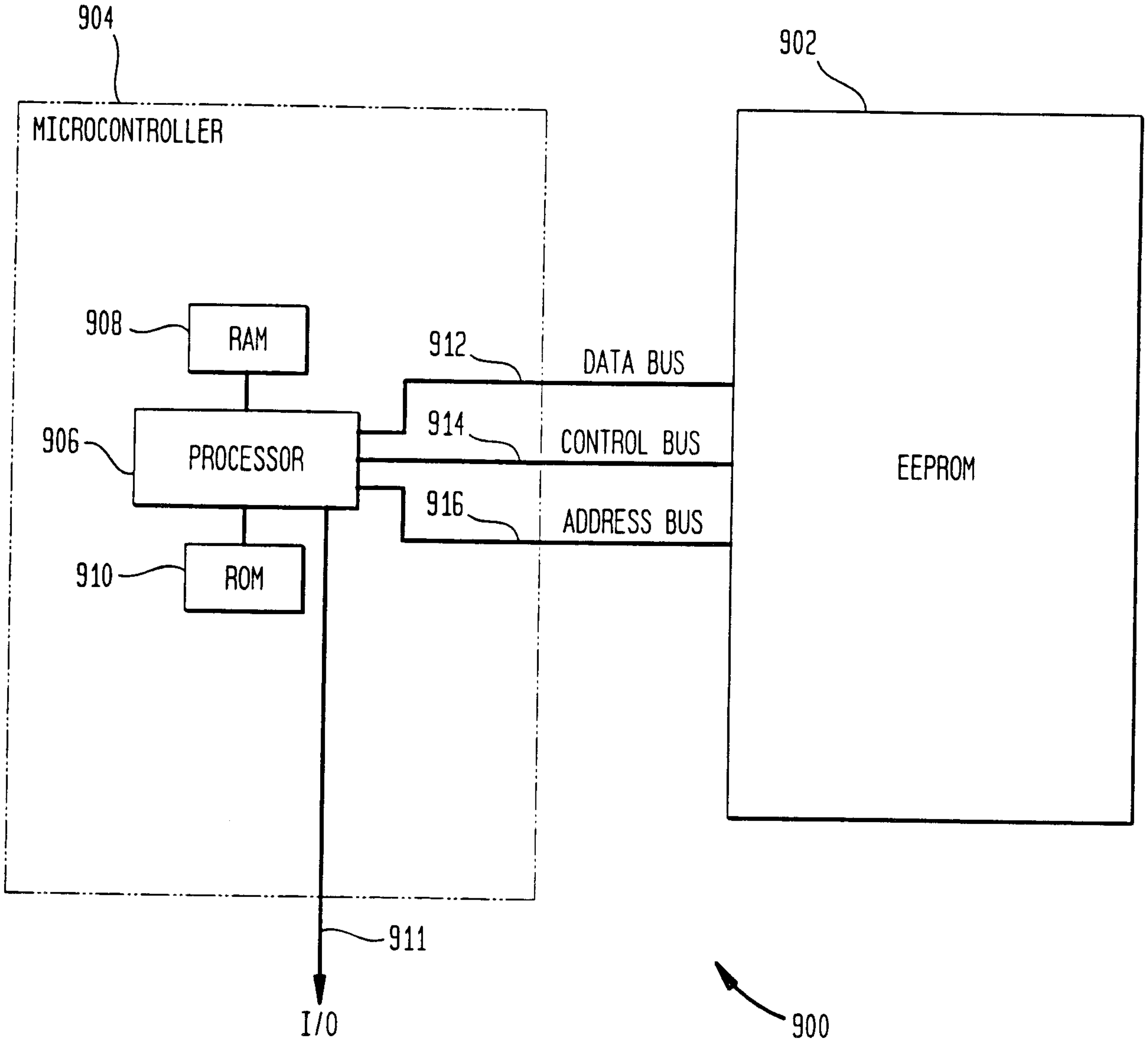

802
WRITE DATA TO MEMORY ARRAY
804
ESTABLISH DESIRED LENGTH OF RANDOM NUMBER
806
ESTABLISH DATA RETRIEVAL SEQUENCE
808
RETRIEVE DATA
800
810
CONVERT DATA TO NUMERICAL REPRESENTATIONS
812
PROCESS REPRESENTATIONS TO YIELD RANDOM NUMBER

FIG. 9


904
MICROCONTROLLER
902
908
RAM
912
DATA BUS
906
PROCESSOR
914
CONTROL BUS
EEPROM
916
ADDRESS BUS
910
ROM
911
I/O
900

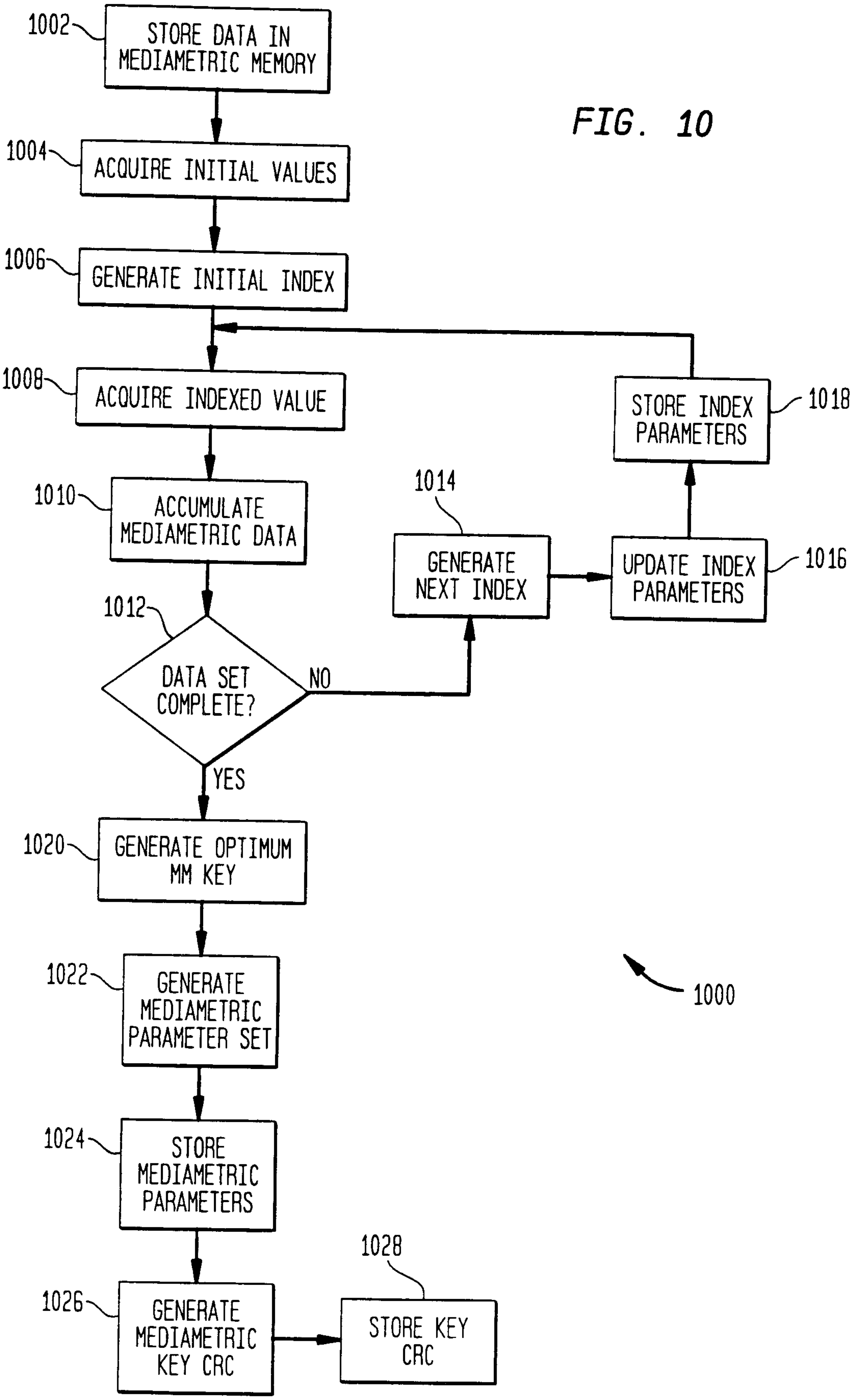

1002
STORE DATA IN MEDIAMETRIC MEMORY
1004
ACQUIRE INITIAL VALUES
1006
GENERATE INITIAL INDEX
1008
ACQUIRE INDEXED VALUE
1010
ACCUMULATE MEDIAMETRIC DATA
1012
DATA SET COMPLETE?
NO
YES
1014
GENERATE NEXT INDEX
1016
UPDATE INDEX PARAMETERS
1018
STORE INDEX PARAMETERS
1020
GENERATE OPTIMUM MM KEY
1022
GENERATE MEDIAMETRIC PARAMETER SET
1024
STORE MEDIAMETRIC PARAMETERS
1026
GENERATE MEDIAMETRIC KEY CRC
1028
STORE KEY CRC
1000

FIG. 10

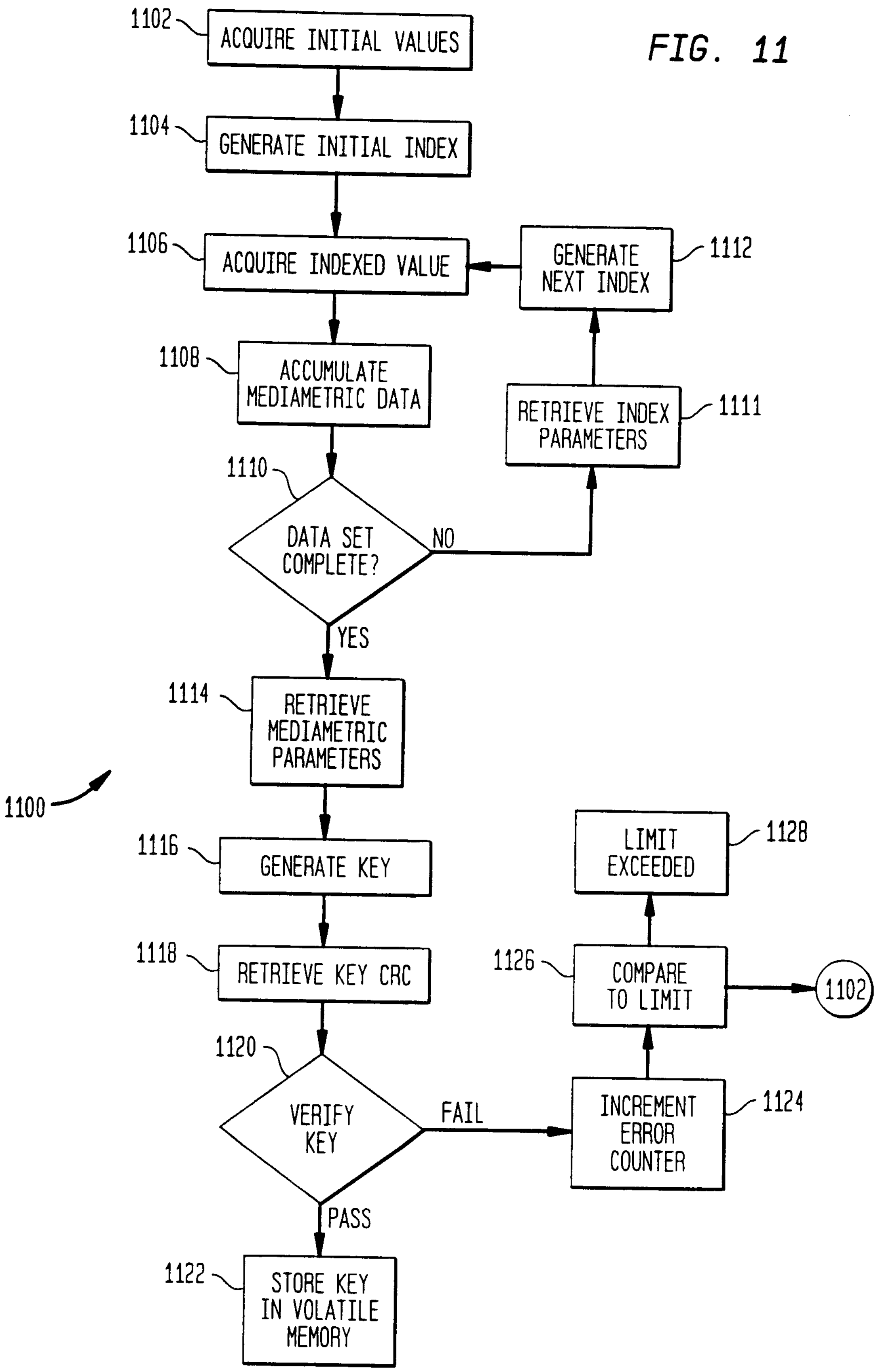
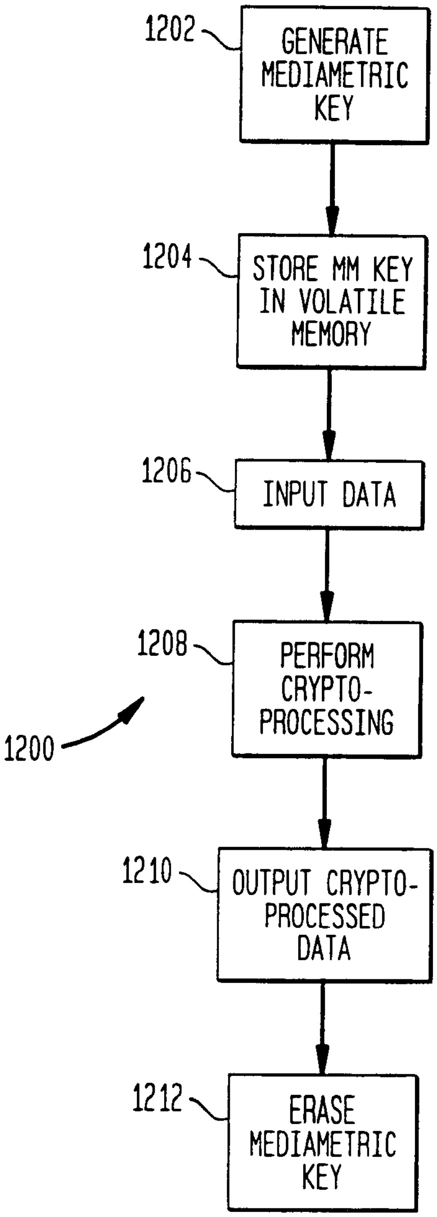

1102
ACQUIRE INITIAL VALUES
1104
GENERATE INITIAL INDEX
1106
ACQUIRE INDEXED VALUE
GENERATE NEXT INDEX
1112
1108
ACCUMULATE MEDIAMETRIC DATA
RETRIEVE INDEX PARAMETERS
1111
1110
DATA SET COMPLETE?
NO
YES
1114
RETRIEVE MEDIAMETRIC PARAMETERS
1100
1116
GENERATE KEY
LIMIT EXCEEDED
1128
1118
RETRIEVE KEY CRC
1126
COMPARE TO LIMIT
1102
1120
VERIFY KEY
FAIL
INCREMENT ERROR COUNTER
1124
PASS
1122
STORE KEY IN VOLATILE MEMORY

FIG. 11

FIG. 12


1202
GENERATE MEDIAMETRIC KEY
1204
STORE MM KEY IN VOLATILE MEMORY
1206
INPUT DATA
1208
PERFORM CRYPTO-PROCESSING
1200
1210
OUTPUT CRYPTO-PROCESSED DATA
1212
ERASE MEDIAMETRIC KEY

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US01/13504

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/00, 9/32, 17/02
US CL : 380/44, 52; 713/194

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)
U.S. : 380/44, 52; 713/194

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 practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P --- Y,P	US 6233339 B1 (KAWANO et al) 15 May 2001 (15.05.2001), claims 9 and 10.	1-5 and 10-13 -------------------- 6-9 and 14-15
Y --- A	Schneier, B. Applied Cryptography. 1996, pages 44-46 and 589	6 - both 9s ----------------- 16
Y	Menezes, A.J. et al. The Handbook of Applied Cryptography. 1996, page 363.	14-15
A	US 5434917 A (NACCACHE et al.) 18 July 1995, abstract.	1-15
A	US 5412718 A (NARASIMHALU et al) 02 May 1995 (02.05.1995), abstract, figure 6A.	1-15

□ 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 application or patent 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

"&" document member of the same patent family

Date of the actual completion of the international search 20 June 2001 (20.06.2001)	Date of mailing of the international search report 31 JUL 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Tod Swann James R. Matthews Telephone No. (703) 305-3900

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/13504

Box I Observations where certain claims were found unsearchable (Continuation of Item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☒ Claim Nos.: 16
because they relate to subject matter not required to be searched by this Authority, namely:
Generating random numbers that are not put to a practical application is non-statutory.

2. □ Claim Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. □ Claim Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of Item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
Please See Continuation Sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. □ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. □ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. □ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest □ The additional search fees were accompanied by the applicant's protest.
□ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US01/13504

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION IS LACKING This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claims 1-15, is drawn to a secure data storage system.

Group II, claim 16, is drawn to a random number generation method.

The inventions listed as Groups I and II do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: they are classified differently and serve distinctly different purposes.