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

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2691789 C 2017/06/06

(11)(21) 2 691 789

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 2008/06/26
(87) Date publication PCT/PCT Publication Date: 2008/12/31
(45) Date de délivrance/Issue Date: 2017/06/06
(85) Entrée phase nationale/National Entry: 2009/12/23
(86) N° demande PCT/PCT Application No.: US 2008/068281
(87) N° publication PCT/PCT Publication No.: 2009/003080
(30) Priorité/Priority: 2007/06/26 (US60/946,224)

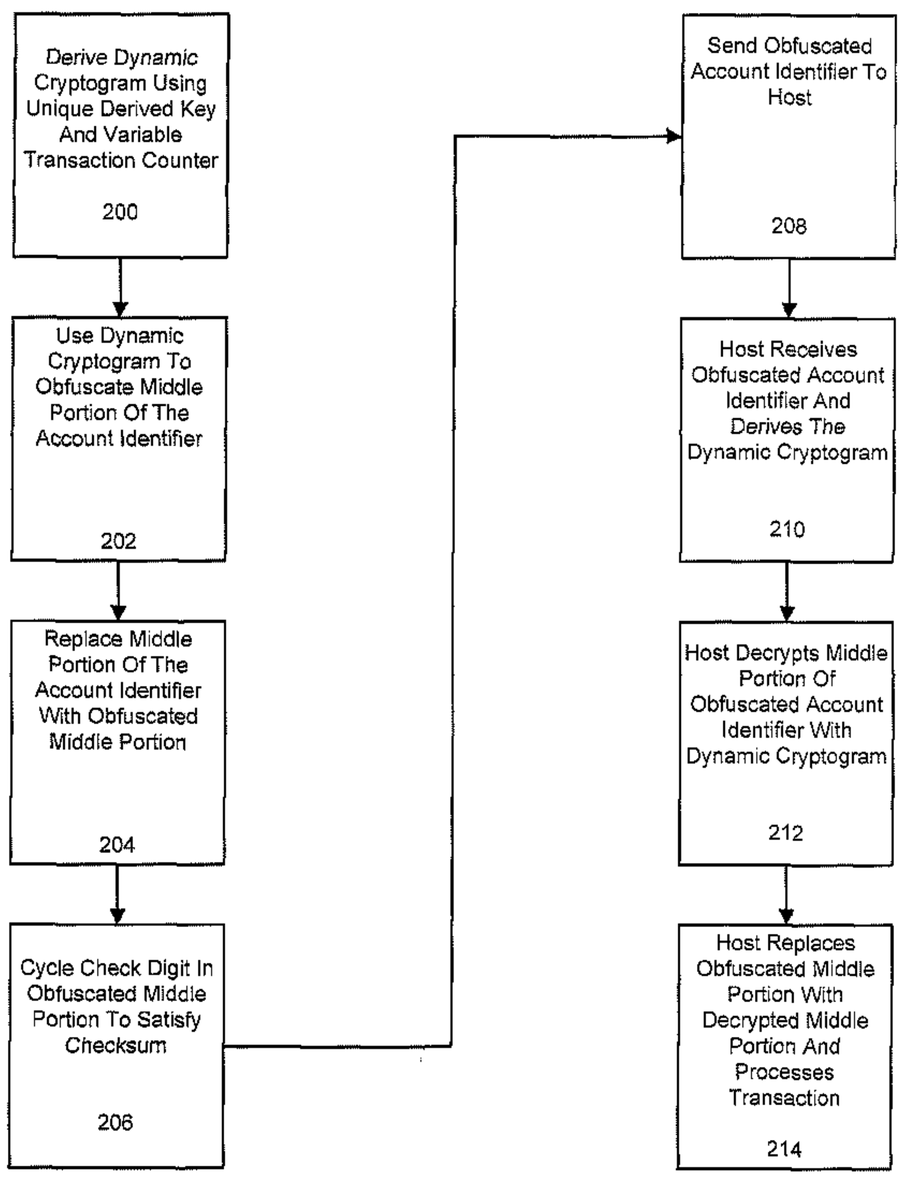
(51) Cl.Int./Int.Cl. *G06Q 20/40* (2012.01),
G06Q 20/34 (2012.01)

(72) Inventeurs/Inventors:
HURRY, SIMON, US;
AABYE, CHRISTIAN, US

(73) Propriétaire/Owner:
VISA U.S.A. INC., US

(74) Agent: BERESKIN & PARR LLP/S.E.N.C.R.L.,S.R.L.

(54) Titre : SYSTEME ET PROCEDE POUR L'OBSCURCISSEMENT D'IDENTIFIANT DE COMPTE
(54) Title: SYSTEM AND METHOD FOR ACCOUNT IDENTIFIER OBFUSCATION



(57) Abrégé/Abstract:
A method is disclosed. The method includes generating an obfuscated portion using a dynamic cryptogram unique to a transaction, where the dynamic cryptogram is determined using a uniquely derived key. The method also includes replacing a middle portion of the account identifier with the obfuscated portion to form an obfuscated account identifier.

Abstract

A method is disclosed. The method includes generating an obfuscated portion using a dynamic cryptogram unique to a transaction, where the dynamic cryptogram is determined using a uniquely derived key. The method also includes replacing a middle portion of the account identifier with the obfuscated portion to form an obfuscated account identifier.

SYSTEM AND METHOD FOR ACCOUNT IDENTIFIER OBFUSCATION

[0001] Blank

BACKGROUND

[0002] Embodiments of the present invention relate in general to payment transactions, and can apply to contactless smart card transactions involving credit or debit cards associated with an account identifier.

[0003] Generally, contactless smart cards are designed to provide a consumer with an efficient method of payment. The smart cards are able to transmit required information to the merchant's point of service (POS) device to complete the transaction by using, for instance, radio frequency (RF) or infrared (IR) signals. The merchant's POS device receives the transmitted information and processes the transaction.

[0004] Because contactless smart cards transmit information, security measures are needed to protect the consumer from sophisticated fraudsters who may intercept this information. To provide protection in transactions, a dynamic card verification value (dCVV) can be derived using an account identifier such as an account number. However, this is problematic because the entire account identifier is transmitted unencrypted as it is sent to an issuer associated with the card.

[0005] As a result, account information may still be intercepted. Intercepted account information can potentially be used to conduct fraudulent transactions.

[0006] One method of countering the theft of sensitive information is to encrypt any transmitted transaction or consumer data. Encryption generally involves encrypting transaction data at one end of a transmission with a key, and then regenerating the

original transaction data by decrypting the received encrypted data with the same key at the other end of the transmission. While encryption is effective in preventing information theft, an existing merchant infrastructure requires upgrading to be capable of processing a received encrypted signal from a smart card. Due to the cost, time, and risk of potential business interruption, many merchants, for example, resist making necessary upgrades to their procedures and systems.

[0007] Therefore, what is needed is a system and method for obscuring the account information in a manner that prevents an unauthorized user from using the account information. There is a further need for a system and method for obscuring the account identifier that does not require any changes to the installed terminal base or network infrastructure.

[0008] It would further be desirable to provide for the ability to authenticate a consumer's card without providing a separate dCVV value in an authentication request message. Authentication request messages contain a small amount of data, since they need to be quickly transmitted to the issuer for approval. If the dCVV value is not included in a dCVV data field in an authorization request message, other useful data could be included therein or less data would need to be transmitted to the issuer.

[0009] Embodiments of the invention address the above problems, and other problems, individually and collectively.

SUMMARY

[0010] Embodiments of the present invention are directed to methods, systems, and computer readable media that can be used to securely communicate an account identifier associated with a portable consumer device such as a contactless smart card from the portable consumer device or a POS terminal (or some other front-end location), to an issuer or some other service provider entity that wants to verify the authenticity of the portable consumer device. Advantageously, in embodiments of the invention, account information is communicated in a manner that is secure and that does not require updating the existing payment infrastructure in any significant way.

[0011] The secure account identifier may be referred to as an "obfuscated account identifier". In embodiments of the invention, the obfuscated account identifier has at least a portion of the account identifier encrypted before the account identifier arrives at the service provider (e.g., the issuer or a payment processing organization such as Visa™).

[0012] One embodiment of the invention provides a method for obfuscating an account identifier. The method comprises generating an obfuscated portion using a dynamic cryptogram, which is unique to a transaction. The dynamic cryptogram is determined using a unique derived key. Then, a middle portion of the account identifier is replaced with the obfuscated portion to form an obfuscated account identifier. This method may be performed by a portable consumer device or an access device at a merchant location.

[0013] Another embodiment of the invention is directed to a computer readable medium. The computer readable medium comprises code for generating an obfuscated portion using a dynamic cryptogram determined using a unique derived key. The computer readable medium further comprises code for replacing a middle portion of the account identifier with the obfuscated portion to form an obfuscated account identifier. A smart card may comprise this computer readable medium.

[0014] Another embodiment of the invention provides a method for decrypting an obfuscated account identifier. The method comprises generating a dynamic cryptogram unique to a transaction. The dynamic cryptogram is determined using a unique derived key. Next, a middle portion of an account identifier is generated using the dynamic cryptogram, and then an obfuscated portion of the obfuscated account identifier is replaced with the middle portion to form the account identifier. This method may be performed by a suitable entity such as a service provider.

[0015] Another embodiment of the invention is directed to a computer readable medium. The computer readable medium comprises code for generating a dynamic cryptogram unique to a transaction. The dynamic cryptogram is determined using a unique derived key. Next, a middle portion of an account identifier is generated using the dynamic cryptogram, and then an obfuscated portion of the obfuscated account identifier is replaced with the middle portion to form the account identifier. A server computer may comprise this computer readable medium.

[0016] These and other embodiments of the invention are described in further detail below, with reference to the Figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] Aspects, features, benefits and advantages of the embodiments of the present invention will be apparent with regard to the following description, appended claims and accompanying drawings where:

[0018] Fig. 1 shows a block diagram illustrating a transaction processing system according to an embodiment of the invention.

[0019] Fig. 2 shows a flow chart illustrating a method of communicating obfuscated account identifier information according to an embodiment of the invention.

[0020] Fig. 3 shows a flow chart illustrating the creation of a derived key according to an embodiment of the present invention.

[0021] Fig. 4 shows a flow chart illustrating the creation of a dynamic cryptogram according to an embodiment of the present invention.

[0022] Fig. 5 shows a flow chart illustrating the construction of an obfuscated account identifier according to an embodiment of the present invention.

[0023] Fig. 6 shows a flow chart illustrating the generation of the account identifier at the host according to an embodiment of the present invention.

[0024] Fig. 7 shows a schematic illustration of an exemplary record format including transaction data in a data field.

[0025] Fig. 8 shows an example illustrating an embodiment of a method of obfuscating an account identifier.

[0026] Fig. 9(a) shows a block diagram of a phone.

[0027] Fig. 9(b) shows an illustration of a payment card.

[0028] Fig. 10 shows a block diagram of a computer apparatus according to an embodiment of the invention.

DETAILED DESCRIPTION

[0029] As described above, in a conventional payment transaction, the consumer's account identifier is not encrypted when it passes from the consumer's portable consumer device or a POS terminal to a service provider such as an issuer. While encryption of the entire account identifier is possible, it may not be practical under all circumstances. If the account identifier is encrypted, a conventional transaction processing system may not be able to successfully process the transaction. For example, a typical account identifier includes a bank identification number (BIN). The BIN is used to route an authorization request message to the proper issuer or payment processor. If the account identifier is encrypted, then the BIN will change. If the BIN changes, then a proper authorization request message cannot be routed to the correct issuer.

[0030] Another restriction associated with encrypting the entire account identifier is related to the need to identify the account associated with a transaction. Consumers want to be able to identify which account is associated with a particular transaction, so merchants print account identifier digits on the purchase receipts. However, privacy and security laws like the federal Fair and Accurate Credit Transaction Act (FACTA) permit no more than five digits of the account identifier to be printed on a transaction receipt. Therefore, merchants typically print the last four digits of the account identifier on the receipt. Thus, if the account identifier is completely encrypted, any numbers printed on the receipt would be meaningless to consumers.

[0031] Another restriction associated with encrypting the entire account identifier is related to an error check that is associated with the sequence of digits in an account identifier. Error checking may be achieved using a checksum algorithm that determines if the digits of the account identifier are in the proper sequence. An example checksum algorithm is a modulo 10 algorithm (which is also known as a "Luhn check").

[0032] Therefore, encryption of an entire account identifier would corrupt at least the BIN, the checksum, and the ability to identify an account identifier via printed digits on a receipt. In addition, for encryption to be successful, merchants would have to upgrade their POS terminals with appropriate encryption keys, which is burdensome.

[0033] The obfuscation process according to embodiments of the invention can be used to protect the account identifier without the need to upgrade the merchant infrastructure to accommodate encryption of the entire account identifier. As will be illustrated in further detail below, embodiments of the invention obfuscate only a portion of an account identifier, which allows the BIN and the last four digits identifying the account to remain unencrypted. In addition, embodiments of the invention can also be used with account identifiers of varying length.

[0034] In one embodiment of the invention, a portion of a transmitted account identifier is obfuscated (or changed) by a contactless smart card. A smart card, also called a chip card or IC (integrated circuit) card, is a pocket-sized card with embedded circuitry. Associated with the smart card is an account identifier. An account identifier may be used by a host (e.g., a server computer at an issuer or payment processing organization) to associate an account with a cardholder. In a preferred embodiment, the account identifier consists of 16 decimal digits. In an embodiment, the first six digits of the account identifier comprise the BIN. Digits 7-15 typically form the account number. Digit 16 may be used for a checksum, created using, for example, the Luhn check algorithm. An expiration date may additionally be stored on the smart card. In a preferred embodiment, the expiration date is represented by 4 decimal digits in a YYMM format, wherein YY indicates a year of the expiration date and MM indicates a month of the expiration date.

[0035] A number of elements may be stored on the smart cart. In one embodiment, a key is also stored on the smart card. This key, derived from a master key and written to the smart card during personalization, is stored on the smart card at or before issuance to a cardholder, and is preferably known to or derivable by an issuer. In some embodiments, the account identifier, expiration date, and key remain static from transaction to transaction (at least until a new card is issued). In addition to the key, a transaction counter (TC) may also be stored on the smart card. In one example, the TC is a 16 bit value, and is incremented for each transaction. However, other TC update operations are possible, such as daily incrementing, or incrementing or decrementing by a value other than 1, or incrementing or decrementing by a variable value.

[0036] An embodiment of the present invention randomly obfuscates the middle five digits of an account identifier while maintaining the integrity of the first six digits (i.e., the BIN) and last four digits of the account identifier, as well as the check digit for the Luhn check. Instead of a BIN, a merchant location identifier, financial institution location identifier, or even an Internet Protocol (IP) address could be part of the account identifier and can remain static. The middle five digits of the account identifier are obfuscated because five obfuscated digits provide sufficient security, while still allowing the BIN and the last four digits of the account identifier to be in the clear when the account identifier information is transmitted from a merchant to an issuer or other service provider. As previously mentioned, this is advantageous, as it is therefore not necessary to regenerate the middle five digits of the account identifier before routing the transaction to the appropriate issuer, if such routing is required. This is further advantageous in that the last four digits of the account identifier may appear on a consumer's receipt. The consumer will not notice any change from conventional transaction receipts.

[0037] Although obfuscating five digits provides a certain measure of security, a further measure of security is gained because the obfuscated portion changes with each transaction. This is advantageous because even if the account identifier is skimmed, the number gained will be useless because it will be invalid if used in a subsequent transaction. Furthermore, a sixth middle digit also provides security. The sixth middle digit is selected to satisfy the Luhn check of the account identifier after the middle five digits have been obfuscated. Thus, there is a total of six digits in a preferred embodiment that are obfuscated. The middle portion can vary in length, either shorter or longer.

[0038] FIG. 1 shows a system that can be used in an embodiment of the invention. The system includes a merchant **114** and an acquirer **116** associated with the merchant **114**. The acquirer **116** communicates with an issuer **120** via a payment-processing network **118**. The acquirer **116** is typically a bank that has a merchant account. The issuer **120** may also be a bank, but could also be a business entity such as a retail store. Some entities are both acquirers and issuers, and embodiments of the invention include such entities. The issuer **120** may include a server computer **122** and a database **124**.

[0039] The consumer **100** may be an individual or an organization such as a business that is capable of purchasing goods and services.

[0040] The portable consumer device **102** may comprise a radio-frequency contactless element **104**. The radio-frequency contactless element **104** may include a computer chip (not shown) configured to store a transaction counter, an account identifier, an expiration date, and encryption keys. The radio-frequency contactless element **104** is configured to determine and transmit an obfuscated account identifier. Examples of portable consumer devices include contactless smart cards such as credit or debit cards, wireless phones, PDAs (personal digital assistants), key fobs, etc. Other examples of portable consumer devices are provided below.

[0041] The merchant **114** in FIG. 1 has an access device **106** located at the merchant **114**, but the access device **106** may be located at any other suitable location in other embodiments of the invention. The access device **106** may include a reader **108**, a processor **110**, and a computer readable medium (CRM) **112**. Examples of access devices include point of sale (POS) terminals, cellular phones, personal digital assistants (PDAs), personal computers, handheld specialized readers, set-top boxes, electronic cash registers, automated teller machines (ATMs), virtual cash registers, kiosks, security systems, access systems, and the like.

[0042] The payment processing network **118** may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. The payment processing network **118** may include a server computer. A server computer is typically a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The payment processing network **118** may use any suitable wired or wireless network, including the Internet.

[0043] One embodiment of the invention provides a method for obfuscating an account identifier. The method comprises generating an obfuscated portion using a dynamic cryptogram, which is unique to each transaction. The dynamic cryptogram is determined using a unique derived key. Then, a middle portion of the account identifier is replaced with the obfuscated portion. In some embodiments, the

obfuscated portion may be determined using all or part of the dynamic cryptogram, using one or more data alteration method (e.g., encryption methods). In other embodiments, the obfuscated portion could be some part or all of the dynamic cryptogram. The method may be performed by a portable consumer device or an access device at a merchant location

[0044] FIG. 2 shows a flowchart illustrating a method of obfuscating (or encrypting) and unobfuscating (or decrypting) the account identifier. In this embodiment, the dynamic cryptogram, unique to the instant purchase, is determined using a unique derived key and a variable transaction counter (step **200)**. After the dynamic cryptogram is determined, it is then used to generate an obfuscated middle portion i.e. to obfuscate a middle portion of the account identifier (step **202**). The obfuscated middle portion is used to replace the middle portion of the account identifier (step **204**). In some embodiments, because the new obfuscated middle portion changes a prior checksum calculation (e.g., a Luhn check), a new check digit is determined. In some embodiments, one of the middle digits is cycled from a value of 0-9 until the checksum is validated (step **206**). After the checksum has been validated with the new check digit, the obfuscated account identifier is transmitted to the host (e.g., a server computer at a service provider) (step **208**).

[0045] Upon receiving the obfuscated account identifier, the host determines a dynamic cryptogram using a unique derived key (step **210**). The dynamic cryptogram is used to unobfuscate the middle obfuscated portion of the received account identifier (step **212**). Upon generating the middle portion, the host then replaces the obfuscated middle portion with the newly generated middle portion to form the account identifier (step **214**). The host can then verify if the unencrypted account identifier is valid. If it is not valid, a fraud alert can be set. A fraud alert may make the host, the merchant, and/or the user aware that unauthorized use of an account identifier may be occurring. The alert may comprise any number of solutions such as an e-mail, phone call, instant message, internet communication, or combination of methods suitable for alerting a party of potential fraud.

[0046] A method for obfuscating an account identifier by replacing several digits of the account identifier with cryptographically derived digits is disclosed with reference to FIG. 3. FIG. 3 illustrates the process of creating a unique derived key, which may

be used to create a transaction-specific cryptogram according to a preferred embodiment. A unique derived key is the result of an encryption process that encrypts unique inputs with a master key. An example encryption process is triple data encryption standard (3DES). Other methods for forming uniquely derived keys may be found in U.S. Patent Application No. 10/642,878, filed on August 18, 2003 to Sahota et al., which is herein incorporated by reference in its entirety for all purposes.

[0047] Referring to FIG. 3, first, the account identifier is converted from decimal digits to hexadecimal (step **300**). Then, the first six and last four digits of the account identifier, with each decimal digit represented in hexadecimal, are concatenated with the expiration date (step **302**). The expiration date is represented by four digits. Each hexadecimal digit can be equivalent to 4 bits or half a byte. Therefore, the result of the concatenation can be a 7 byte value (e.g., 6 digits for the account identifier, 4 digits for the last four digits of the account identifier, and 4 digits for the expiration date is equal to 14 digits, where each digit is half of a byte).

[0048] In the preferred method, a triple DES (3DES) encryption algorithm, which can use a 16 byte input value, is used. To generate the 16 byte value, the 7 byte value created above can be concatenated with hexadecimal digits FF (1 byte) in order to pad the value out to 8 bytes (step **304**). Now that half (8 bytes) of the input to the 3DES operation is created, this value is then inverted to create another 8 byte value to serve as the second half of the 3DES input (step **306**). To invert the 8 byte value, the value is converted to binary, and then each binary digit is swapped. For example, if the result (in binary) is 11010011, then the inverted result would equate to 00101100. The inverted 8 byte value is converted to hexadecimal and concatenated to the original 8 byte value to form a 16 byte value acceptable for a 3DES operation (step **308**). This 16 byte quantity is then input into a 3DES operation as the message (step **310**).

[0049] The key for this 3DES operation is a master key. The master key may be either sixteen or twenty-four bytes depending on the variant of DES selected (e.g., using two different keys (2TDES) or three different keys (3TDES)). The output of this 3DES operation is a double-length sixteen byte unique derived key. A master key may be unique to each issuer, and generally, the master key is only known by

the issuer to provide security. Therefore, as is apparent, the derived key need not be calculated at transaction-time, but instead may be calculated at or before issuance of a portable consumer device to a cardholder. If the derived key is calculated at or before card personalization, the master key need not be stored on the card, resulting in increased security.

[0050] FIG. 4 illustrates the creation of the dynamic cryptogram to be used in obfuscating the middle digits of the account identifier according to one embodiment. To prevent the unauthorized use of the obfuscated account identifier by a potential skimmer, the middle portion of the obfuscated account identifier is varied with each transaction. In order to provide the unique obfuscated digits for each transaction, the cryptogram used to generate the obfuscated digits can vary with each transaction. When a consumer wants to conduct a transaction, the TC is concatenated with the expiration date (step **400**). As explained before, the TC changes with each transaction, and if this changing value is used to determine the cryptogram, the cryptogram will also change with each transaction. Alternatively, another variable data element (e.g. a time stamp) could be used instead of or in addition to the TC to provide the dynamic cryptogram.

[0051] The dynamic cryptogram can be generated using the same 3DES operation used in the creation of the unique derived key. The key for this operation is the unique derived key, and the input can be a 16 byte value. The TC can be a 2 byte value and the expiration date can be a 2 byte value. Thus, to generate an 8 byte value that can be inverted and concatenated with the original 8 byte value (as explained with reference to FIG. 3), 4 bytes of padding are also concatenated (step **402**). In some embodiments, the expiration date is concatenated with the TC, and is then padded out to eight bytes with hexadecimal (FFFF FFFF). This eight byte value is then inverted (step **404**). The inverted value is then concatenated with the original value to form a 16 byte input value suitable for a 3DES operation (step **406**). The 3DES operation uses this input and the unique derived key to determine the cryptogram that will be used to uniquely obfuscate the middle portion of the account identifier (step **408**).

[0052] It is to be understood that the above described method of constructing a cryptogram is illustrative, and is not intended to be limiting. For instance, it is

possible to use ciphers other than 3DES. It is further possible to use inputs to the cipher other than those inputs used above. Further, it is not necessary to derive a key, as the master key may be used in lieu of the derived key. One of ordinary skill in the art will understand that additional modifications are possible while remaining within the scope of the present invention.

[0053] FIG. 5 illustrates the derivation of five decimal digits to replace five decimal digits of the account identifier according to an embodiment of the invention. FIG. 5 further illustrates the creation of an obfuscated account identifier that is sixteen digits long.

[0054] First, each of digits 7-11 of the account identifier is converted into hexadecimal, resulting in a three byte hex value when zero-filled on the left (step **500**). For example, if the middle digits are (99999), then the decimal conversion would be (1001 10011001 10011001), which is 4 bits short of a full 3 bytes since there are only 5 digits (2 digits = 1 byte). Thus, zero filling on the left creates a full 3 byte value: (00001001 10011001 10011001) or (099999) in hexadecimal.

[0055] Then, this three byte hex value is bitwise XORed with two bytes of the cryptogram, zero-filled on the left to expand the cryptogram out to three bytes (step **502**). In an embodiment, the last two bytes of the cryptogram are used for this XOR operation, the result of which is a three byte raw value. If the resulting raw value is greater than a first constant (1869F) (step **504**), an overflow flag is set (step **506**). Hexadecimal (1869F), converted to decimal is (99999), which is the largest number that can replace the five middle digits. Anything larger would result in six digits. Therefore, if the result is larger, the overflow flag is set, and a second constant, hexadecimal (186A0) (which in decimal equates to 100000), is subtracted from the raw value to limit the result to five digits (step **508**). The overflow flag is preferably placed in a field associated with the account identifier called the dynamic card verification value (dCVV). If the result of the XOR operation is equal to or less than hexadecimal (1869F), then no overflow flag is set and the operation proceeds directly from step **504** to step **510**.

[0056] The dCVV field is used to store the overflow flag because in some embodiments, the dCVV value is not needed. Typically, the dCVV value provides extra security in standard transactions as it is used by an issuer or other service

provider to authenticate a portable consumer device such as a smart card. However, the function of the dCVV is replaced by the obfuscated portion, because the obfuscated portion provides greater security that the dCVV value provides. The dCVV value is three digits. Because the obfuscated portion is preferably at least five digits in embodiments of the invention, the obfuscated portion provides increased security over the dCVV value. Longer verification values generally provide greater security than shorter values. Additionally, since the dCVV data field in an authorization request message is used to store, for example, an overflow flag, no alteration or modification of existing software or hardware is required to perform embodiments of the invention.

[0057] FIG. 7 illustrates an example of transaction data in a record format as it would be present in various data fields including a dCVV data field **712**. The transaction data may be stored in a memory in a portable consumer device such as a smart card.

[0058] In FIG. 7, an account identifier **700** occupies the first 16 digits. Next, a separator **702** provides a buffer between the account identifier **700** and the expiration date **704**. The service code **706** follows the expiration date **704**. Then, a personal identification number (PIN) verification indicator (PVKI) **708** and the PIN verification data **710** follow. Finally, the dCVV field **712**, the transaction counter **714**, a contactless indicator **716**, and padding **718** complete the data fields.

[0059] Returning to FIG. 5, the resulting value from either step **504** or step **508** is converted into a five digit decimal number (step **510**). This five digit decimal number is intended to replace digits 7-11 of the account identifier. The first six digits of the account identifier are concatenated with the five digit decimal number and the last four digits of the account identifier (step **512**). This results in the obfuscated account identifier.

[0060] Then, digit 12 (or another digit) is then cycled (0 through 9) until a value is found such that a checksum of the obfuscated account identifier matches the checksum of the original account identifier. The original value of digit 12 is stored in the dCVV field with the overflow flag (step **516**). Because digit 12 (or some other digit) may be changed to satisfy the checksum, this also contributes to the obfuscation of the middle digits. The obfuscated account identifier, expiration date,

TC, and dCVV field are then transmitted, unencrypted, to the host as part of a transaction (step **518**). As is apparent, the first six digits and last four digits of the obfuscated account identifier are identical to the first six digits and last four digits of the account identifier. This is desirable in some circumstances because, in some payment networks, the first six digits serve to route the message to the correct issuer. Further, the last four digits may appear on a customer's receipt to identify the card used in the transaction.

[0061] FIG. 6 illustrates the generation of the account identifier from the obfuscated account identifier in a preferred embodiment. The account identifier may be generated by the host from the obfuscated account identifier, the transaction counter, and the information in the dCVV field, namely the original twelfth digit, and the overflow flag.

[0062] Upon receiving a number that appears to be an account identifier or an obfuscated account identifier, the host may determine whether the received number is first a valid account identifier or whether the host may need to generate the account identifier from the received number using the method described in FIG. 6. As is apparent, if the received number is a valid account identifier, then applying the method in FIG. 6 would result in an invalid account identifier. In one embodiment, the host may attempt to process the received number as a valid account number, and if the received number fails, then apply the method of FIG. 6. Alternatively, a field associated with the account identifier may store an indicator that the received number is an obfuscated account identifier. Numerous other methods could be used to indicate to a host that the received number is obfuscated.

[0063] In addition, once the host determines that the received number is an obfuscated account identifier, the host may determine which digits comprise the obfuscated portion of the obfuscated account identifier if this information is not known in advance by the host. For example, in one embodiment, a smart card could randomly select which middle digit will be the check digit. Preferably, digits 7-11 serve as the obfuscated portion with digit 12 being the new check digit. However, to provide added security, the check digit, for example, could be randomly chosen among digits 7-12 to be digit 8 leaving digits 7, and 9-12 to be obfuscated. In another example, instead of digits 7-12, digits 7, 9, and 12 might be chosen to be

obfuscated. Advantageously, this provides additional security because even if a fraudster could decode obfuscated digits, the fraudster would still need to know which digits to decode. A field associated with the account identifier may store an indicator as to which digits are obfuscated.

[0064] Referring to Fig. 6, first, each of digits 7-11 of the obfuscated account identifier can be converted to hexadecimal, resulting in a three byte hexadecimal value (step **600**). Then, a unique derived key is calculated as described above with respect to Fig. 3 (step **602**). This unique derived key can be calculated using the first six and last four digits of the obfuscated account identifier (which, as is apparent, are identical to the first six and last four digits of the account identifier). The unique derived key can be identical to the derived key discussed above with respect to Fig. 3. Then, a cryptogram is calculated as described above with respect to Fig. 4 (step **604**). This cryptogram is calculated using the TC, expiration date, and derived key. Once again, this cryptogram is identical to the cryptogram discussed above with respect to Fig. 4.

[0065] If the overflow flag is set in the dCVV field (step **606**), then hexadecimal value 186A0 is added to the three byte value determined in step **600** (step **608**). Otherwise, the method proceeds to step **610** where the three byte hexadecimal value is bitwise XORed with the last two bytes of the cryptogram to form a raw value. Then, the raw value of the XOR operation is converted to five decimal digits (step **612**). These five decimal digits are identical to digits 7-11 of the account identifier. Finally, the first six digits of the obfuscated account identifier, the five decimal digits, the original twelfth digit (received in the dCVV field), and the last four digits of the obfuscated account identifier are concatenated together to form the account identifier at the host (step **614**). If the result of this process is not a valid account identifier or otherwise indicates a fraudulent attempt to complete a transaction, then the host may set a fraud alert.

[0066] In some embodiments, in order to reduce the processing load at the host at the expense of memory usage, instead of regenerating digits 7-11 of the account identifier at the host, a lookup table may be used. In an embodiment, the obfuscated account identifier may be an entry, preferably created at issuance, in a lookup table corresponding to digits 7-11 of the account identifier. The entry may be created by

iterating, at issuance, through the process outlined in Figs. 1-3 to generate the obfuscated account identifier at the host and placing an entry in the lookup table corresponding to the same.

[0067] In the manner shown above, a host may regenerate an account identifier from an obfuscated account identifier. Further, the obfuscated account identifier may be transmitted unencrypted without fear of compromising the account identifier. Further, the format of data transmitted from the smart card to the host, often by means of a terminal at a point of sale, including the obfuscated account identifier, expiration date, and dCVV field (containing an overflow flag and the original twelfth digit) is compatible with the installed terminal base.

[0068] As is apparent, there is no way to directly derive the account identifier from the data sent from the smart card to the host (i.e., the obfuscated account identifier, transaction counter, expiration date, and dCVV) without knowledge of the master key or derived key, or a brute force replacement of the digits 7-11 of the obfuscated account identifier. Although a brute force attack on five decimal digits would be a relatively simple brute force attack, this attack must be launched against the host. Therefore, the systems and methods described herein should preferably be combined with a brute force attack detection system located at the host. Thus, this attack is easily detected and thus thwarted.

[0069] Referring to FIG. 1 in an exemplary embodiment, a consumer **100** may purchase goods or services at the merchant **114** using a portable consumer device **102**, such as a contactless smart card or credit card. The portable consumer device **102** interacts via the radio-frequency transponder **104** with the reader **108** of the access device **106**, such as a POS terminal, at the merchant **114** in a contactless manner. During the interaction, the portable consumer device **102** determines an obfuscated account identifier and transmits, via the radio-frequency transponder **104**, the obfuscated account identifier to the reader **108** of the access device **106** at the merchant **114**.

[0070] FIG. 8 illustrates an exemplary determination of the obfuscated account identifier using the methods disclosed above. In this example, an original account identifier **802** is obfuscated to yield an obfuscated account identifier **800**. Digits 1-6 of the account identifier represent the BIN **804**. Digits 13-16 are the digits used by

the consumer to identify the consumer's account **810**. Digits 7-11 **806** represent the obfuscated portion. Digit 12 **808** is changed to satisfy the checksum calculation with the obfuscated account identifier.

[0071] The first step that is performed by the portable consumer device **102** is to determine a unique derived key as disclosed in Fig. 3. The unique derived key is unique because it is based on the first six and last four digits of the original account identifier. In this example, those digits would be (432101) and (1234). Using the unique derived key, a dynamic cryptogram can be determined as disclosed in FIG. 4. In this example, a value of (FFFD) is used for the dynamic cryptogram **816**.

[0072] Next, applying the method disclosed in Fig. 5 and with reference to Figs. 1 and 8, step **500** converts digits 7-11 of the original account identifier to hexadecimal. The original digits are (86066), and when converted to hexadecimal, the result is (015032) **812**. In step **502**, hexadecimal digits **812** are used in an Exclusive-OR (XOR) operation with the previously calculated cryptogram (FFFD) **816**. The result of the XOR operation is hexadecimal (1AFCF) **822**. The digital equivalent of (1AFCF) is (110543) **818**. Referring to step **504**, because (1AFCF) is greater than (1869F) (decimal equivalent = 99999), an overflow flag is set **506**, and the result **822** is reduced by a fixed value of (186A0) (decimal equivalent = 100000) in step **508** to yield (292F). Step **510** converts hexadecimal (292F) to decimal equivalent (10543) **820**. These digits represent the obfuscated account portion of the account identifier, and in step **512,** they replace digits (86066) of the original account identifier as shown in obfuscated account identifier **800**. Finally, step **514** cycles digit 12 until a value is found that satisfies the Luhn check using digits (10543) in place of the original (86066) digits. In this example, digit 12 needs to be set to 7, so the original value of 1 is stored in a dCVV field as indicated by step **516**, and digit 12 is replaced with a 7. Thus, the resulting obfuscated account identifier **800** is (4321 0110 5437 1234). This number is transmitted (step **518**), for example, from the portable consumer device **102** to the merchant's access device **106**. In this example, only a designated party with a valid master key will be able to decrypt this obfuscated account identifier and determine the original account identifier (4321 0186 0661 1234) using the method disclosed in FIG. 6.

[0073] Once the merchant **114** receives the obfuscated account identifier, it is transmitted in an authorization request message (which may include a transaction amount, merchant category code, etc.) to the issuer **120** via the acquirer **116** and the payment processing network **118**. Once the authorization request is received by the issuer **120**, the issuer's server **122** (which can serve as the previously described "host") can retrieve information from the database **124** to determine the original account identifier using the received obfuscated account identifier. If the original account identifier is valid, then the issuer **120** may determine if there are sufficient funds or credit in the consumer's account to conduct the current transaction. If there are insufficient funds or credit, an authorization response message indicating that the transaction is not approved is sent back to the access device **106** via the acquirer **116**, and the payment processing network **118**. If there are sufficient funds or credit, then the authorization response message would indicate that the transaction is approved. A clearing and settlement process can then occur at the end of the day.

[0074] Some variations are also possible. For example, instead of the issuer **120**, the payment processing network **118** could serve as the host which determines the original account number from the unobfuscated account number. Also, in some embodiments, the access device **106** could generate the obfuscated account number instead of the portable consumer device **102**. In these embodiments, the portable consumer device **102** could simply pass consumer information such as an account number and expiration date to the access device **106**, and the access device may determine the obfuscated account number as described above. Further, although the embodiments described above are in the context of a "card present" type of transaction where a consumer is using a portable consumer device to conduct a transaction at a merchant with a physical location, it is understood that embodiments of the invention may also be used in "card not present" situations where a computer terminal is transmitting an obfuscated account number to a host.

[0075] Note that in the embodiments just described with reference to Fig. 1, and other Figures, the determination of the original account identifier at the host not only provides the original account identifier at the host, but also authenticates the portable consumer device **102** without using a separate dCVV. This is because the obfuscated portion of the obfuscated account identifier is derived from a transaction counter, which can be used to determine if the correct transaction is being

conducted. For instance, if the host correctly determines the original account number from the obfuscated account number, then the transaction counter at the host would match the transaction counter on the portable consumer device. This would indicate that the portable consumer device is authentic and that no skimming has taken place. Conversely, if the host cannot determine the original account number from the obfuscated account number, then the host may determine that the data has been skimmed. The transaction counter used to form the obfuscated portion of the obfuscated account number and the transaction counter at the host would not match in this case, thus, indicating possible skimming. Some embodiments of the invention can be advantageously conducted without using a 3 digit dCVV. Embodiments of the invention advantageously allow for the secure transmission of data from a front end to a back end of a transaction, while also providing for an effective way to authenticate a device (e.g., a portable consumer device) at a front end of the transaction.

[0076] Other embodiments of the invention are also possible which do not require any processing on a smart card or other portable consumer device. In an embodiment, the smart card does not store the account identifier, even though the account identifier may be embossed on the card. Rather, the smart card stores two numbers. The first is a masked account identifier, identical to the account identifier except for the fact that digits 7-12 are masked out, preferably with zeros, and that digit 12 is recalculated to satisfy the Luhn check. This masked account identifier may be stored on the smart card where an account identifier would typically be stored. Further, digits 7-12 of the account identifier are encrypted, preferably using 3DES and a master key known only to the host, to create an account identifier cryptogram, 64 bits long if 3DES is used. Encrypted digits 7-12 are also stored on the smart card, preferably in a supplemental data field.

[0077] When a contactless transaction takes place, the card reader (or other access device) reads both the masked account identifier and the account identifier cryptogram, and sends the masked account identifier and the account identifier cryptogram, together with other transaction information, to the host for authorization. At the host, the master key is used to decrypt the encrypted account identifier, thereby regenerating digits 7-12 of the account identifier, which may then be combined with digits 1-6 and 13-16 of the masked account identifier to regenerate

the account identifier. If the host is also the issuer, the host then performs the authorization, and sends a response to the reader at a point of sale. If the host is not the issuer (but is instead, for example, a payment service), then the account identifier may be forwarded to the appropriate issuer for authorization. Thus, this encryption would be transparent to the issuer authorization process.

[0078] This alternative method of obfuscating an account identifier has some advantages over the earlier solution. For instance, there need be no calculations performed on the smart card, and no key stored on the smartcard. Further, the issuer need not change its authorization procedures.

[0079] It is to be understood that there are a number of ways in which an account identifier may be obscured while still remaining within the scope of the present invention. For instance, rather than using a 3DES operation to generate the cryptogram and the derived key, other block ciphers or cryptographic transformations may be used.

[0080] Examples of portable consumer devices and computer apparatuses that can be used in embodiments of the invention are described below.

[0081] FIGS. 9(a)-9(b) show block diagrams of portable computer devices and subsystems that may be present in computer apparatuses in systems according to embodiments of the invention.

[0082] The portable consumer device **102** (shown in FIG. 1) may be in any suitable form. For example, suitable portable consumer devices can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart cards, ordinary credit or debit cards (with a magnetic strip and without a microprocessor), keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of portable consumer devices include cellular phones, personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, and the like. The portable consumer devices can also be debit devices (e.g., a debit card), credit devices (e.g., a credit card), or stored value devices (e.g., a stored value card).

[0083] An exemplary portable consumer device **32'** in the form of a phone may comprise a computer readable medium and a body as shown in FIG. 9(a). (FIG. 9(a) shows a number of components, and the portable consumer devices according to embodiments of the invention may comprise any suitable combination or subset of such components.) A computer readable medium **32(b)** may be present within a body **32(h)**, or may be detachable from it. The body **32(h)** may be in the form of a plastic substrate, housing, or other structure. The computer readable medium **32(b)** may be a memory that stores data and may be in any suitable form including a magnetic strip, a memory chip, uniquely derived keys (such as those described above), encryption algorithms, etc. The memory also preferably stores information such as financial information, transit information (e.g., as in a subway or train pass), access information (e.g., as in access badges), etc. Financial information may include information such as bank account information, bank identification number (BIN), credit or debit card number information, account balance information, expiration date, consumer information such as name, date of birth, etc. Any of this information may be transmitted by the portable consumer device **32'**.

[0084] Information in the memory may also be in the form of data tracks that are traditionally associated with credits cards. Such tracks include Track 1 and Track 2. Track 1 ("International Air Transport Association") stores more information than Track 2, and contains the cardholder's name as well as account number and other discretionary data. This track is sometimes used by the airlines when securing reservations with a credit card. Track 2 ("American Banking Association") is currently most commonly used. This is the track that is read by ATMs and credit card checkers. The ABA (American Banking Association) designed the specifications of this track and all world banks must abide by it. It contains the cardholder's account, encrypted PIN, plus other discretionary data.

[0085] The portable consumer device **32'** may further include a contactless element **32(g)**, which is typically implemented in the form of a semiconductor chip (or other data storage element) with an associated wireless transfer (e.g., data transmission) element, such as an antenna. Contactless element **32(g)** is associated with (e.g., embedded within) portable consumer device **32'** and data or control instructions transmitted via a cellular network may be applied to contactless element **32(g)** by means of a contactless element interface (not shown). The contactless element

interface functions to permit the exchange of data and/or control instructions between the mobile device circuitry (and hence the cellular network) and the optional contactless element **32(g)**.

[0086] Contactless element **32(g)** is capable of transferring and receiving data using a near field communications ("NFC") capability (or near field communications medium) typically in accordance with a standardized protocol or data transfer mechanism (e.g., ISO 14443/NFC). Near field communications capability is a short-range communications capability, such as RFID, Bluetooth™, infra-red, or other data transfer capability that can be used to exchange data between the portable consumer device **32'** and an interrogation device. Thus, the portable consumer device **32'** is capable of communicating and transferring data and/or control instructions via both cellular network and near field communications capability.

[0087] The portable consumer device **32'** may also include a processor **32(c)** (e.g., a microprocessor) for processing the functions of the portable consumer device **32'** and a display **32(d)** to allow a consumer to see phone numbers and other information and messages. The portable consumer device **32'** may further include input elements **32(e)** to allow a consumer to input information into the device, a speaker **32(f)** to allow the consumer to hear voice communication, music, etc., and a microphone **32(i)** to allow the consumer to transmit the consumer's voice through the portable consumer device **32'**. The portable consumer device **32'** may also include an antenna **32(a)** for wireless data transfer (e.g., data transmission).

[0088] If the portable consumer device is in the form of a debit, credit, or smartcard, the portable consumer device may also optionally have features such as magnetic strips. Such devices can operate in either a contact or contactless mode.

[0089] An example of a portable consumer device **32"** in the form of a card is shown in FIG. 9(b). FIG. 9(b) shows a plastic substrate **32(m)**. A contactless element **32(o)** for interfacing with an access device **34** may be present on or embedded within the plastic substrate **32(m)**. A consumer information region **32(p)** may include information such as an account number, expiration date, and consumer name, which may be printed or embossed on the card. Further, a magnetic strip **32(n)** may also be on the plastic substrate **32(m)** and may be an example of a computer readable medium. In this embodiment, the portable consumer device **32"**

may or may not have a processor. If it does not, then a corresponding access device may be used to form a dynamic verification value using information stored on the magnetic strip 32(n).

[0090] As shown in FIG. 9(b), the portable consumer device 32" may include both a magnetic strip 32(n) and a contactless element 32(o). In other embodiments, both the magnetic strip 32(n) and the contactless element 32(o) may be in the portable consumer device 32". In other embodiments, either the magnetic strip 32(n) or the contactless element 32(o) may be present in the portable consumer device 32".

[0091] The various participants and elements in FIG. 1 may operate one or more computer apparatuses to facilitate the functions described herein. Any of the elements in FIG. 1 may use any suitable number of subsystems to facilitate the functions described herein. Examples of such subsystems or components are shown in FIG. 10. The subsystems shown in FIG. 10 are interconnected via a system bus 775. Additional subsystems such as a printer 774, keyboard 778, fixed disk 779 (or other memory comprising computer readable media), monitor 776, which is coupled to display adapter 782, and others are shown. Peripherals and input/output (I/O) devices, which couple to I/O controller 771, can be connected to the computer system by any number of means known in the art, such as serial port 777. For example, serial port 777 or external interface 781 can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus allows the central processor 773 to communicate with each subsystem and to control the execution of instructions from system memory 772 or the fixed disk 779, as well as the exchange of information between subsystems. The system memory 772 and/or the fixed disk 779 may embody a computer readable medium.

[0092] Any of the above described steps may be embodied as computer code on a computer readable medium. The computer readable medium may reside on one or more computational apparatuses and may use any suitable data storage technology.

[0093] Embodiments of the present invention can be implemented in the form of control logic in software or hardware or a combination of both. The control logic may be stored in an information storage medium as a plurality of instructions adapted to direct an information processing device to perform a set of steps disclosed in embodiment of the present invention. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will appreciate other ways and/or methods to implement the present invention.

[0094] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++, or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0095] Although preferred embodiments of the invention have been disclosed for illustrative purposes, those skilled in the art will appreciate that many additions, modifications, and substitutions are possible and that the scope of the claims should not be limited by the embodiments set forth herein, but should be given the broadest interpretation consistent with the description as a whole.

[0096] A recitation of "a", "an", or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0097] None of the patents, patent applications, publications, and descriptions mentioned above are admitted to be prior art.

Replacement Claims for CA Patent Application No. 2,691,789
Agent Ref. No. 5985-P36240CA00

WHAT IS CLAIMED IS:

1. A method for obfuscating an account identifier comprising:

determining a dynamic cryptogram unique to a transaction using a unique derived key, wherein the unique derived key is determined based upon a first end portion of the account identifier and a second end portion of the account identifier;

generating an obfuscated portion using the dynamic cryptogram; and

replacing a middle portion of the account identifier with the obfuscated portion to form an obfuscated account identifier, wherein the middle portion of the account identifier excludes the first end portion and the second end portion.

2. The method of claim 1, wherein the second end portion comprises five characters or less.

3. The method of claim 1 or 2, further comprising:

changing a check digit of the obfuscated account identifier from a first value to a second value, wherein the check digit is exclusive of the first end portion, the second end portion, and the obfuscated portion, and wherein the first value is stored in a verification field associated with the account identifier.

4. The method of claim 3, wherein the second value satisfies a checksum calculation of the obfuscated account identifier.

5. The method of any one of claims 1 to 4, wherein the unique derived key is further determined based upon using a master key.

6. The method of any one of claims 1 to 5, wherein the dynamic cryptogram is further determined using a variable transaction counter and an expiration date.

7. The method of any one of claims 1 to 6, wherein the generation of the obfuscated portion comprises:

converting the middle portion to hexadecimal digits;

performing an Exclusive-OR (XOR) operation on the hexadecimal digits and the dynamic cryptogram to form a raw value; and

converting the raw value to decimal digits to form the obfuscated portion.

8. The method of claim 7, further comprising:

when the raw value exceeds a first constant:

storing a flag in a verification field associated with the account identifier; and

subtracting a second constant from the raw value.

9. The method of any one of claims 1 to 8, further comprising communicating the obfuscated account identifier to a host.

10. The method of claim 9, wherein the host generates a fraud alert if the host is unsuccessful in determining the account identifier from the obfuscated account identifier.

11. The method of claim 1, wherein in addition to the first end portion and the second end portion of the account identifier, the unique derived key is determined based upon an expiration date associated with the account identifier.

12. A computer program product comprising a computer readable memory storing computer executable instructions thereon that when executed by a computer perform the method steps comprising:

determining a dynamic cryptogram unique to a transaction using a unique derived key, wherein the unique derived key is determined based upon a first end portion and a second end portion of the obfuscated account identifier;

generating an obfuscated portion using the dynamic cryptogram; and

replacing a middle portion of the account identifier with the obfuscated portion to form an obfuscated account identifier, wherein the middle portion of the account

identifier excludes a first end portion comprising a bank identification number and a second end portion.

13. The computer program product of claim 12, wherein in addition to the first end portion and the second end portion of the account identifier, the unique derived key is determined based upon an expiration date associated with the account identifier.

14. A smart card comprising the computer program product of claim 12.

15. A mobile phone comprising the computer program product of claim 12.

16. A method for decrypting an obfuscated account identifier comprising:

generating a dynamic cryptogram unique to a transaction using a unique derived key, wherein the unique derived key is determined based upon a first end portion and a second end portion of the obfuscated account identifier;

generating a middle portion of an account identifier using the dynamic cryptogram, wherein the middle portion of the account identifier excludes a first end portion comprising a bank identification number and a second end portion; and

replacing an obfuscated portion of the obfuscated account identifier with the middle portion to form the account identifier.

17. The method of claim 16, further comprising determining which digits of the obfuscated account identifier comprise the obfuscated portion of the obfuscated account identifier.

18. The method of claim 16 or 17, wherein the unique derived key is further determined based upon using a master key.

19. The method of any one of claims 16 to 18, wherein the dynamic cryptogram is determined using a variable transaction counter and an expiration date.

20. The method of any one of claims 16 to 19, wherein the generating the middle portion of the account identifier comprises:

converting the obfuscated portion to hexadecimal digits;

performing an Exclusive-OR (XOR) operation on the dynamic cryptogram and the obfuscated portion to form a raw value; and

converting the raw value to decimal digits to form the middle portion.

21. The method of any one of claims 16 to 20, further comprising:

determining if a flag is set in a verification field associated with the obfuscated account identifier; and

adding a fixed value to the obfuscated portion, if the flag is set.

22. The method of claim 20, further comprising:

retrieving a stored check digit from a verification field; and

concatenating the raw value with the stored check digit.

23. The method of any one of claims 16 to 22, further comprising generating a fraud alert if the account identifier is invalid.

24. The method of claim 16, wherein in addition to the first end portion and the second end portion of the account identifier, the unique derived key is determined based upon an expiration date associated with the account identifier.

25. A computer program product comprising a computer readable memory storing computer executable instructions thereon that when executed by a computer perform the method steps comprising:

generating a dynamic cryptogram unique to a transaction using a unique derived key, wherein the unique derived key is determined based upon a first end portion and a second end portion of the obfuscated account identifier;

generating a middle portion of an account identifier using the dynamic cryptogram, wherein the middle portion of the account identifier excludes a first end portion comprising a bank identification number and a second end portion; and

replacing an obfuscated portion of the obfuscated account identifier with the middle portion to form the account identifier.

26. A server computer comprising the computer program product of claim 25.

27. The computer program product of claim 25, wherein in addition to the first end portion and the second end portion of the account identifier, the unique derived key is determined based upon an expiration date associated with the account identifier.

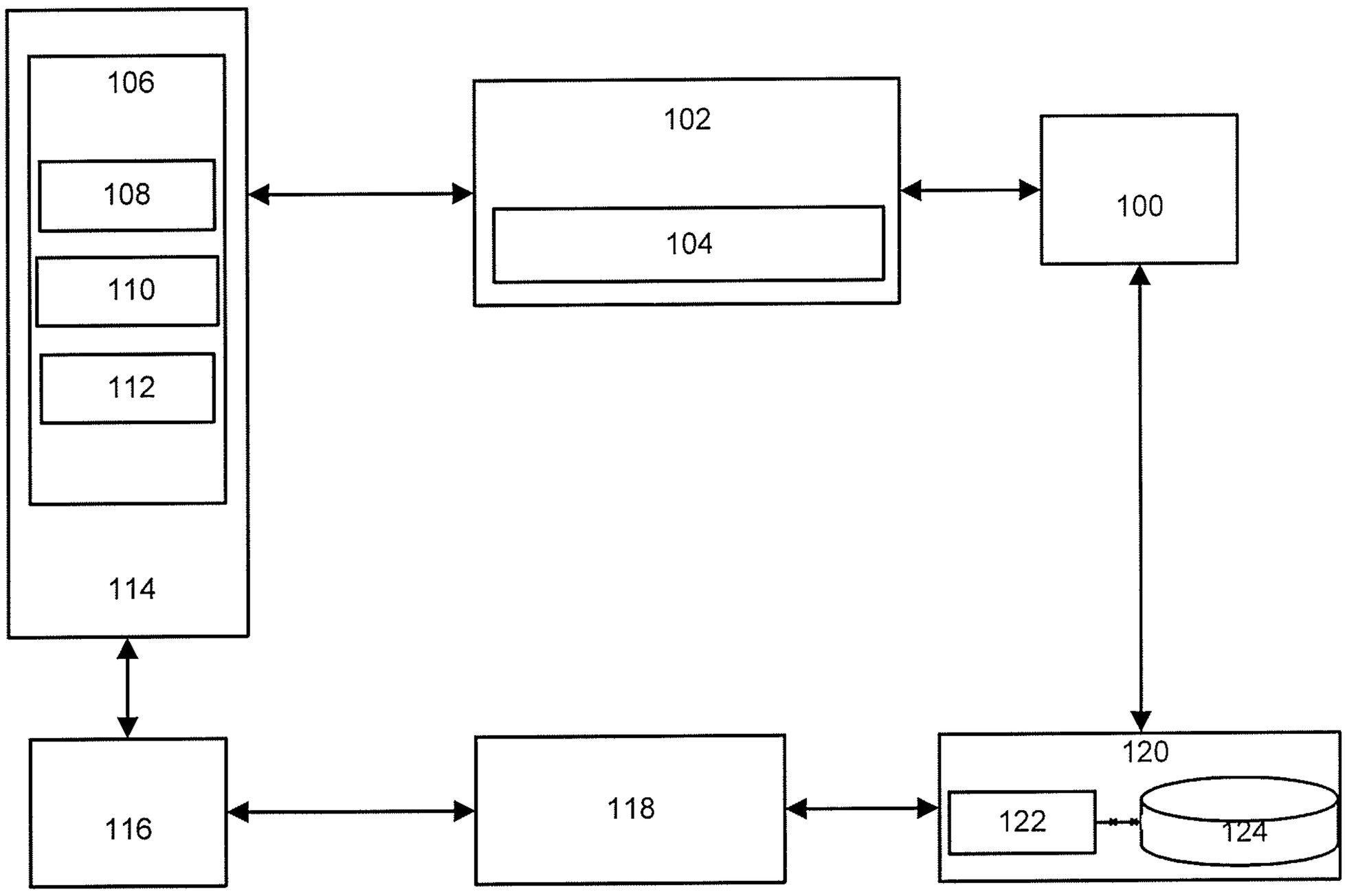


FIG. 1

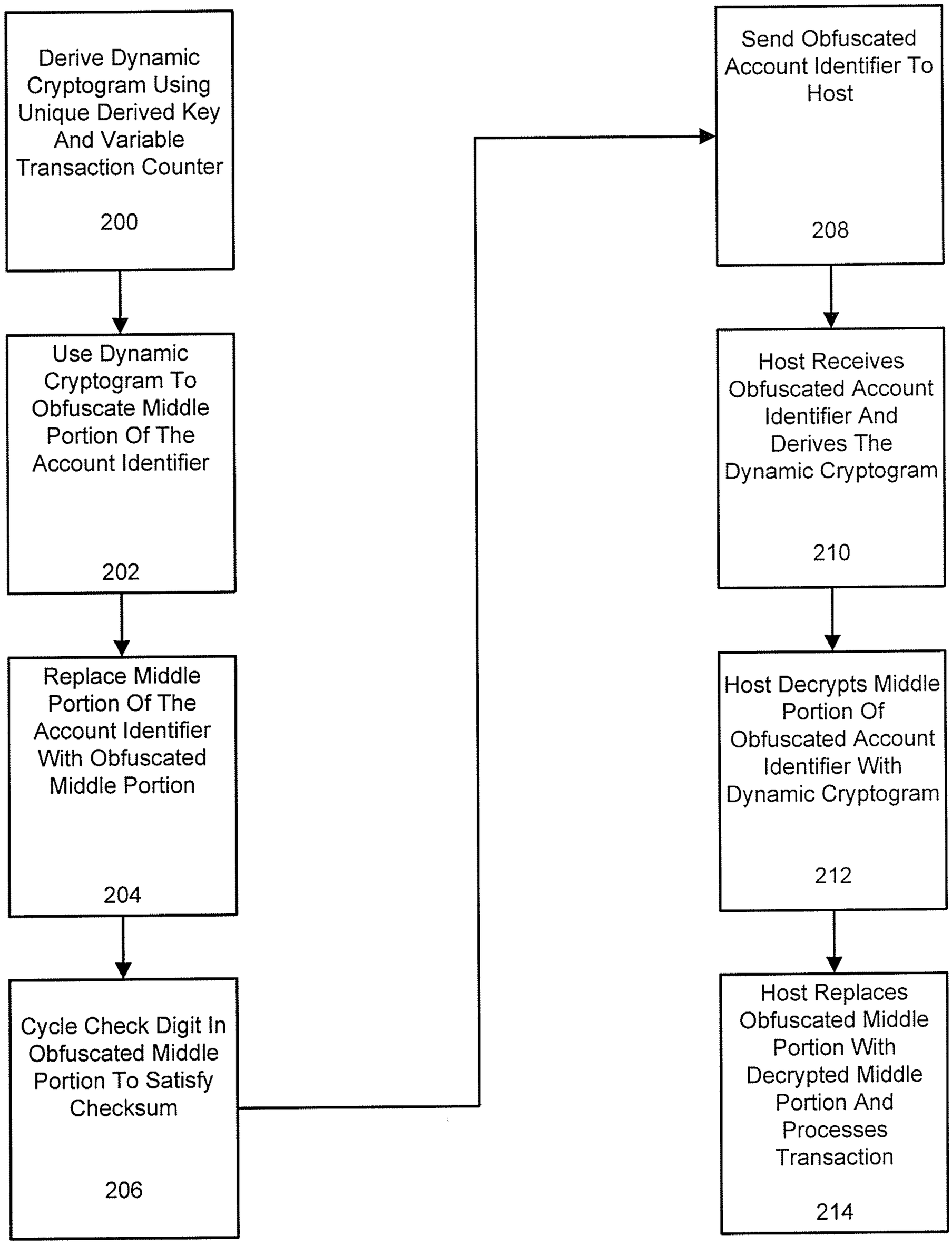

Derive Dynamic Cryptogram Using Unique Derived Key And Variable Transaction Counter
200
Use Dynamic Cryptogram To Obfuscate Middle Portion Of The Account Identifier
202
Replace Middle Portion Of The Account Identifier With Obfuscated Middle Portion
204
Cycle Check Digit In Obfuscated Middle Portion To Satisfy Checksum
206
Send Obfuscated Account Identifier To Host
208
Host Receives Obfuscated Account Identifier And Derives The Dynamic Cryptogram
210
Host Decrypts Middle Portion Of Obfuscated Account Identifier With Dynamic Cryptogram
212
Host Replaces Obfuscated Middle Portion With Decrypted Middle Portion And Processes Transaction
214

FIG. 2

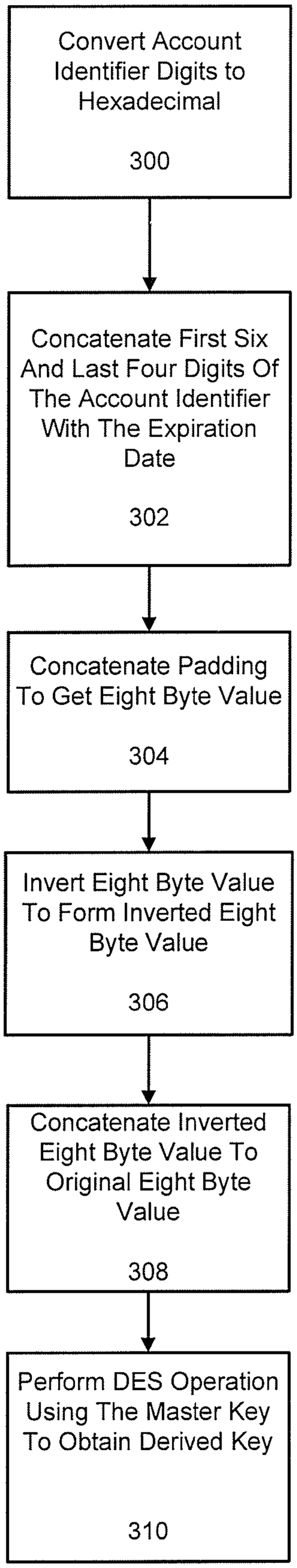

Convert Account Identifier Digits to Hexadecimal
300
Concatenate First Six And Last Four Digits Of The Account Identifier With The Expiration Date
302
Concatenate Padding To Get Eight Byte Value
304
Invert Eight Byte Value To Form Inverted Eight Byte Value
306
Concatenate Inverted Eight Byte Value To Original Eight Byte Value
308
Perform DES Operation Using The Master Key To Obtain Derived Key
310

FIG. 3

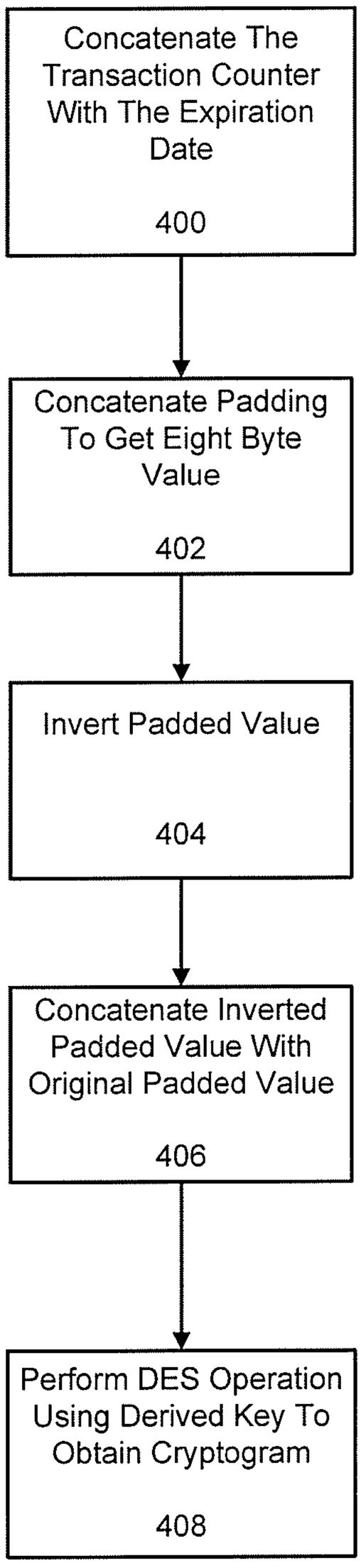

Concatenate The Transaction Counter With The Expiration Date
400
Concatenate Padding To Get Eight Byte Value
402
Invert Padded Value
404
Concatenate Inverted Padded Value With Original Padded Value
406
Perform DES Operation Using Derived Key To Obtain Cryptogram
408

FIG. 4

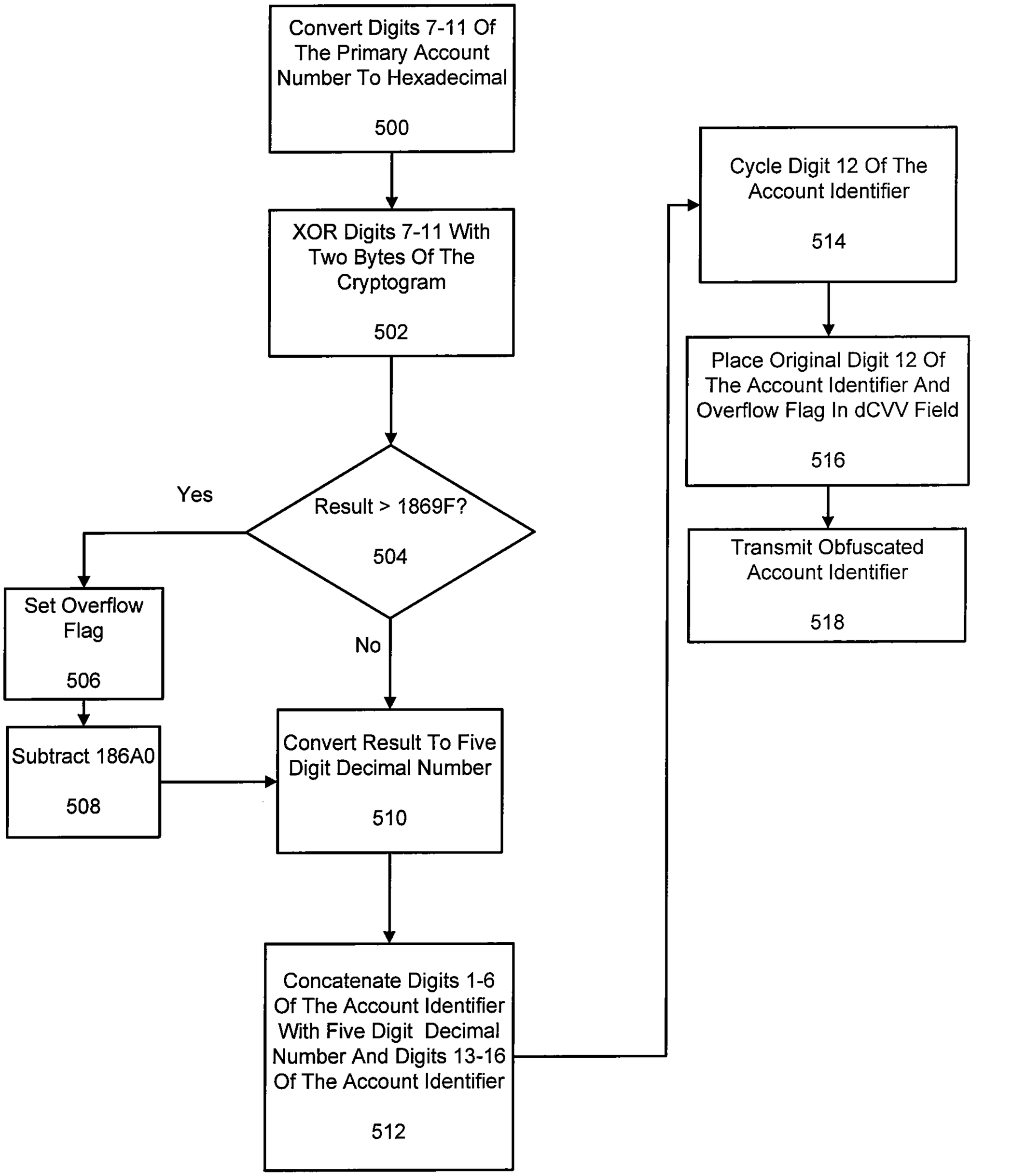

Convert Digits 7-11 Of The Primary Account Number To Hexadecimal
500
XOR Digits 7-11 With Two Bytes Of The Cryptogram
502
Result > 1869F?
504
Yes
No
Set Overflow Flag
506
Subtract 186A0
508
Convert Result To Five Digit Decimal Number
510
Concatenate Digits 1-6 Of The Account Identifier With Five Digit Decimal Number And Digits 13-16 Of The Account Identifier
512
Cycle Digit 12 Of The Account Identifier
514
Place Original Digit 12 Of The Account Identifier And Overflow Flag In dCVV Field
516
Transmit Obfuscated Account Identifier
518

FIG. 5

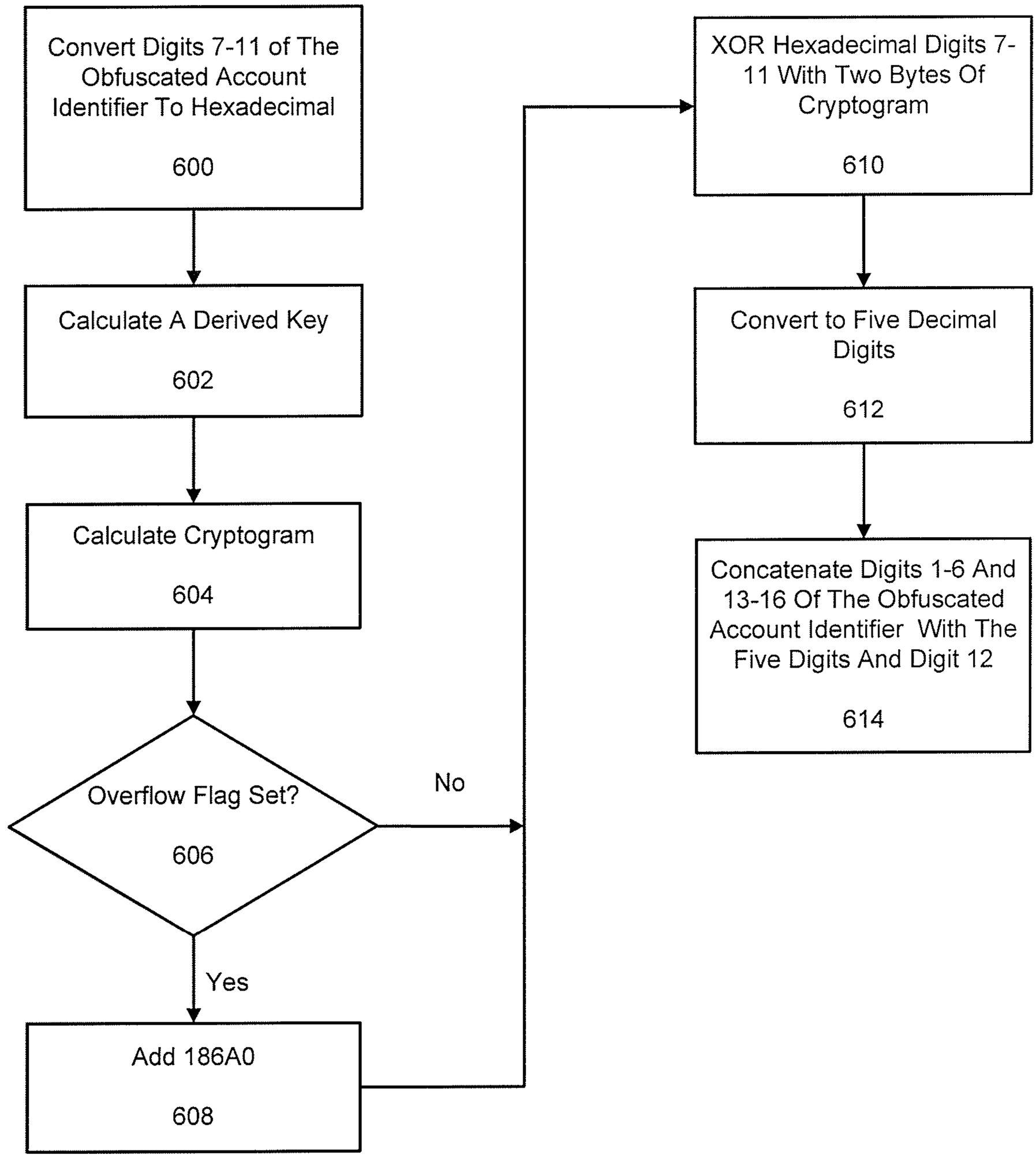

Convert Digits 7-11 of The Obfuscated Account Identifier To Hexadecimal
600
Calculate A Derived Key
602
Calculate Cryptogram
604
Overflow Flag Set?
606
No
Yes
Add 186A0
608
XOR Hexadecimal Digits 7-11 With Two Bytes Of Cryptogram
610
Convert to Five Decimal Digits
612
Concatenate Digits 1-6 And 13-16 Of The Obfuscated Account Identifier With The Five Digits And Digit 12
614

FIG. 6

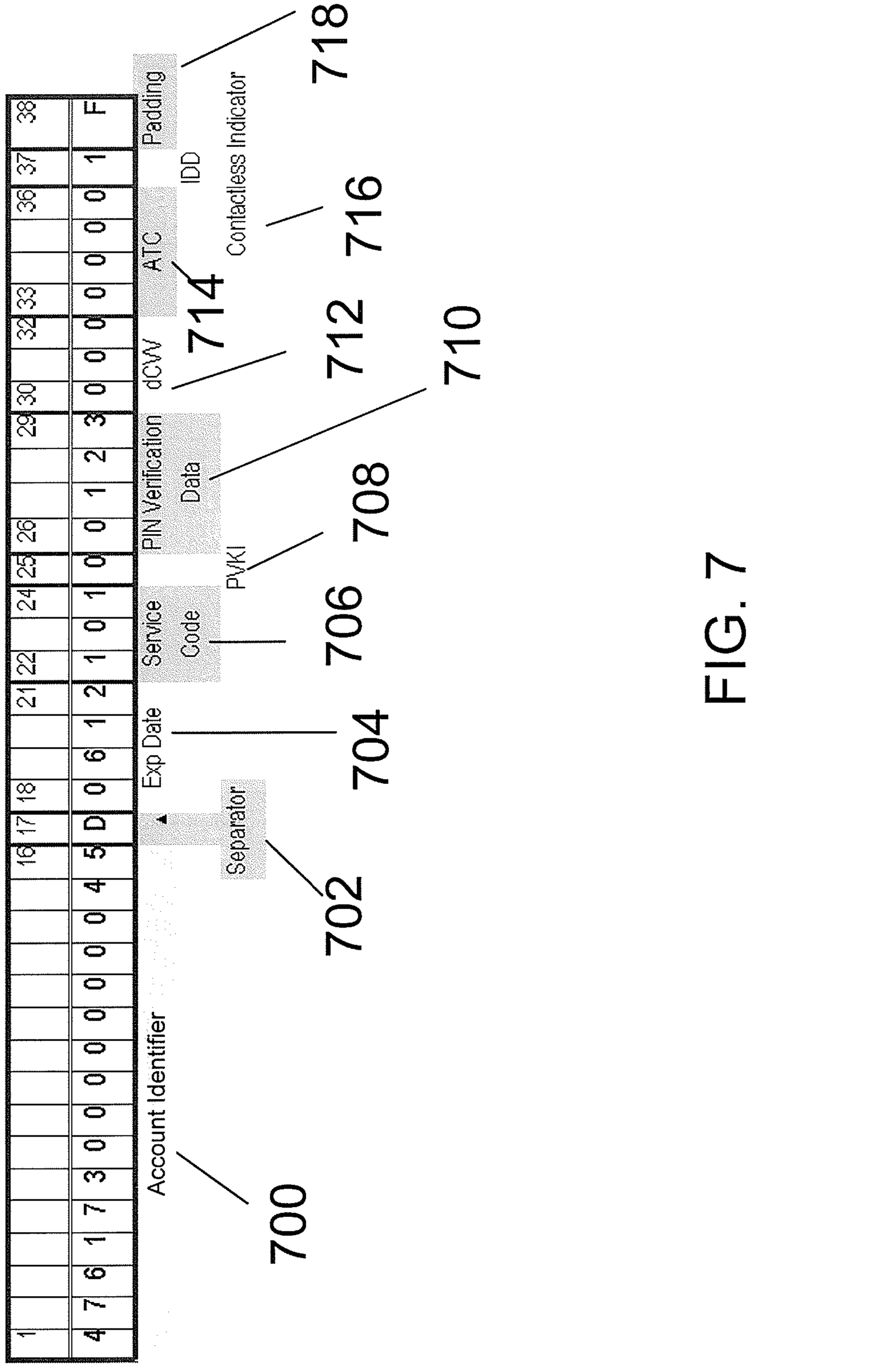

Account Identifier
Separator
Exp Date
Service Code
PVKI
PIN Verification Data
dCVV
ATC
Contactless Indicator
IDD
Padding
700
702
704
706
708
710
712
714
716
718

FIG. 7

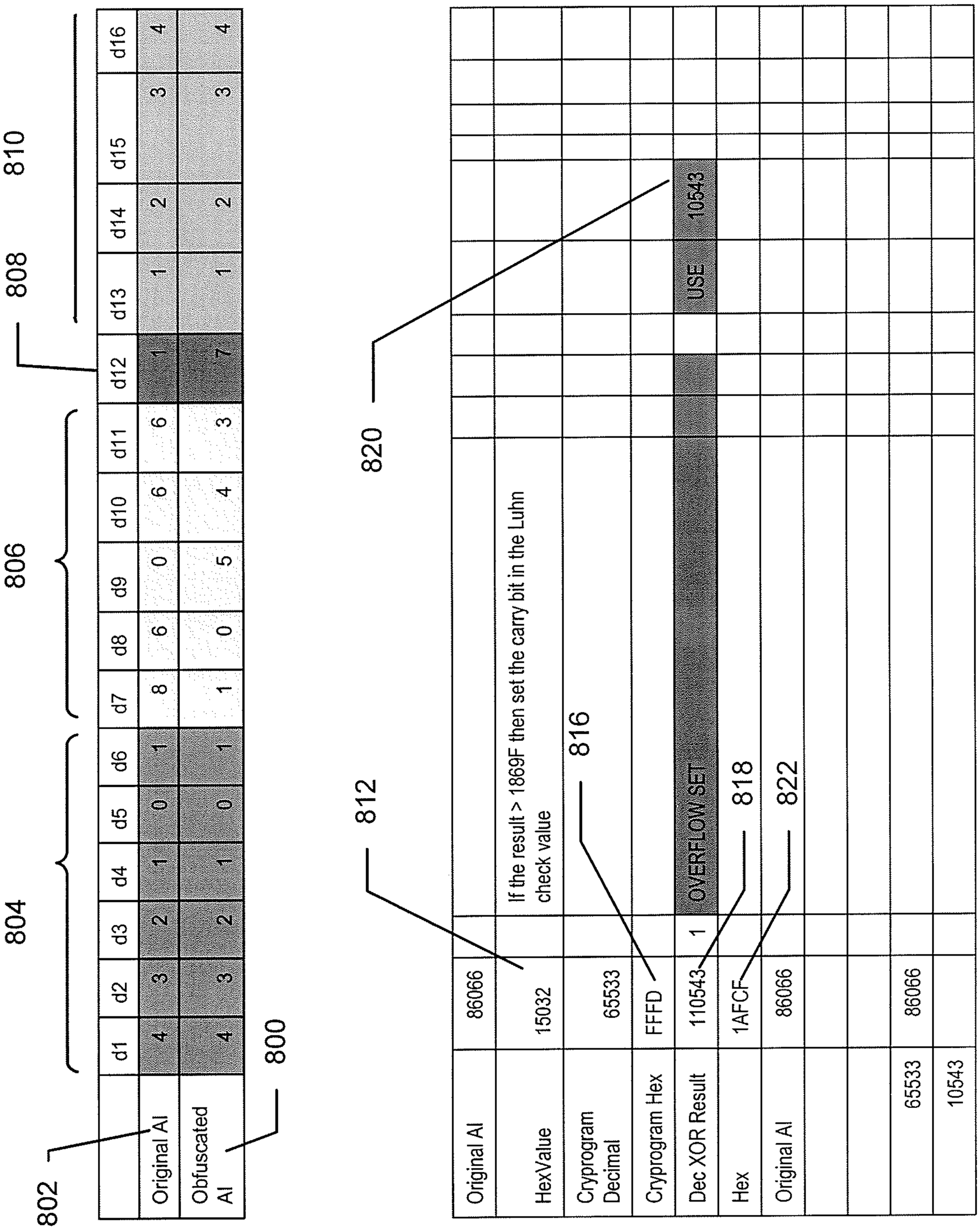

800
802
804
806
808
810
812
816
818
820
822
Original AI
Obfuscated AI
d1 d2 d3 d4 d5 d6 d7 d8 d9 d10 d11 d12 d13 d14 d15 d16
4 3 2 1 0 1 8 6 0 6 6 1 1 2 3 4
4 3 2 1 0 1 1 0 5 4 3 7 1 2 3 4
Original AI
HexValue
Cryprogram Decimal
Cryprogram Hex
Dec XOR Result
Hex
Original AI
86066
15032
65533
FFFD
110543
1AFCF
86066
If the result > 1869F then set the carry bit in the Luhn check value
OVERFLOW SET
USE
10543
65533
86066
10543

FIG. 8

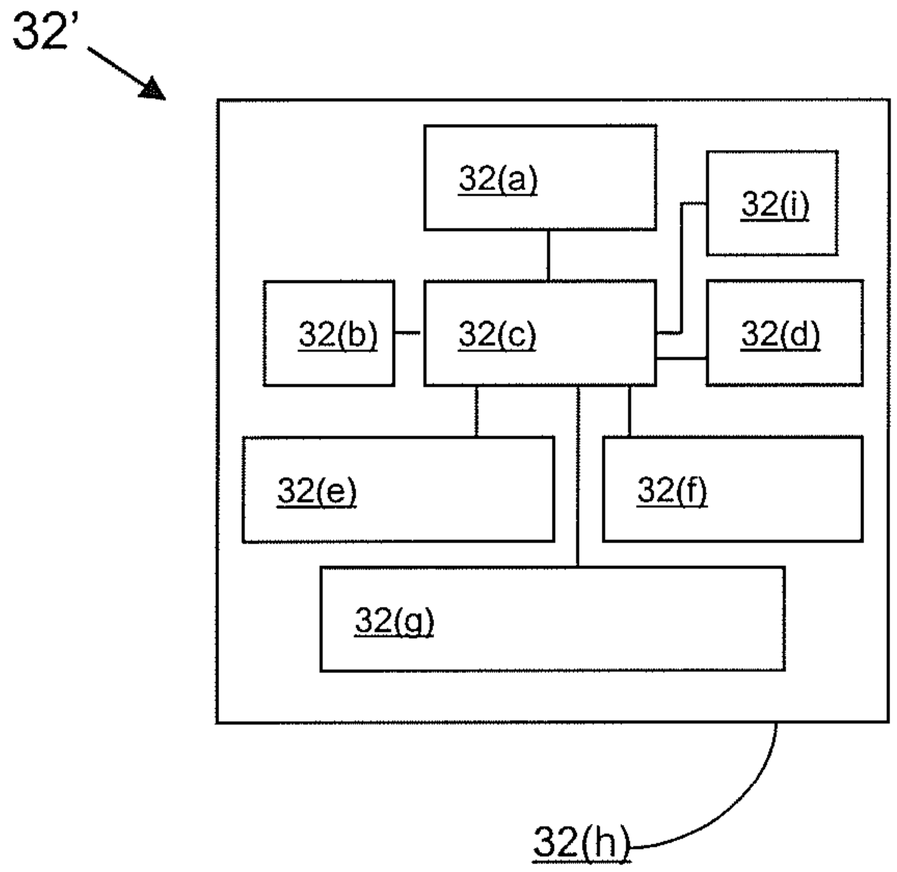


FIG. 9A

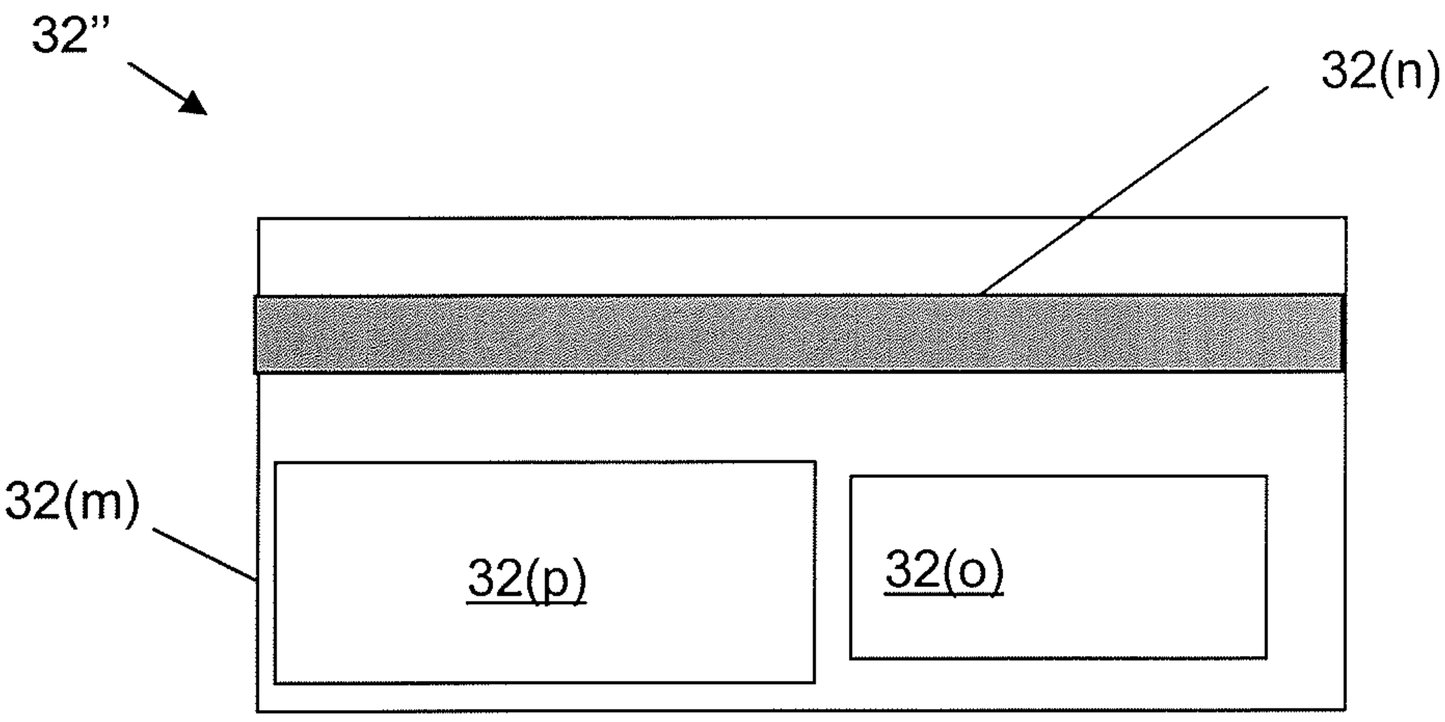


FIG. 9B

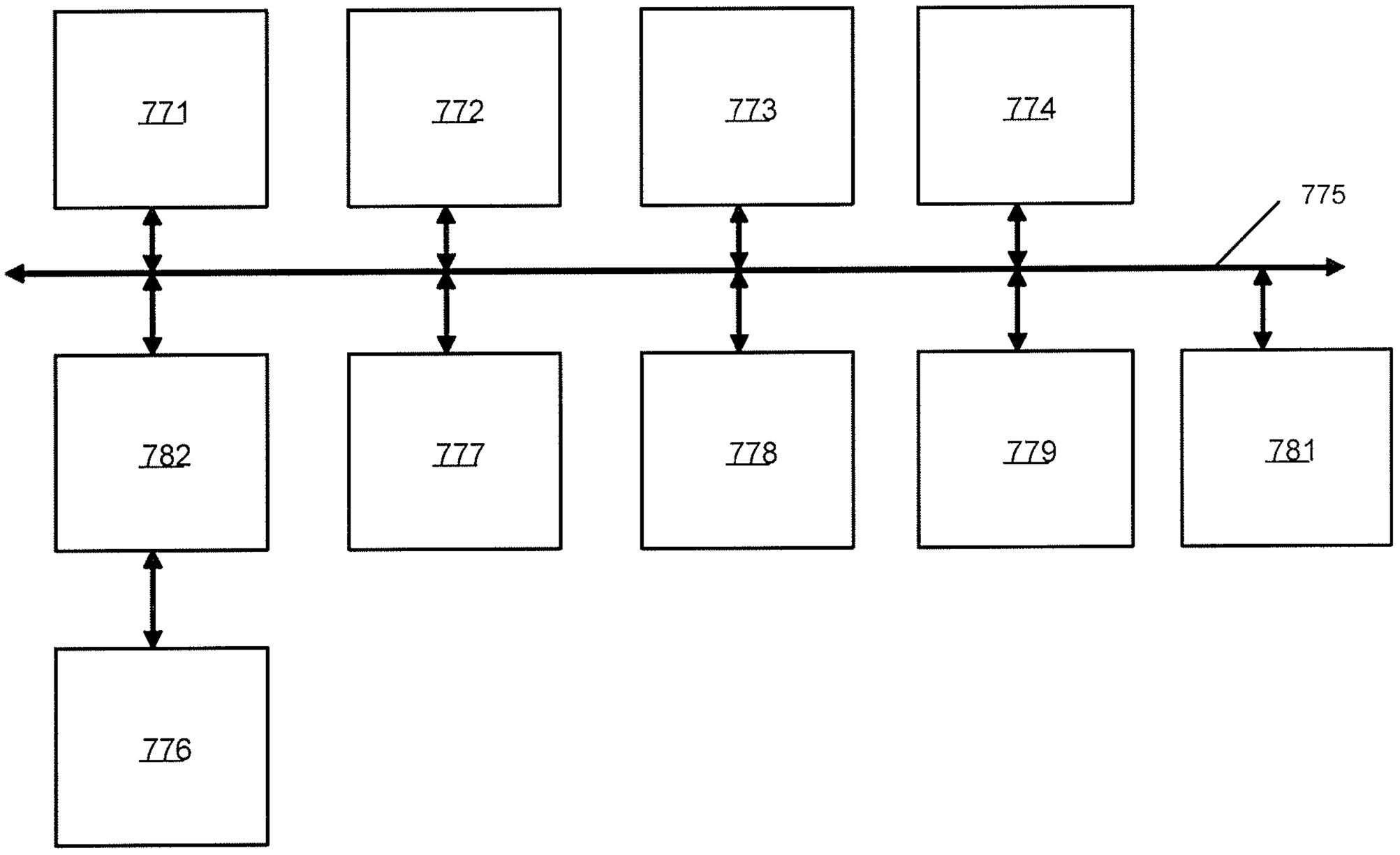
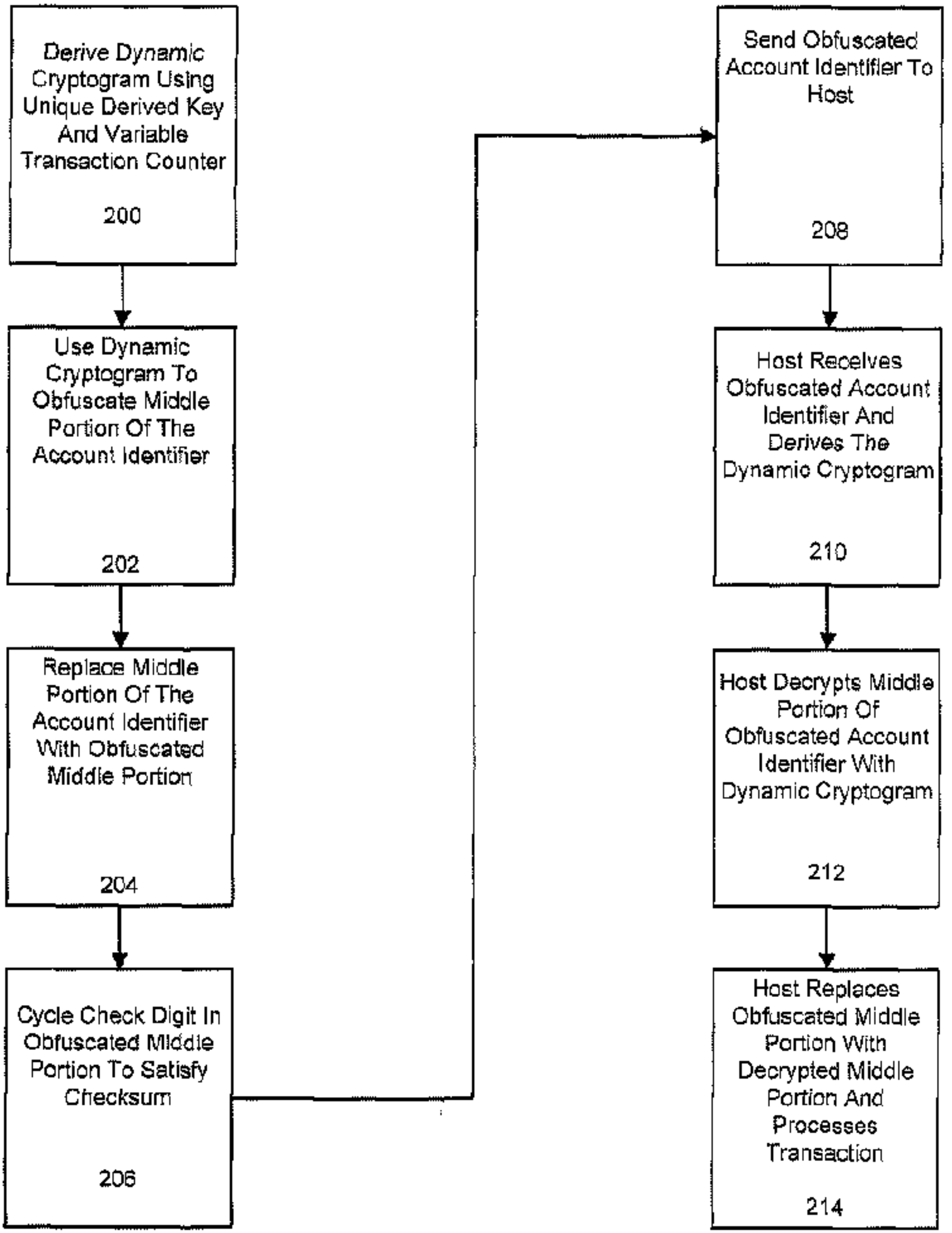


FIG. 10


Derive Dynamic Cryptogram Using Unique Derived Key And Variable Transaction Counter
200
Use Dynamic Cryptogram To Obfuscate Middle Portion Of The Account Identifier
202
Replace Middle Portion Of The Account Identifier With Obfuscated Middle Portion
204
Cycle Check Digit In Obfuscated Middle Portion To Satisfy Checksum
206
Send Obfuscated Account Identifier To Host
208
Host Receives Obfuscated Account Identifier And Derives The Dynamic Cryptogram
210
Host Decrypts Middle Portion Of Obfuscated Account Identifier With Dynamic Cryptogram
212
Host Replaces Obfuscated Middle Portion With Decrypted Middle Portion And Processes Transaction
214