

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
27 May 2004 (27.05.2004)

PCT

(10) International Publication Number
WO 2004/044715 A1

(51) International Patent Classification⁷: **G06F 1/00**,
G07F 7/00, 17/32

(21) International Application Number:
PCT/US2003/032874

(22) International Filing Date: 15 October 2003 (15.10.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/291,926 7 November 2002 (07.11.2002) US

(71) Applicant (for all designated States except US): **IGT**
[US/US]; 9295 Prototype Drive, Reno, NV 89521 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **BROSNAN,**

William [US/US]; 4751 W. Creek Ridge Trail, Reno, NV 89509 (US). **BENBRAHIM, Jamal** [MA/US]; 8455 Offenhauser #1022, Reno, NV 89511 (US). **LEMAY, Steven, G.** [US/US]; 17085 Pine Castle Drive, Reno, NV 89511 (US).

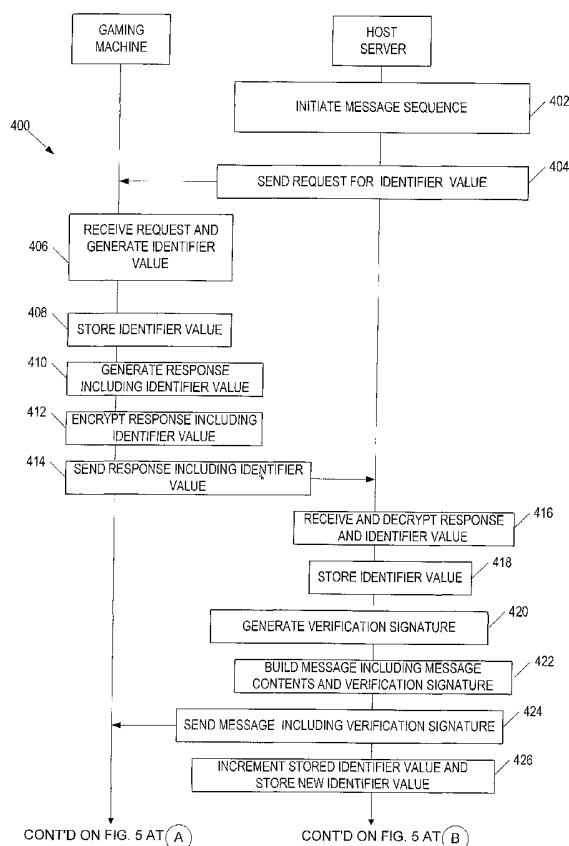
(74) Agent: **OLYNICK, David, P.**; P.O. Box 778, Berkeley, CA 94704-0778 (US).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: IDENTIFYING MESSAGE SENDERS FOR GAMING DEVICES



(57) Abstract: A disclosed gaming network provides a method and system for identifying message senders through use of a communication protocol that includes a message field containing message contents and a verification field containing a verification signature. The verification signature is calculated by a message sender utilizing a valuation of the message contents and an identifier value provided by the message receiver.

WO 2004/044715 A1



European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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.

IDENTIFYING MESSAGE SENDERS FOR GAMING DEVICES

FIELD OF THE INVENTION

The present invention relates to gaming machines, such as slot machines and video poker machines. More particularly, the present invention relates to methods and systems for identifying the sender of a message to a gaming machine or the host server of a gaming machine.

BACKGROUND OF THE INVENTION

There are a wide variety of associated devices that can be connected to a gaming machine such as a slot machine or video poker machine. Some examples of these devices are lights, ticket printers, card readers, speakers, bill validators, ticket readers, coin acceptors, display panels, key pads, coin hoppers and button pads. Many of these devices are built into the gaming machine or components associated with the gaming machine such as a top box which usually sits on top of the gaming machine.

Typically, utilizing a master gaming controller, the gaming machine controls various combinations of devices that allow a player to play a game on the gaming machine and also encourage game play on the gaming machine. For example, a game played on a gaming machine usually requires a player to input money or indicia of credit into the gaming machine, indicate a wager amount, and initiate a game play. These steps require the gaming machine to control input devices, such as bill validators and coin acceptors, to accept money into the gaming machine and recognize user inputs from devices, including key pads and button pads, to determine the wager amount and initiate game play. After game play has been initiated, the gaming machine determines a game outcome, presents the game outcome to the player and may dispense an award of some type depending on the outcome of the game.

The operations described above may be carried out on the gaming machine when the gaming machine is operating as a "stand alone" unit or linked in a network of some type to a group of gaming machines. As technology in the gaming industry progresses, more and more gaming services are being provided to gaming machines via communication networks that link groups of gaming machines to a remote computer that provides one or more gaming services. As an example, gaming

services that may be provided by a remote computer to a gaming machine via a communication network of some type include player tracking, accounting, cashless award ticketing, lottery, progressive games and bonus games.

Typically, network gaming services enhance the game playing capabilities of the gaming machine or provide some operational advantage in regards to maintaining the gaming machine, such as better accounting management or player tracking. Thus, network gaming services provided to groups of gaming machines linked over a dedicated communication network of some type have become very popular in the gaming industry.

In general, the dedicated communication network is not accessible to the public. To justify the costs associated with the infrastructure needed to provide network gaming services on a dedicated communication network, a certain critical number of gaming machines linked in a network of some type must utilize the service. Thus, many of the network gaming services are only provided at larger gaming establishments where a large number of gaming machines are deployed.

A progressive game network offering progressive game services is one example where a group of gaming machines are linked together using a dedicated network to provide a network gaming service. The progressive game services enabled by the progressive game network increase the game playing capabilities of a particular gaming machine by enabling a larger jackpot than would be possible if the gaming machine was operating in a "stand alone" mode. The potential size of the jackpot increases as the number of gaming machines connected in the progressive network is increased. The size of the jackpot tends to increase game play on gaming machines offering a progressive jackpot which justifies the costs associated with installing and maintaining the dedicated progressive game network. Another example would be a bonus network that enables players to choose a particular prize they play for, and in some instances to access information related to the prize over the network.

Within the gaming industry, a particular gaming entity may also desire to provide network gaming services and track the performance of gaming machines under the control of the entity. Thus, other dedicated networks may also connect the gaming machines to host servers which enable accounting management, electronic

fund transfers (EFTs), cashless ticketing, such as EZPayTM, marketing management, and data tracking, such as player tracking.

FIG. 1 is a block diagram depicting gaming machines within a dedicated communication network for a typical gaming entity currently operating in the gaming industry. On a casino floor, there are typically several different types of gaming machines produced by different manufacturers. Each of the gaming machines may include a variety of different systems that allow a casino to manage different aspects of the gaming machine.

In FIG. 1, the gaming machines, 102, 126, 128, 130, and 132 are connected to a host server 124 that receives data for a particular dedicated network 122. Within a casino, the gaming machines 102 and 126 – 132 are typically located on the floor for player access while the host server 124 is usually located in the backroom of the casino for security purposes. In some designs, a device for concentrating the data and/or converting the physical transmission medium of the network to a format accepted by the host server 124 may be present between the gaming machines 102 and 126-132 and the host server 124.

Gaming machine 102 and the other gaming machines on the network typically include a main cabinet 106 and a top box 104. The main cabinet 106 usually houses the main gaming elements, although the top box 104 may include some peripheral systems, such as a player tracking system.

As earlier described, the master gaming controller 108 typically controls the game play on the gaming machine 102 and receives or send data to various input/output devices on the gaming machine 102. The master gaming controller 108 may also communicate with a display 110, electronic funds transfer system 112, bonus system 114, EZ pay system 116, e.g., cashless ticketing system and player tracking system 120. The systems of the gaming machine 102 typically communicate with the host server 124 via a communication board 118. In some instances, the gaming machine 102 may also include an encryption system for decrypting or encrypting data communicated from or to the host server 124.

Due to the sensitive nature of much of the information, such as electronic fund transfer information, usually the manufacturer of a system or group of systems employs a particular networking language having proprietary protocols. These proprietary protocols are usually considered highly confidential and are not released

publicly. As a receiving entity on the network cannot identify the sender of data on the network, the proprietary protocol is used to prevent unauthorized communications, such as tampered data. In theory, a communication from a sender using the proprietary protocol must be legitimate as only an approved sender would
5 have access to the proprietary protocol.

Further, when a new system is introduced for use with a gaming machine, rather than trying to interpret all the different protocols utilized by different manufacturers, which are typically proprietary and thus not accessible, the new system is typically designed as a separate network. Consequently, as more systems
10 are introduced, the independent network structures continue to build up in the casino. Thus, it will be appreciated that although one dedicated network 122 is shown in the present illustration linking the gaming machines 102 and 126-132 to the host server 124, the gaming machines may have other dedicated networks connecting them to one or more host servers 124.

15 The use of many different proprietary protocols and their attendant dedicated networks, becomes costly for the gaming entity and introduces logistic costs whenever the network needs to be moved during a casino layout change or when gaming devices utilizing a new proprietary protocol are added to the network. With increasing sophistication of data tampering devices, it is becoming more difficult to
20 ensure that the data received from a sender is indeed sent by an authorized sender even when an authorized proprietary protocol has been used. Therefore, the security benefits of using proprietary protocols may be outweighed by the logistics and maintenance costs associated with ensuring communication compatibility in a gaming network gaming devices that utilize many different non-compatible
25 proprietary communication protocols.

In view of the above, it would be desirable to have a method and/or device that identifies the sender of a message on a network as an authorized sender.

SUMMARY OF THE INVENTION

The present invention addresses the needs indicated above through a method
30 and system which identify the sender of message using a message transport protocol that includes a verification field in addition to a message field.

One aspect of the present invention includes a method for identifying the sender of a message on a gaming machine network. The method may be generally

characterized as including: sending a request for a first identifier value from a host server to a target gaming machine, the host server having message contents to be sent to the target gaming machine; receiving the request at the target gaming machine; generating a first identifier value at the target gaming machine; storing the first identifier value in a memory structure at the target gaming machine; sending
5 the first identifier value from the target gaming machine to the host server; receiving the first identifier value at the host server; storing the first identifier value in a memory structure at the host server; generating a verification signature at the host server using a valuation of the message contents and the first identifier value;
10 sending the message contents and the verification signature from the host server to the target gaming machine; receiving the message contents and the verification signature at the target gaming machine; calculating a check value at the target gaming machine; determining at the gaming machine whether the check value is equal to the verification signature, and if equal, accepting the message for further
15 processing by the gaming machine.

Another aspect of the present invention provides a gaming machine network. The gaming machine network may be generally characterized as including: at least one host sever, the host server including verification software that enables the host server to obtain an identifier value from a gaming machine, and in response to
20 obtaining the identifier value, enables the host server to generate a message according to a protocol that permits the gaming machine to identify the sender of the message; a plurality of gaming machines, each gaming machine including: a master gaming controller configured to control one or more games played on the gaming machine, a memory configured to store a plurality of verification software elements
25 that allow the gaming machine to identify the sender of a message on the gaming machine network; and a network allowing communication between the host server and the plurality of gaming machines.

Another aspect of the invention pertains to computer program products including a machine-readable medium on which is stored program instructions for
30 implementing any of the methods described above. Any of the methods of this invention may be represented as program instructions and/or data structures, databases, etc. that can be provided on such computer readable media. Yet another embodiment of the present invention is a system for delivering computer readable

instructions, such as transmission, over a signal transmission medium, of signals representative of instructions for remotely administering any of the methods as described above.

These and other features of the present invention will be presented in more detail in the following detailed description of the invention and the associated figures.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is an illustration of a gaming machine found in the prior art.

FIG. 2 is a block diagram representation of a prior art message format including a message field.

FIG. 3 is a block diagram representation of a communication protocol having a verification field in addition to a message field according to one embodiment of the present invention.

FIGS. 4 and 5 are flow diagrams illustrating a method of identifying a message sender according to one embodiment of the present invention.

FIG. 6 is a flow diagram illustrating the key loading of the host server according to one embodiment of the present invention.

FIG. 7 is a flow diagram illustrating the key loading of the gaming machine according to one embodiment of the present invention.

FIG. 8 is an illustration of a gaming network including a verification system according to one embodiment of the present invention.

FIG. 9 is a block diagram representation of a host server verification module according to one embodiment of the present invention.

FIG. 10 is a block diagram representation of a gaming machine verification module according to one embodiment of the present invention.

FIG. 11 is a perspective drawing of a gaming machine for one embodiment of the present invention.

FIG. 12 is a block diagram of a gaming network for one embodiment of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides for identifying message senders in a gaming machine network to enable gaming machines to verify they are communicating to a legitimate host system, as well as the reverse.

FIG.2 is a block diagram representation of a prior art message format including a message field. Typically, the message field 202 includes message contents to be sent to a gaming machine or host system according to a particular gaming network protocol. As earlier discussed gaming protocols are generally proprietary to prevent tampering of the message contents. As such, the devices on the gaming network do not identify the message sender, but rather recognize the proprietary protocol.

FIGs. 3 through 10 illustrate several embodiments of the present invention which provide for identification of a message sender in a gaming machine. It will be appreciated that various hardware and software architectures may be used to implement the present invention and that the embodiments shown in FIGURES 3 - 10 are intended to illustrate the present invention rather than limit it. Any of the embodiments may also provide for the further encryption and/or physical protection of the information being stored and transmitted. Additionally, although the present invention will be described primarily in regard to identification of a message from a host server by a gaming machine, the reverse may also be implemented, as well as both.

As discussed with reference to FIG. 2, current communication protocols used between a gaming machine and host server typically include a message field 202. When the message contents includes sensitive data, such as electronic fund transfer data, bonus transfer data, or electronic credit data, the data is typically sent in the clear, or encrypted prior to sending. The former method relies on the security of the gaming network communication protocol used and/or the physical security of the transmission lines to prevent data tampering. The latter method increases the processing time and data load on the transmission lines, and can be costly to install a secure network.

In mitigation of the above-mentioned considerations, the present invention provides for a communication protocol in which a verification field is used in addition to the message field.

FIG. 3 is a block diagram representation of a communication protocol having a verification field in addition to a message field according to one embodiment of the present invention. The message field 202 contains the message contents to be transmitted to a first gaming device, such as a gaming machine, from a second gaming device, such as another gaming machine or a remote server. The verification field 304 contains a verification signature. The verification signature may be primarily used for two purposes: 1) to identify the sender of the message and 2) to determine whether the contents of the message in the message field 202 have been modified or altered.

In one embodiment, a verification signature using public-private signature key pairs may be used. In public-private signature key pair verification method, a first gaming device may give its public signature key to a number of other gaming devices (see FIGs. 6 and 7). When the first gaming device desires to send a message to a second gaming device that possesses its public signature key with a verification signature, the first gaming device applies a hash algorithm to the message contents in the message field 202 to generate a message digest. A verification signature may be generated from the message digest using a digital signature algorithm. The digital signature algorithm may use the private signature key and the message digest to generate the verification signature. A message with the message contents in the message field 202 and the verification signature may be sent to the second gaming device. The second gaming device applies the hash algorithm to generate a message digest. Then, with the message digest, the first gaming device's public signature key and the verification signature, the second gaming device may apply a verification algorithm.

The verification algorithm is designed such that only a verification signature generated from the message digest and the private signature key will match the output from the verification algorithm generated using the public signature key and the message digest. The output from the verification algorithm is compared to the verification signature received in the message. When the output matches the verification signature, it may be assumed that the message contents have not been altered and the identity of the message sender is the first gaming device. One example of a method that may be used with the present invention is the digital signature standard (DSS) approved by the U.S. government.

In the present invention, to provide further security against lost or inserted messages, a secret value may be appended to the message contents sent in each message exchanged between two gaming devices. The secret value changes the hash value of the message contents and may change with each message. The secret value
5 may be exchanged beforehand by the two gaming devices (i.e., prior to initiating communications) or may be exchanged at the time communication between the two gaming devices is initiated. For instance, a public-private encryption scheme may be used to exchange a secret value between the two devices. The secret value may be used to prevent an attacker from sneaking in during a message exchange between
10 the two gaming devices and pretending to be one or both parties.

The verification signature in the verification field 304 may be used with or without encryption in the following manners. The message field 202 may be encrypted but a verification signature may not be generated. In this case, only a recipient with an encryption key can read the message. However, the recipient may
15 not determine an identity of the sender of the message. In another embodiment, the message may include the verification signature but the message contents may not be encrypted. In this case, any recipient of the message may determine from the signature the identity of the sender. In yet another embodiment, the message contents in the message field 202 may be encrypted and then a verification signature
20 may be generated. In this case, only a recipient with an appropriate encryption key may read the message but any recipient of the message may be able to tell who sent the message. In another embodiment, the verification signature may be generated and then the verification signature and the message contents may be encrypted. In this case, only a recipient of the message with an appropriate encryption key may be
25 able to read the message and determine the identity of the sender of the message.

In one embodiment, public-private asymmetric encryption keys may be used with the present invention. In a public-private encryption method, information encrypted with the public encryption key may be decrypted only using the corresponding private encryption key of the public-private encryption key pair and
30 information encrypted with the public encryption key may be decrypted only using the private encryption key. Thus, an entity with a private encryption key of public-private encryption key pair may give its public encryption key to many other entities. The public encryption key may be made available (via an Internet server, e-

mail, or some other means) to whoever needs or wants it. The private encryption key, on the other hand, is kept secret. Only the owner of the key pair is allowed to possess the private encryption key. The other entities may use the public encryption key to encrypt data. However, as long as the private encryption key remains private, only the entity with the private encryption key can decrypt information encrypted with the public encryption key.

In one embodiment, the identity of a message sender may be determined using public-private encryption key pairs. Two gaming devices, each storing public-private encryption key pairs, may exchange public encryption keys (see Figs. 6 and 7). Then, the gaming devices may exchange a series of messages that are encrypted with each other's public keys. For instance, a first gaming device may send a message with information that is encrypted with a second gaming device's public encryption key. As an example, the information may be a randomly generated number. The information sent by the first gaming device is also stored by the first gaming device.

The second gaming device may receive the message from the first gaming device and decrypt the information with its private key. Then, the second gaming device may encrypt the information with the first gaming device's public encryption key and send a reply message with encrypted information to the first gaming device. The first gaming device decrypts the information in the message using its private encryption key. Then, the first gaming device compares the information sent in the original message with the information received in the reply message. When the information received in the reply message from the second gaming device matches the information sent to the second gaming device, the identity of the second gaming device is authenticated since only the possessor of the private key may decrypt a message encrypted with its public key. Details of exchanging encryption keys in a secure manner, which may be applied to the present invention, are described in co-pending U.S. application no. 09/993,163, by Rowe et al., filed November 16, 2001 and entitled "A Cashless Transaction Clearinghouse," which are incorporated herein by reference in its entirety and for all purposes.

In general, public-key algorithms are very slow and it is impractical to use them to encrypt large amounts of data. In a symmetric encryption algorithm, the same encryption key is used to encrypt and decrypt information. In practice,

symmetric algorithms are used for encryption/decryption of large amounts of data, while the public-private encryption key algorithms are used merely to encrypt the symmetric keys. Methods of asymmetric and symmetric keys that may be used to transfer encrypted data in the present invention are described co-pending U.S.
5 application no. 10/116,424, filed April 3, 2002, by Nguyen et al. and entitled, "Secured Virtual Network in a Gaming Environment," which is incorporated herein in its entirety and for all purposes.

FIGs. 4 and 5 are flow diagrams illustrating a method for identifying message senders according to one embodiment of the present invention. The method
10 in FIGs. 4 and 5 may be implemented between any two gaming devices in a gaming network (see FIG. 12). However, for illustrative purposes only, a message exchange between a gaming machine and a host server is described. Prior to beginning the method, the host server and gaming machine are started up and may be loaded with
1) encryption keys, 2) signature keys and 3) combinations thereof. Start up
15 procedures for a gaming machine and host server are well-known to those of skill in the art and will only be briefly described herein.

In one embodiment, the host server is loaded with a private encryption key and the gaming machine is loaded with a public encryption key corresponding to the host server's private encryption. The host server private key is kept secret and is
20 used to decrypt data encrypted with its public encryption key by other gaming devices, such as the gaming machine. Messages encrypted with the public key can be decrypted using the private key. The public key is not secret and is used to encrypt data sent to the host server although the public key may initially be given only to gaming devices authorized to communicate with the host server. The gaming
25 machine may be loaded with a private-public encryption key pair and the gaming machine's public encryption key may be loaded onto the host server. Encryption key loading of both the gaming machine and host server are briefly discussed herein with reference to FIGs. 6 and 7.

In another embodiment, the host server and/or the gaming machine may be
30 loaded with public-private signature key pairs. In a public-private signature key method, a message may be signed with a verification signature using a private signature key. The private signature key is kept secret. The verification signature may only be reproduced when the corresponding public signature key is applied to

the message contents. When the verification signature is reproduced using the public signature key and the message contents of the message, the recipient of the message can assume that 1) the message contents have not been altered and 2) the message was sent by the owner of the private signature key that generated the verification signature. As described with respect to FIG. 3, public-private encryption keys and public-private signature keys may be used in combination.

At step 402, the host server initiates a secure communication sequence with the gaming machine. The secure communication sequence may comprise a plurality of messages exchanged between the host server and the gaming machine. The secure communication sequence may be initiated after a request for the secure communication sequence is received from the gaming machine. In some instances, as will be later described herein with reference to step 438 of FIG. 5, this initial step may also be the result of a request from the gaming machine to the host server to reinitiate a connection with the gaming machine.

At step 404, the host server sends a request to the gaming machine for an identifier value. Preferably, this request is sent unencrypted as the request contains no sensitive data.

At step 406, the gaming machine receives the request, and, in response to the request, the gaming machine generates an identifier value. In a preferred embodiment, the identifier value is a numerical value produced using an algorithm, such as a random number generator algorithm.

At step 408, the gaming machine then stores the generated identifier value in memory, and preferably, in a secure memory structure. For instance, in one embodiment, the secure memory structure may be a non-volatile RAM used on the gaming machine. Details of a secure memory structure that may be used with present invention are described in co-pending U.S. application no. 09/689,498, filed October 17, 2000, by Stockdale, et al., and entitled, "High Performance Battery Backed Ram Interface," which is incorporated by reference in its entirety and for all purposes.

At step 410, the gaming machine generates a response including the identifier value.

At step 412, the gaming machine encrypts the response using the public encryption key for the host server.

At step 414, the gaming machine sends the encrypted response to the host server.

At step 416, the host server receives and decrypts the response using its private encryption key.

5 At step 418, the host server stores the identifier value in memory, and preferably, in a secure memory structure.

At step 420, the host server calculates a sent verification signature using the identifier value and the message contents. In one embodiment, the sent verification signature is a value calculated by applying a one-way computational algorithm to
10 the message contents and to the identifier value and combining the values. For example, a check-sum algorithm may be applied to both the message contents and to the identifier value. The resulting check-sum values may then be added together to produce a verification signature.

In general, an output from the one-way computational algorithm that
15 operates on an information string, such as the message contents, is referred to as the message digest. For instance, the check sum values from the check sum algorithm are the message digest for the check sum algorithm. A characteristic of the one-way computational algorithms applied to the information strings are that the algorithms provide one-way computations. In a one-way computation, there is no known way,
20 without infeasible amounts of computation, to determine the information string used to generate the message digest using the one-way computational algorithm. These algorithms are similar to the scrambling operations used in symmetric key encryption, with the exception that there is no decryption key. Thus, the operation is irreversible.

25 In other embodiments, the verification signature may be a value calculated by applying an algorithm to only the message contents, and then combining the obtained message digest value with the identifier value. For example, the check-sum algorithm may be applied to the message contents only, and then the identifier value added to the message contents value. In another embodiment, the identifier
30 value may be appended to the message contents and then verification signature may be generated from the combined message contents and identifier signature.

In still other embodiments, other algorithms may be used in place of a check-sum algorithm. For example, hashing algorithms, such as MD5, MD2, MD4,

and SHA (secure hash algorithm), may be also used. SHA is used with the digital signature standard approved by the U.S. government. Further, the combination of the method contents value and the identifier value, may also be made using other mathematical operations, such as, multiplying, dividing, subtracting, etc.

5 Regardless of the algorithm used to calculate the verification signature, it is calculated using both the identifier value and a valuation of the message contents.

At step 422, the host server builds a message having the message contents in the message field and the verification signature in the verification field.

At step 424, the host server sends the message including the verification
10 signature to the gaming machine. In one embodiment, neither the message contents nor the verification signature are encrypted, however, in other embodiments, part of or all of the message may be encrypted, such as when personal information or other sensitive information is part of the message contents. For example, the identifier value may be used to generate a symmetric encryption key which is used to encrypt
15 the message. In another example, the gaming machine may have provided the host server with its public encryption key. An advantage of not using encryption is that the network traffic loads in the gaming network may be reduced and computation loads for the gaming devices may be reduced.

At step 426, the host server increments the identifier value stored in memory
20 according to some algorithm to produce a new identifier value. For example, the host server may increment the identifier value by one. As will be seen further herein, the gaming machine will also increment its stored identifier value according to the same algorithm. In this way, both the gaming machine and the host server will independently increment their identifier values after each message completion
25 until a connection disruption or re-initiate circumstance occurs, such as when the verification signature sent does not equal the check value calculated by the gaming machine.

In one embodiment, the identifier value, which may have been randomly generated, may be used to generate a sequence of message numbers. For instance,
30 the identifier value may be used as a seed in a random number generator. When both the gaming machine and the host server use the same seed in the same random number generator, the sequence of random numbers generated from the random number generators will be the same. In general, any numerical formula may be used

to generate a sequence of message numbers as long as both the gaming machine and the host server can reproduce the sequence of message numbers.

The numbers in the sequence of message numbers specified by the identifier value may be appended to the message contents and a message digest used in the verification signature may be generated from message contents. In another example, a first message digest may be generated from the message contents and a second message digest may be generated from the message number. The first message digest and the second message digest may be combined via a formula. For instance, the numbers may be simply added together or multiplied together to provide the verification signature for the message. The message number is not sent with the message contents. Therefore, an attacker that has intercepted the message with message contents and is attempting to generate a fake message with the message contents and a verification signature is not able to generate the correct verification signature unless it knows the message number used in the verification sequence.

In another embodiment, the sequence of message numbers may specify the algorithm used to generate the message digest used in the verification sequence. For example in a first message sequence, the first message may use a first hash algorithm to generate the verification signature, the second message may use a second hash algorithm to generate the verification signature and the third message may use a check-sum algorithm to generate the verification signature. In a second message sequence, the first message may use the second hash algorithm to generate the verification signature, the second message may use the check-sum algorithm to generate the verification signature and the third message may use the first hash algorithm to generate the verification signature. The order of which algorithms to use for each message the sequence of messages may be determined by the identifier value.

At step 428, the gaming machine receives the message.

At step 430, the gaming machine calculates a message digest from the message contents and a corresponding verification signature.

At step 432, the gaming machine determines when verification signature it has generated equals the verification signature sent in the message.

At step 434, if the verification signatures match, then the gaming machine accepts the message and forwards it on for further processing by the gaming machine, e.g., the message sender is identified.

At step 436, the gaming machine increments the stored identifier value
5 according to the same algorithm used by the host server and stores the incremented identifier value in its place.

Alternatively, if the gaming machine determines that the verification signature that it has generated does not equal the verification signature sent in the message, at step 438, the message is not accepted, and an alert message or a request
10 to reinitiate a connection with the gaming machine may be sent to the host server. It will be appreciated that the unaccepted message may also be simply discarded, however, this is not a preferred method of handling the unaccepted message as a legitimately sent message may have been corrupted during sending. Thus, it would be preferable to contact the sending host server of the disruption to allow a resend of
15 the message.

In one embodiment of the present invention, hardware serial numbers may be used to identify message senders. For instance, a MAC address from a devices network card may be used in the message identifying process. In other example, gaming machines usually store one or more unique serial numbers. The unique
20 serial numbers, which may be encrypted, may be used in the identifying process. For instance, a host server may store a table or list of unique serial numbers for each gaming machine and/or gaming device that may communicate with the host server. The unique serial number may be used with an algorithm to generate a message digest that is used in a verification signature. Thus, when the gaming machine
25 identifies itself in a message, the verification signature is compared to the verification signature expected from the gaming machine with the serial number identified in the message. For the gaming machine identified in the message, the host server may obtain the serial number using a table look-up. The verification signatures will only match when the correct serial numbers have been used.

30 As earlier described, prior to implementing the present invention, as described in FIGs. 4 and 5, encryption keys are loaded in both the host server and the gaming machines of the gaming network. Descriptions of these processes are briefly described below.

FIG. 6 is a flow diagram illustrating the key loading of the host server according to one embodiment of the present invention. As earlier described, the host server, at step 602, is loaded with a private encryption key which, at step 604, is stored in memory structure either in or associated with the host server. Loading of the private encryption key may be made in any of a variety of ways, such as through a network connection, via a hand held device, such as a key loader, individual key insertion, or wireless transmission. The host server may be loaded with other information depending on how the messages are identified. For instance, the host server may be loaded with a list of gaming device serial numbers used to identify the gaming devices, a list of public encryption keys used by different gaming devices and a list of public signature keys used by other gaming devices.

FIG. 7 is a flow diagram illustrating the key loading of the gaming machine according to one embodiment of the present invention. As earlier described, the gaming machines, at step 702, are loaded with a public encryption key which, at step 704, is stored in a memory structure in each gaming machine. Loading of the encryption key may be made in any of a variety of ways, such as through a network connection, via a hand held device, such as a key loader, individual key insertion, or wireless transmission. The gaming machine may be loaded with other information depending on how the messages are identified. For instance, the gaming machine may be loaded with a list of gaming device serial numbers used to identify the gaming devices, a list of public encryption keys used by different gaming devices, a list of public signature keys used by other gaming device, a private signature key and a private encryption key.

FIG. 8 is an illustration of a gaming network including a verification system according to one embodiment of the present invention. As illustrated, the gaming machines 802, as well as gaming machines 826-832, includes a gaming machine verification module 834 and the host server 824 includes a host verification module 836 that enable the implementation of the present invention, for example, as described with reference to FIGs. 3-7. Although the gaming machine verification module 834 is shown connected to the network 822 via the communication board 818, it will be appreciated that the module 834 may be differently connected so long as verification of the message sender can be implemented.

The present invention can be embodied in a wide variety of software and/or hardware implementations. FIGs. 9 and 10 described below, provide only one example of a host server verification module and of a gaming machine verification module that may be used in implementing the present invention.

5 FIG. 9 is a block diagram representation of a host server verification module according to one embodiment of the present invention. In the present embodiment, assume the host server requires a message to be sent to a gaming machine on the gaming network. The host server sends the message contents to the host server verification module 836. If there is no identifier value stored in memory, such as in
10 secure memory 910, the request generator 904 may generate a request to be sent to the gaming machine for an identifier value.

As earlier discussed, the response including the identifier value returned from the gaming machine may be encrypted either entirely or partially. Thus, when the identifier value is received, the module 836 will decrypt the identifier value
15 using a private key stored in memory 914. When decrypted, the identifier value may be stored in secure memory 910.

Verification signature generator 908 will generate a verification signature using a valuation of the message contents and the identifier value. The message generator 904 then generates a message including the message contents and the
20 verification signature to be sent from the host server to the gaming machine. Depending upon the message contents, for example, personal information, the message contents may be encrypted prior to sending.

FIG. 10 is a block diagram representation of a gaming machine verification module according to one embodiment of the present invention. When the gaming
25 machine receives the request, the gaming machine verification module 834 generates an identifier value at identifier value generator/incrementor 1006. The identifier value is stored in a memory structure, such as secure memory 1010.

The response generator 1004 then generates a response including the identifier value and encrypts the response and/or the identifier value using the public
30 key stored in memory 1014 of encryption module 1012. The response is then sent from the gaming machine verification module 834 to the gaming machine for sending to the host server.

When the gaming machine verification module 834 receives the message, including the message contents and verification signature, from the host server, it will first decrypt any encrypted portions using the public key stored in memory 1014 of encryption module 1012.

5 The check verification signature generator 1008 then generates a verification signature using the identifier value stored in memory 1010, the message contents and an appropriate algorithm. If the generated verification signature equals the verification signature received in the message, the message sender is verified, e.g., identified, and the message is accepted. The message is then communicated as
10 needed to the gaming machine components and the identifier value held in memory 1010 is incremented, for example, by one or according to some other algorithm, by the identifier value generator/incrementor 1006. The incremented value is then stored in memory, such as memory 1010.

 If the generated verification signature does not equal the verification
15 signature received in the message then the message is not accepted and the gaming machine verification module 834, may send an alert and or may request a reinitiate message to the host server, for example, utilizing the response generator 1004.

 For general communications between two gaming devices, each of the gaming devices may have two modules corresponding to a host server module 836
20 and the gaming machine verification module as described in FIGs. 8-10. Thus, either of the gaming devices may assume the role of the host or the gaming machine as previously described. An advantage of gaming devices with both modules, the gaming network may be configured more flexibly. For instance, gaming devices with both modules may act as hosts, clients or both host and clients.

25 Turning to FIG 11, a video gaming machine 2 of the present invention is shown. Machine 2 includes a main cabinet 4, which generally surrounds the machine interior (not shown) and is viewable by users. The main cabinet includes a main door 8 on the front of the machine, which opens to provide access to the interior of the machine. Typically, the main door 8 and/or any other portals which
30 provide access to the interior of the machine utilize a locking mechanism of some sort as a security feature to limit access to the interior of the gaming machine. Attached to the main door are player-input switches or buttons 32, a coin acceptor 28, and a bill validator 30, a coin tray 38, and a belly glass 40. Viewable through the

main door is a video display monitor 34 and an information panel 36. The display monitor 34 will typically be a cathode ray tube, high resolution flat-panel LCD, or other conventional electronically controlled video monitor. Further, the video display monitor 34 may be a touch screen. The touch screen may respond to inputs made by a player touching certain portions of the screen. The information panel 36 is a back-lit, silk screened glass panel with lettering to indicate general game information including, for example, the number of coins played. The bill validator 30, player-input switches 32, video display monitor 34, and information panel are devices used to play a game on the game machine 2. The devices are controlled by a master gaming controller (not shown) housed inside the main cabinet 4 of the machine 2. Many possible games, including traditional slot games, video slot games, video poker, and keno, may be provided with gaming machines of this invention.

The gaming machine 2 includes a top box 6, which sits on top of the main cabinet 4. The top box 6 houses a number of devices, which may be used to add features to a game being played on the gaming machine 2, including speakers 10, 12, 14, a ticket printer 18 which prints bar-coded tickets 20, a key pad 22 for entering player tracking information, a florescent display 16 for displaying player tracking information, a card reader 24 for entering a magnetic striped card containing player tracking information, and a video display screen 42. Further, the top box 6 may house different or additional devices than shown in the FIGs. 11. For example, the top box may contain a bonus wheel or a back-lit silk screened panel which may be used to add bonus features to the game being played on the gaming machine. During a game, these devices are controlled, in part, by the master gaming controller (not shown) housed within the main cabinet 4 of the machine 2.

Understand that gaming machine 2 is but one example from a wide range of gaming machine designs on which the present invention may be implemented. For example, not all suitable gaming machines have top boxes or player tracking features. Further, some gaming machines have only a single game display – mechanical or video, while others are designed for bar tables and have displays that face upwards. As another example, a game may be generated in on a host computer and may be displayed on a remote gaming terminal or a remote gaming device. The remote gaming device may be connected to the host computer via a network of

some type such as a local area network, a wide area network, an intranet or the Internet. The remote gaming device may be a portable gaming device such as but not limited to a cell phone, a personal digital assistant, and a wireless game player. Thus, those of skill in the art will understand that the present invention, as described
5 below, can be deployed on most any gaming machine now available or hereafter developed.

Returning to the example of Figure 11, when a user wishes to play the gaming machine 2, he or she inserts cash through the coin acceptor 28 or bill validator 30. At the start of the game, the player may enter playing tracking
10 information using the card reader 24, the keypad 22, and the florescent display 16. Further, other game preferences of the player playing the game may be read from a card inserted into the card reader. During the game, the player views game information using the video display 34. Other game and prize information may also be displayed in the video display screen 42 located in the top box.

15 During the course of a game, a player may be required to make a number of decisions, which affect the outcome of the game. For example, a player may vary his or her wager on a particular game, select a prize for a particular game, or make game decisions which affect the outcome of a particular game. The player may make these choices using the player-input switches 32, the video display screen 34
20 or using some other device which enables a player to input information into the gaming machine. During certain game events, the gaming machine 2 may display visual and auditory effects that can be perceived by the player. These effects add to the excitement of a game, which makes a player more likely to continue playing. Auditory effects include various sounds that are projected by the speakers 10, 12,
25 14. Visual effects include flashing lights, strobing lights or other patterns displayed from lights on the gaming machine 2 or from lights behind the belly glass 40. After the player has completed a game, the player may receive game tokens from the coin tray 38 or the ticket 20 from the printer 18, which may be used for further games or to redeem a prize. Further, the player may receive a ticket 20 for food, merchandise,
30 or games from the printer 18.

FIG. 12 is a block diagram of networked gaming machines and gaming devices that may exchange messages that are identified using the apparatus and methods of the present invention. Messages may be exchanged between one or more

of the gaming devices and the methods and apparatus of the present invention may be used to identify the message sender. A master gaming controller 224 is used to present one or more games of chance on the gaming machines 61, 62 and 63. The master gaming controller 224 in a gaming machine may also communicate with
5 other gaming devices in the gaming network, such as the game server 90, other gaming machines, a cashless system server 99, a player tracking accounting server 96, a bonus server 94, remote file storage devices 81 and 82, devices linked to the gaming machine via the internet 97 or devices linked to the gaming machine via a wide area progressive network 98.

10 For linked game play involving a plurality of linked gaming machines, a game server 90 with a game controller 92 and/or the bonus server 94 may be used to generate the outcomes of games of chance and/or bonus games which may be displayed on the plurality of gaming machines such as 61, 62 and 63. The game server 90 may also be used to download gaming software and gaming information
15 to each of the gaming machines. The outcomes of bonus games and other linked games may be based upon game play generated on the plurality of gaming machines in communication with the game server 90. The communication between gaming machines 61, 62, 63 and the bonus server 94 and/or game server 90 may require that the senders of the messages are identified and for a sequence of messages an
20 appropriate signature is assigned to each message.

The master gaming controllers 224 may communication with devices located outside of the gaming machines by using the main communication board 215 and network connections 71. The network connections 71 may allow communications with remote gaming devices via a local area network, an intranet, the Internet or
25 combinations thereof. The game server 90 and bonus game server 94 may also communicate with a number of game devices via the network connections 71 such as but not limited to the gaming machines 61, 62 and 63, the player tracking accounting server 96, the cashless system server 99 and the remote file storage devices 81 and 82. In general, the methods and apparatus of the present invention
30 may be used to identify message senders between any two gaming devices that communicate with one another.

The gaming machines 61, 62 and 63 may use gaming software modules to generate a game of chance that are distributed between local file storage devices and

remote file storage devices. For example, to play a game of chance on gaming machine 61, the master gaming controller may load gaming software modules into RAM 56 that may be located in 1) a file storage device 226 on gaming machine 61, 2) a game server 90, 3) a file storage device 226 on gaming machine 62, 4) a file storage device 226 on gaming machine 63, 5) the remote file storage devices 81 and 82 or 6) combinations thereof. In one embodiment of the present invention, the gaming operating system may allow files stored on the local file storage devices and remote file storage devices to be used as part of a shared file system where the files on the remote file storage devices are remotely mounted to the local file system. The file storage devices may be a hard-drive, CD-ROM, CD-DVD, static RAM, flash memory, EPROM's, compact flash, smart media, disk-on-chip, removable media (e.g. ZIP drives with ZIP disks, floppies or combinations thereof. For both security and regulatory purposes, gaming software executed on the gaming machines 61, 62 and 63 by the master gaming controllers 224 may be regularly verified by comparing software stored in RAM 56 for execution on the gaming machines with certified copies of the software stored on the gaming machine (e.g. files may be stored on file storage device 226), accessible to the gaming machine via a remote communication connection. The transfer of software between devices may be enabled by the methods of the present invention, which allow an identity of a sender of data to be identified.

The game server 90 may also be a repository for game software modules and software for other game services provided on the gaming machines 61, 62 and 63. In one embodiment of the present invention, the gaming machines 61, 62 and 63 may download game software modules from the game server 90 to a local file storage device to play a game of chance. The downloading of game software may be initiated by the game server 90, the gaming machines 61, 62 and 63, a remote gaming device or combinations thereof. One example of a game server that may be used with the present invention is described in co-pending U.S. patent application 09/042,192, filed on 6/16/00, entitled "Using a Gaming Machine as a Server" which is incorporated herein in its entirety and for all purposes. In another example, the game server might also be a dedicated computer or a service running on a server with other application programs.

In one embodiment of the present invention, the processors used to generate a game of chance may be distributed among different machines. For instance, the game flow logic to play a game of chance may be executed on the game server 90 by the processors 92 while the game presentation logic for the game may be executed on gaming machines 61, 62 and 63 by the master gaming controllers 224. The gaming operating systems on gaming machines 61, 62 and 63 and the game server 90 may allow gaming events to be communicated between different gaming software modules executing on different gaming machines via defined APIs. The communication of gaming events between gaming machines and gaming devices may require that the senders of the message are identified. Details a gaming software architecture that describes the game flow logic and the presentation logic used in the present invention are described in co-pending U.S. application no. 10/040, 239, filed on September 28, 2001, by LeMay, et al., and entitled, "Game Development Architecture That Decouples The Game Logic From The Graphics Logic," which is incorporated herein in its entirety and for all purposes.

After the identities of communicating gaming devices has been established, a game flow software module executed on the trajectory-based game server 90 may send gaming events to a game presentation software module executed on gaming machine 61, 62 or 63 to control the play of a game of chance, to control the play of a bonus game of chance presented on gaming machines 61, 62 and 63. As another example, the gaming machines 61, 62 and 63 may send gaming events to one another via network connection 71 to control the play of the shared bonus game played simultaneously on the different gaming machines.

As illustrated in the foregoing description and drawings, the present invention provides identification of message sender on a gaming network utilizing a verification signature generated using both the message contents and an identifier value.

Although the foregoing invention has been described in some detail for purposes of clarity of understanding, it will be apparent that certain changes and modifications may be practiced within the scope of the appended claims. For instance, while the gaming machines of this invention have been depicted as having a top box mounted on top of the main gaming machine cabinet, the use of gaming devices in accordance with this invention is not so limited. For example, a gaming

machine may be provided without a top box, or may have additional boxes or devices attached, or may be configured in bar tops, table tops, or other structures.

Further, the location of the signature input devices on the gaming machine may vary widely in different embodiments, thus, the examples described herein are not

- 5 intended to be limiting of the present invention. Additionally, the gaming machine may be designed as a stand alone gaming device or networked with other gaming devices including other servers or gaming devices over the Internet or through other wired and wireless systems.

CLAIMS

What is claimed is:

1. A method of communicating between two gaming devices on a gaming machine network, the method comprising:
 - 5 sending a request for a first identifier value from a first gaming device to a second gaming device, the first gaming device having message contents to be sent to the second gaming device;
 - receiving the first identifier value from the second gaming device;
 - generating a verification signature at the first gaming device using a
 - 10 valuation of the message contents and the first identifier value; and
 - sending the message contents and the verification signature from the first gaming device to the second gaming device.
 2. The method of claim 1, further comprising:
 - storing the first identifier value in a memory structure at the first gaming
 - 15 device.
 3. The method of claim 1, further comprising:
 - receiving a request from the second gaming device to resend the message contents and the verification signature;
 - resending the message contents and the verification signature.
 - 20 4. The method of claim 1, further comprising:
 - sending a plurality of messages to the second gaming device from the first gaming device, the sending of each message comprising:
 - generating a message identifier value;
 - generating a message verification signature using a valuation of the
 - 25 message contents and the message identifier value; and
 - generating a message with the message contents and the message verification signature.
 - wherein the message identifier value generated in each message is from a sequence of identifier values that are known by the second gaming device.
 - 30 5. The method of claim 4, wherein the sequence of identifier values is a random number sequence generated using a random number generator seeded with the first identifier value.

6. The method of claim 4, wherein a message verification algorithm used to generate the message verification signature changes from message to message.
7. The method of claim 1, wherein the verification signature is generated using a private signature key.
- 5 8. The method of claim 1, wherein the message contents and the verification signature are sent from the host server to the target gaming machine according to a protocol comprising at least:
- a message field containing the message contents, and
 - a verification field containing the first verification signature.
- 10 9. The method of claim 1, further comprising:
- decrypting the first identifier value using a private encryption key.
10. The method of claim 1, further comprising:
- generating a symmetric encryption key;
 - encrypting the symmetric encryption key using a public encryption key from
- 15 the second gaming device;
- encrypting the message contents using the symmetric encryption key;
 - and sending the encrypted symmetric encryption key to the second gaming device.
11. The method of claim 1, further comprising:
- 20 identifying the second gaming device.
12. The method of claim 11, wherein the second gaming device is identified using a unique hardware serial number stored on the first gaming device.
13. The method of claim 1, wherein the first gaming device is a gaming machine and the second gaming device is a gaming machine.
- 25 14. The method of claim 1, wherein the first gaming device is a host server and the second gaming device is a gaming machine.
15. The method of claim 1, wherein first gaming device is selected from the group consisting of a gaming machine, a cell phone, a personal digital assistant, a host server, a remote computer and a portable gaming device.
- 30 16. The method of claim 1, wherein second gaming device is selected from the group consisting of a gaming machine, a cell phone, a personal digital assistant, a host server, a remote computer and a portable gaming device.

17. The method of claim 1, wherein the message contents are at least one of player tracking information, accounting information, bonus game information, a game event from a game of chance played on a gaming machine, electronic fund transfer information, gaming software and combinations thereof.
- 5 18. A method of communicating between two gaming devices on a gaming machine network, the method comprising:
- receiving a request at the first gaming device from a second gaming device for a first identifier value wherein the first gaming device has message contents to be sent to the second gaming device;
- 10 generating a first identifier value;
- sending the first identifier value to the second gaming device;
- receiving a first message comprising the message contents and a verification signature from the second gaming device;
- generating a second verification signature using the message contents and
- 15 the stored first identifier value; and
- determining whether the second verification signature is equal to the verification signature, and if equal, accepting the first message for further processing by the gaming machine.
19. The method of claim 18, further comprising:
- 20 storing the first identifier value in a memory structure at the second gaming device.
20. The method of claim 18, further comprising:
- rejecting the verification signature and
- terminating the processing of the first message.
- 25 21. The method of claim 18, further comprising:
- encrypting the first identifier value prior to sending it to the second gaming device.
22. The method of claim 21, wherein the first identifier value is encrypted using a public encryption key for the second gaming device.
- 30 23. The method of claim 18, further comprising:
- authenticating an identify of the second gaming device.
24. The method of claim 23, wherein the identity of the second gaming device is authenticated using a serial number supplied by the second gaming device.

25. The method of claim 23, wherein the identity of the second gaming device is authenticated using a public signature key provided by the second gaming device.
26. The method of claim 18, further comprising:
generating the second verification signature using a public signature key
5 corresponding to a private signature key used by the second gaming device to generate the verification signature.
27. The method of claim 18, further comprising:
decrypting at least one of the a portion of the message contents, the verification signature and combinations thereof.
- 10 28. The method of claim 27, wherein the at least one of the portion of the message contents, the first verification and combinations thereof have been encrypted with a public encryption key corresponding to a private encryption key used by the first gaming device.
29. The method of claim 18, further comprising:
15 receiving a plurality of messages from the second gaming device, the receiving of each message comprising:
receiving first message contents and a first verification signature for each of the plurality of message;
determining a message identifier value in a sequence of message
20 identifier values used to generate the first verification signature;
generating a message verification signature using a valuation of the message contents and the message identifier value; and
determining whether the first verification signature is equal to the message verification signature.
- 25 30. The method of claim 18, wherein the first gaming device is a gaming machine and the second gaming device is a gaming machine.
31. The method of claim 18, wherein the first gaming device is a host server and the second gaming device is a gaming machine.
32. The method of claim 18, wherein first gaming device is selected from the
30 group consisting of a gaming machine, a cell phone, a personal digital assistant, a host server, a remote computer and a portable gaming device.

33. The method of claim 18, wherein second gaming device is selected from the group consisting of a gaming machine, a cell phone, a personal digital assistant, a host server, a remote computer and a portable gaming device.

34. The method of claim 18, wherein the message contents are at least one of
5 player tracking information, accounting information, bonus game information, a game event from a game of chance played on a gaming machine, electronic fund transfer information, gaming software and combinations thereof.

35. A gaming machine network comprising:

at least one host server, the host server including verification software that
10 enables the host server to obtain an identifier value from a gaming machine, and in response to obtaining the identifier value, enables the host server to generate a message according to a protocol that permits the gaming machine to identify a sender of the message;

a plurality of gaming machines, each gaming machine comprising:

15 a master gaming controller configured to control one or more games of chance played on the gaming machine,

a memory configured to store a plurality of verification software elements that allow the gaming machine to identify the sender of a message on the gaming machine network; and

20 a network allowing communication between the host server and the plurality of gaming machines.

36. The gaming machine network of claim 35, wherein the protocol further comprises:

a message field; and

25 a verification field.

37. The gaming machine network of claim 36, wherein the message field contains message contents and the verification field contains a verification signature.

38. The gaming machine network of claim 37, wherein the verification signature
30 is generated using a valuation of the message contents and the identifier value.

39. The gaming machine network of claim 35, wherein the host server further comprises:

host server encryption software for decrypting the identifier value encrypted by the gaming machine and for encrypting, as needed, at least a portion of the message sent to the gaming machine.

40. The gaming machine network of claim 39, wherein the host server
5 encryption software utilizes a private encryption key.

41. The gaming machine network of claim 35, wherein the gaming machine further comprises:

- gaming machine encryption software for encrypting the identifier value prior to sending to the host server and for decrypting, as needed, at least a portion of the
10 message encrypted by the host server.

42. The gaming machine network of claim 41, wherein the gaming machine encryption software utilizes a public key.

43. The gaming machine network of claim 35, wherein the verification software further comprises:

- 15 verification signature generation software for generating a verification signature.

44. The gaming machine network of claim 43, wherein the verification signature generation software utilizes at least one of a private signature key, the identifier value, message contents and combinations thereof to generate the verification
20 signature.

45. The gaming machine network of claim 35, wherein the verification software elements further comprise:

verification signature authentication software elements for determining the authenticity of a verification signature.

- 25 46. The gaming machine network of claim 45, wherein the verification signature authentication software utilizes at least one of a public signature key, the identifier value, message contents and combinations thereof to authenticate the verification signature.

47. The gaming machine network of claim 35, wherein the host server and the
30 plurality of gaming machines further comprise:

identifier generation software for generating a sequence of message identifier values that are used to generate verification signatures for a sequence of messages.

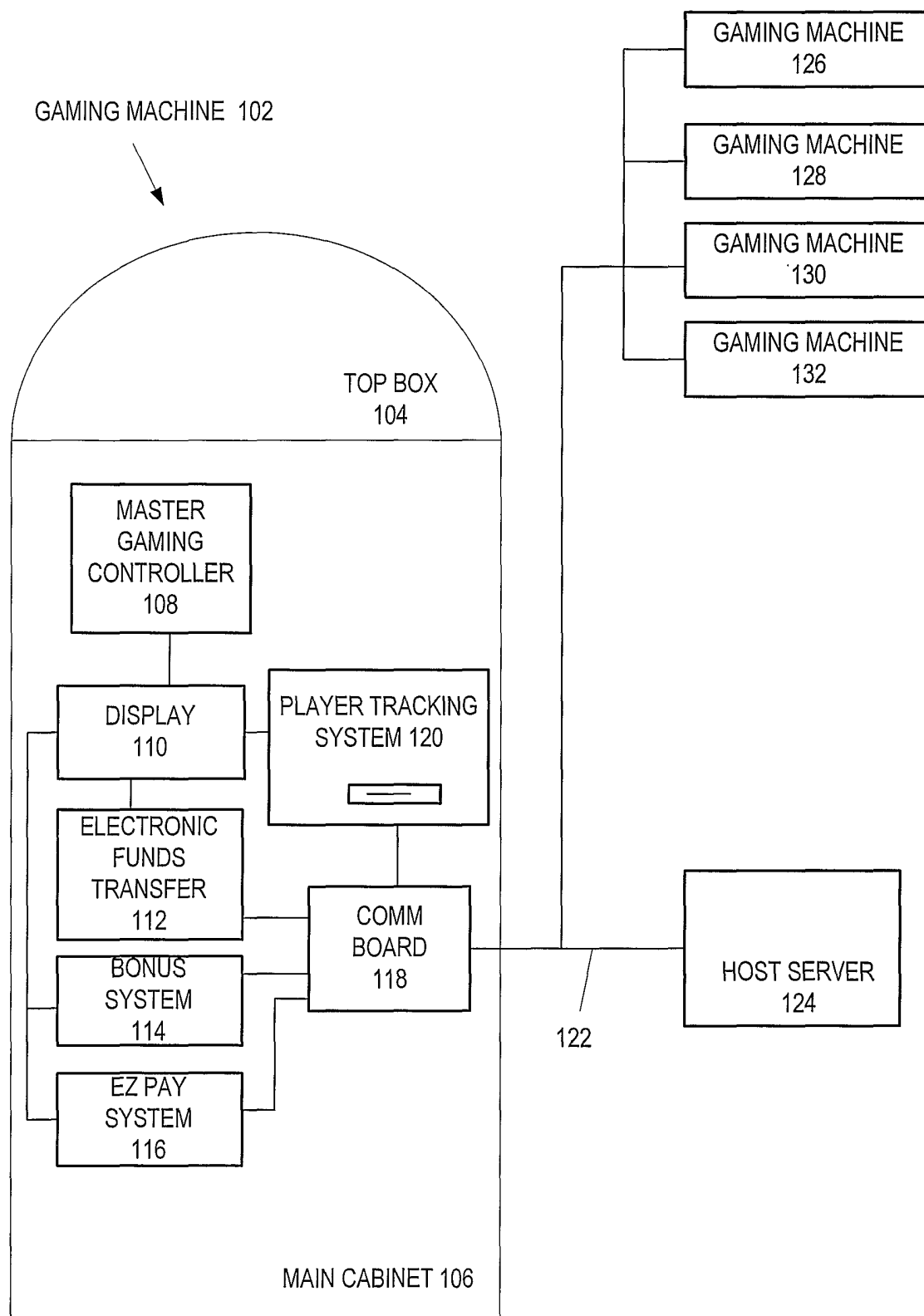


FIG. 1
(PRIOR ART)

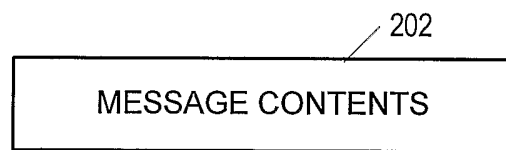


FIG. 2
(PRIOR ART)

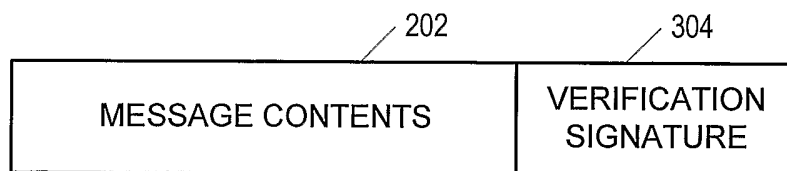


FIG. 3

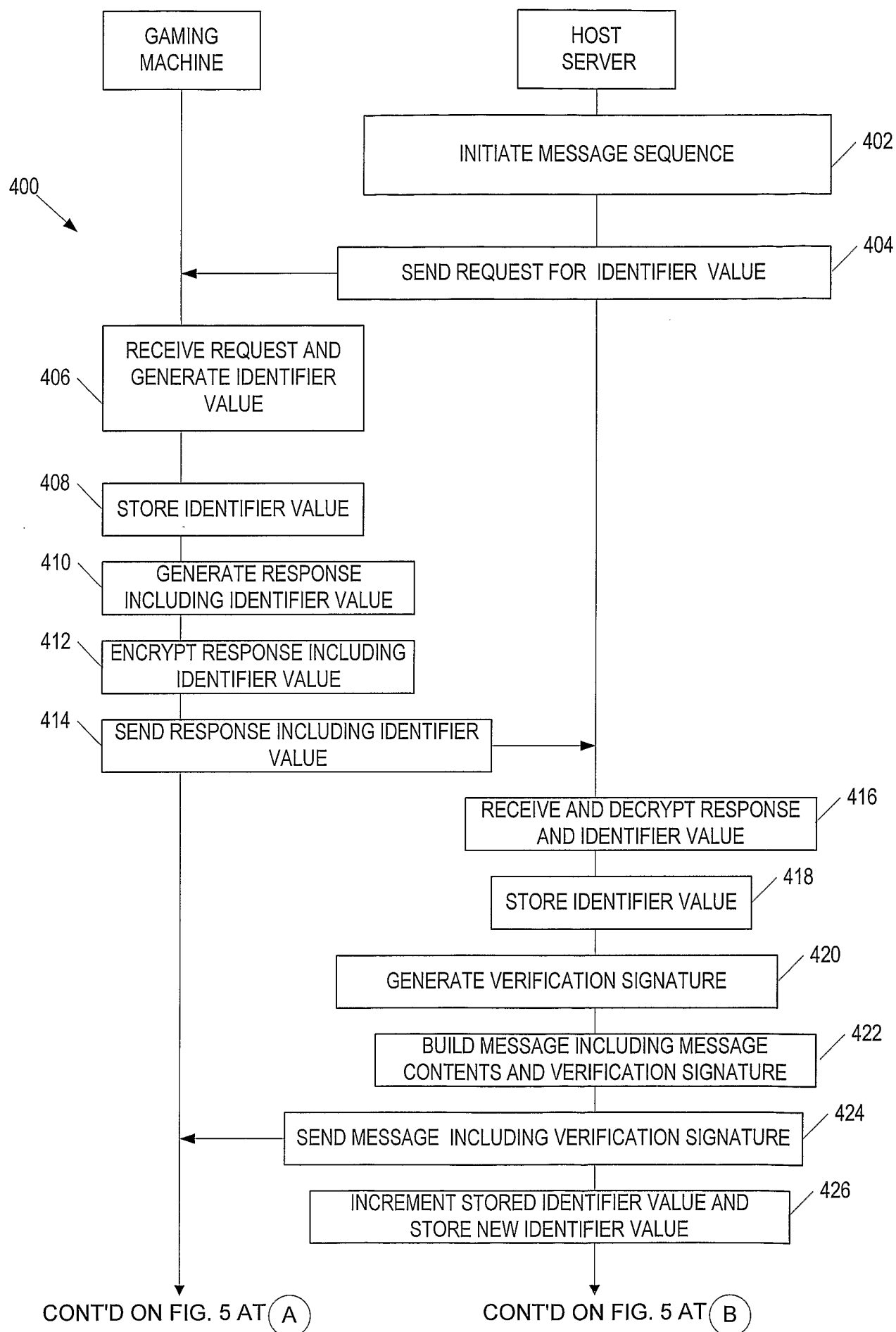


FIG. 4

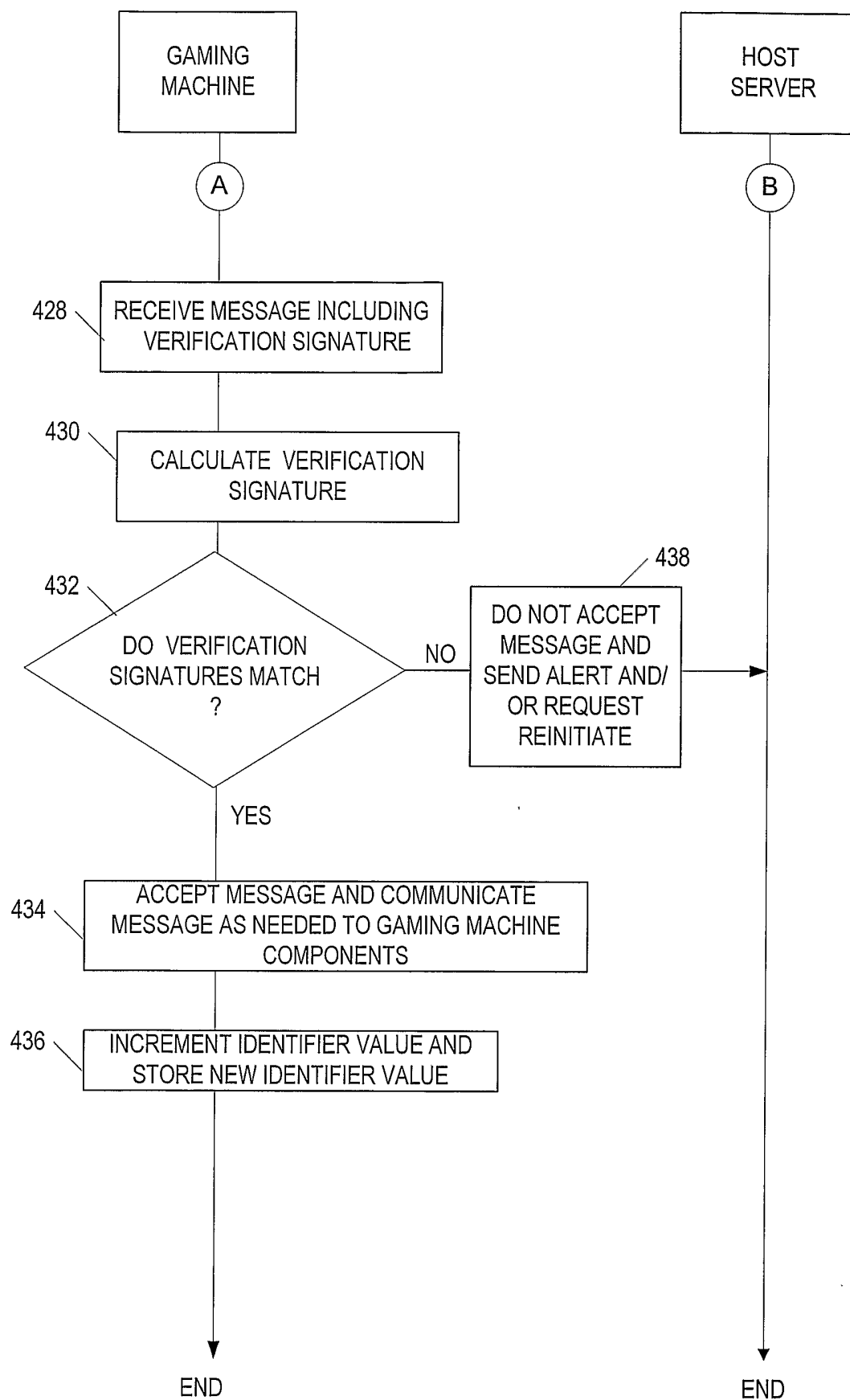


FIG. 5

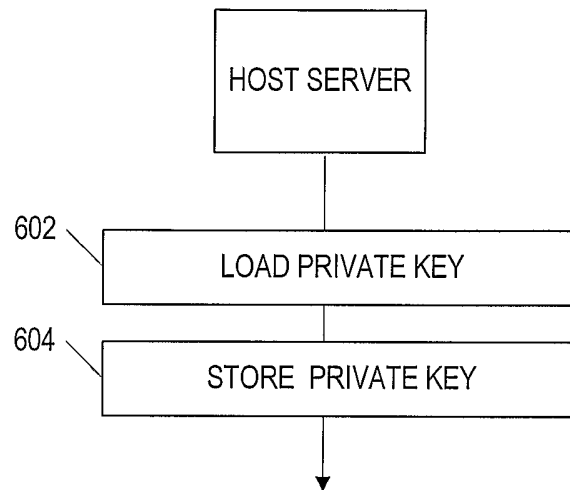
HOST SERVER KEY
LOADING

FIG. 6

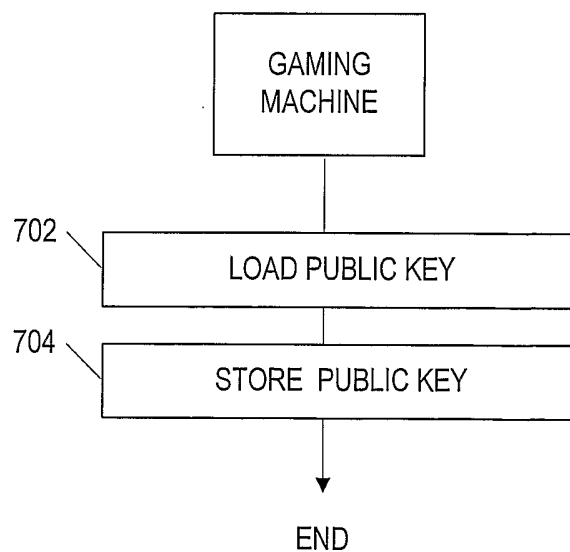
GAMING MACHINE KEY
LOADING

FIG. 7

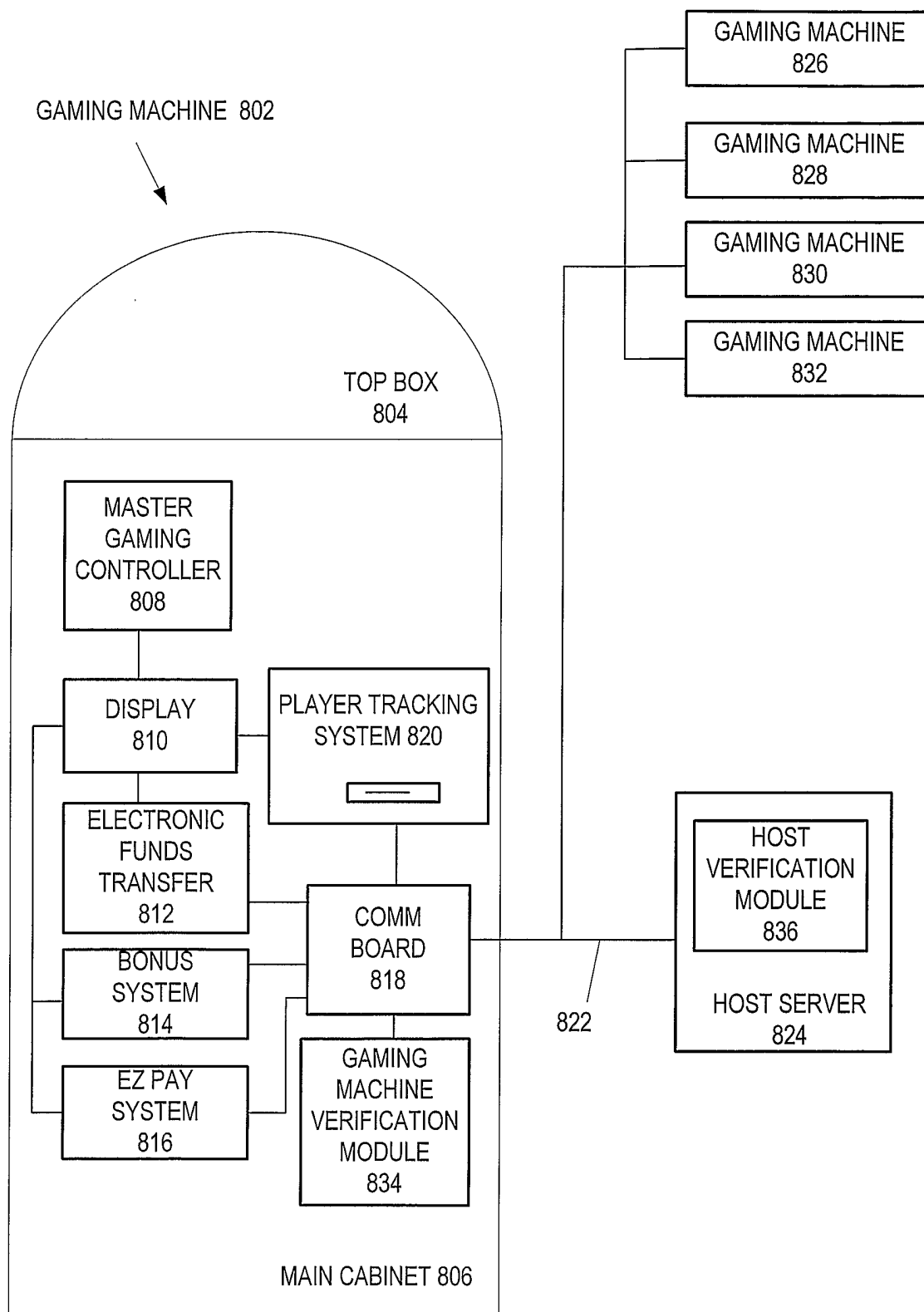


FIG. 8

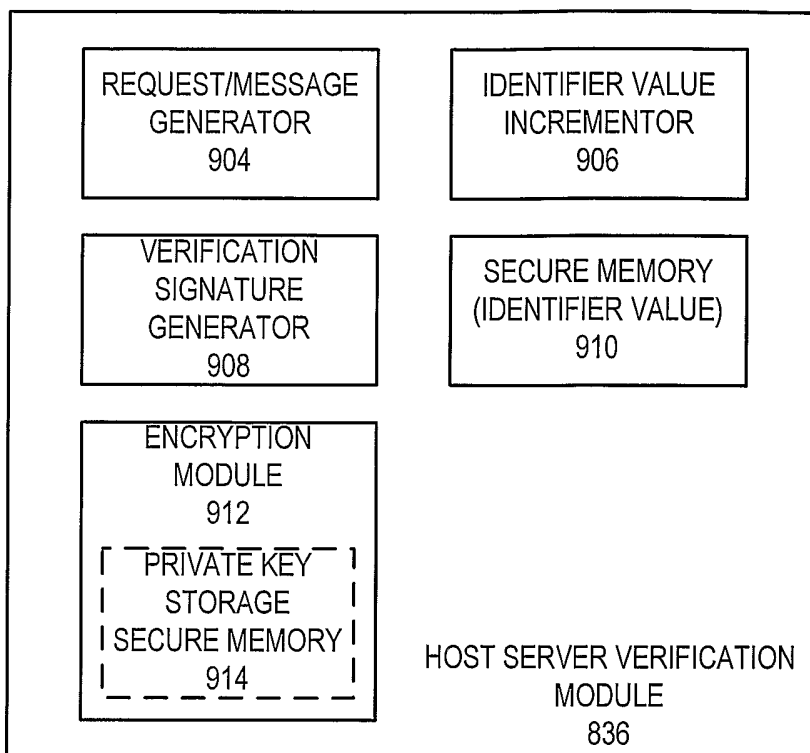


FIG. 9

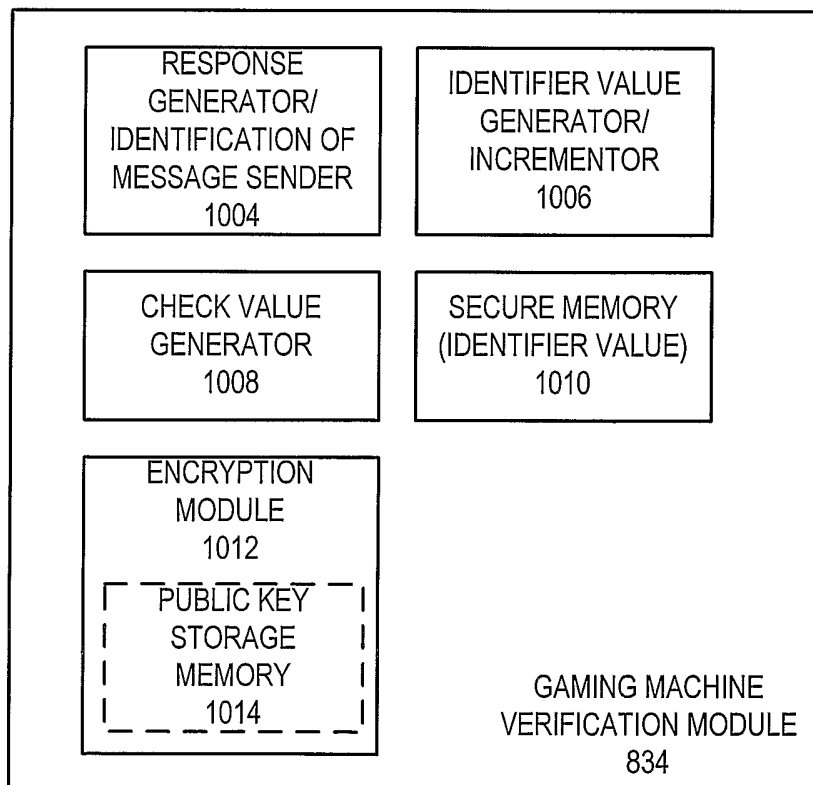


FIG. 10

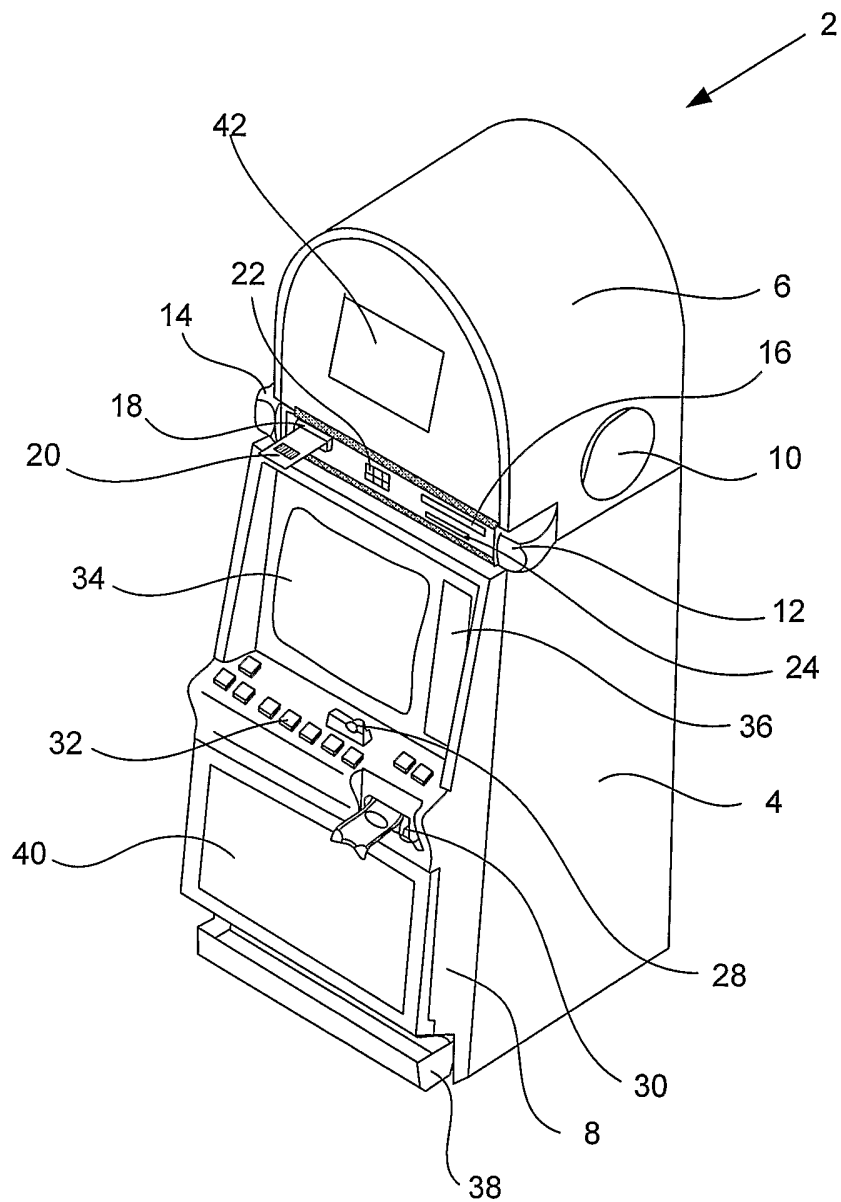


FIG. 11

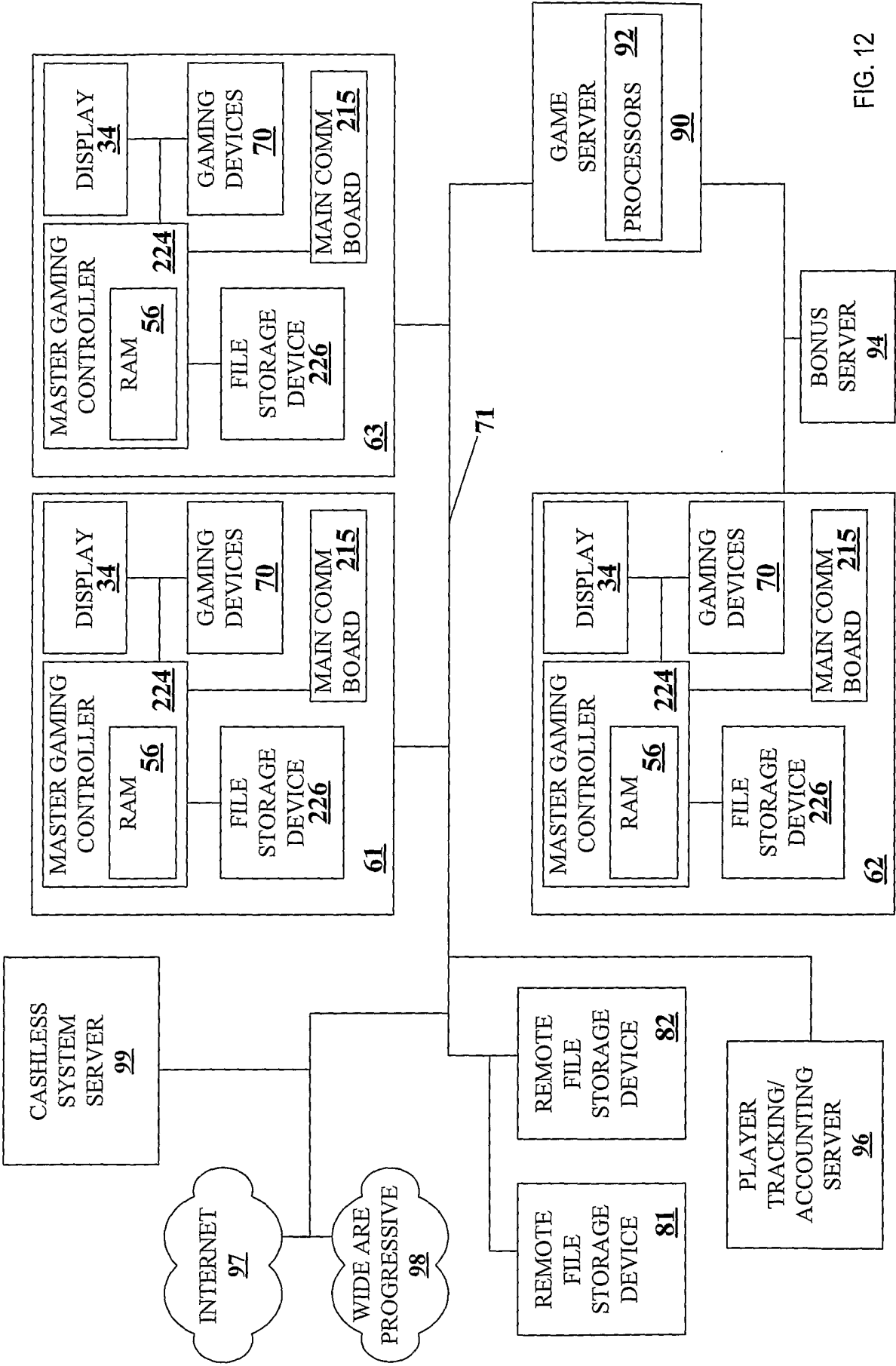


FIG. 12

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 03/32874

A. CLASSIFICATION OF SUBJECT MATTER IPC 7 G06F1/00 G07F7/00 G07F17/32		
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) IPC 7 G06F G07F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CHRUS MITCHELL: "Authentication Using Cryptography" INFORMATION SECURITY TECHNICAL REPORT, vol. 2, no. 2, 1997, pages 25-32, XP002274759 the whole document	1-47
X	A. BEUTELSPACHER: "Kryptologie" 1996, VIEWEG, BRAUNSCHWEIG, XP002274760 page 82 - page 85 page 113 - page 115 page 136	1-47
X	A. MENEZES: "Handbook of Applied Cryptography" 1997, CRC PRESS, BOCA RATON, XP002274761 page 400 - page 405	1-47
-/--		
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C. <input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents : *A* document defining the general state of the art which is not considered to be of particular relevance *E* earlier document but published on or after the international filing date *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) *O* document referring to an oral disclosure, use, exhibition or other means *P* document published prior to the international filing date but later than the priority date claimed *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. *&* document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
24 March 2004		14/04/2004
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016		Authorized officer
		Neppel, C

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 03/32874

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/116615 A1 (PARROTT GREGORY HOPKINS ET AL) 22 August 2002 (2002-08-22) paragraph '0142! - paragraph '0153! -----	1,18,35
A	BAUSPIESS F ET AL: "REQUIREMENTS FOR CRYPTOGRAPHIC HASH FUNCTIONS" COMPUTERS & SECURITY, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, vol. 11, no. 5, 1 September 1992 (1992-09-01), pages 427-437, XP000296996 ISSN: 0167-4048 -----	1-47
A	US 5 643 086 A (ALCORN ALLAN E ET AL) 1 July 1997 (1997-07-01) -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 03/32874

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002116615 A1	22-08-2002	US 2002071557 A1	13-06-2002
		WO 03085613 A1	16-10-2003
		AU 9715401 A	13-06-2002
		CA 2364424 A1	07-06-2002
US 5643086 A	01-07-1997	AU 6282096 A	30-01-1997
		CA 2225805 A1	16-01-1997
		CN 1191644 A	26-08-1998
		EP 0882339 A1	09-12-1998
		JP 2002515765 T	28-05-2002
		TR 9701723 T1	21-04-1998
		WO 9701902 A1	16-01-1997
		US 6149522 A	21-11-2000
		US 2004002381 A1	01-01-2004
		US 6620047 B1	16-09-2003
		US 6106396 A	22-08-2000
		ZA 9700320 A	22-09-1997