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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 April 2006 (13.04.2006)

PCT

(10) International Publication Number
WO 2006/037220 A1

(51) International Patent Classification[7]: G07F 17/32, 1/06, G06K 19/07

(21) International Application Number:
PCT/CA2005/001519

(22) International Filing Date:
30 September 2005 (30.09.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/614,957 1 October 2004 (01.10.2004) US

(71) Applicant *(for all designated States except US)*: **UBI-TRAK INC.** [CA/CA]; 740 St-Maurice, Suite 201, Montreal, Quebec H3C 1L5 (CA).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **RICHARD, Christian** [CA/CA]; 203 Lagacé, Dorval, Quebec H9S 2L9 (CA).

(74) Agent: **ROBIC**; Centre CDP Capital, 1001 VCictoria Square, Bloc E - 8th Floor, Montreal, Quebec H2Z 2B7 (CA).

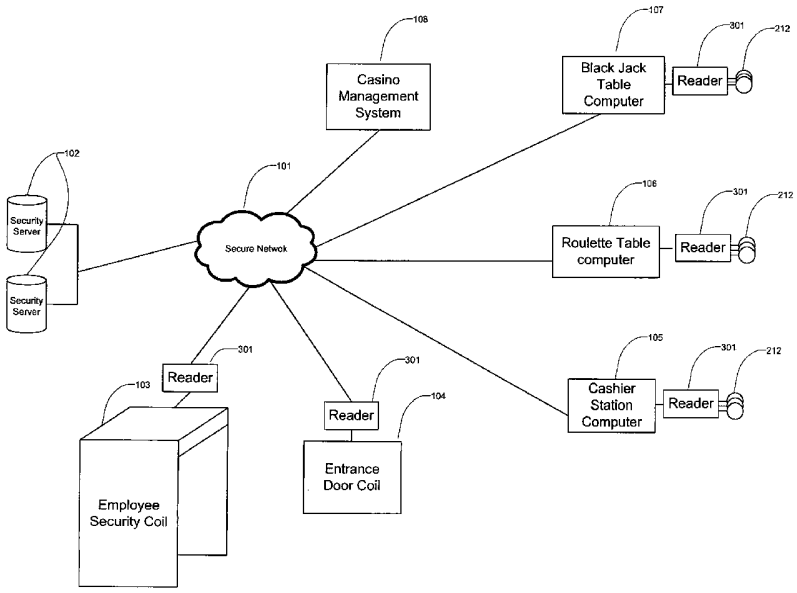
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK,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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

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

(54) **Title:** SECURITY SYSTEM FOR AUTHENTICATING GAMING CHIPS



(57) **Abstract:** A system for authenticating RFID-capable gaming chips in a casino. The system includes at least one security server, at least one secure network, a casino management system and a plurality of magnetic couplers distributed within the casino. The gaming chips are adapted to provide a response to a challenge issued by the magnetic couplers when the chips are located in the vicinity of the magnetic couplers. The chip is authenticated when the response matches a computed response by the server. Preferably, the authentication information is loaded into the chip prior to the chip being used in the casino. The response preferably takes the form of a one time password, so that when the password list is depleted within the chip, the chip must be re-commissioned.

WO 2006/037220 A1

SECURITY SYSTEM FOR AUTHENTICATING GAMING CHIPS

Technical field

This invention relates to the use of cryptographic algorithms for the authentication of RFID capable devices used within casino environment and, more specifically to the cryptographic authentication of RFID capable gaming chips.

Background of the invention

Among all the approaches and measures that have been presented in the past years as concrete solutions for deterring counterfeiting and prevent unlawful and fraudulent wins within casinos, RFID-based solutions have received the greatest attention from both the industry and research communities.

Radio Frequency Identification technology is currently widely used in multiple industry sectors including manufacturing, transportation, postal tracking, medical, pharmaceutical and highway toll management. A typical RFID system configuration comprises an RFID transponder usually located on the object to be identified, an RFID interrogator or reader and a computing device. The interrogator is typically made of a radio frequency module, a control unit and a coupling element that transfers a sufficient amount of energy to the transponder. The transponder actually carries the data and it normally consists of a coupling element and an electronic microchip.

Several patents pertaining to RFID-based casino gaming chip monitoring for anti-counterfeiting purposes and player tracking have been issued. U.S. Pat. No. 5,166,502 (Rendelman et al.) shows a construction of radio frequency transponder embedded in a gaming chip. The transponder is tagged with information

concerning the chip such as chip identity and value. The particular transponder described in that patent was specifically designed to work with slot machines. However, extending the application field of afore mentioned chip to gaming tables such as black jack tables or baccarat was not considered in this patent, and it would not work because the information contained in the chip cannot be changed.

In U.S. Pat. Nos. 5, 651,548 and 5, 735,742, French et al. present other RFID-based apparatus and methods of tracking gaming chip movement within casinos. These methods address the flaws of the previous patent by allowing chip tracking at various places within the casino including gaming tables and chip trays. Possibility of reading and writing in the integrated circuit containing token information is also explored. However, the solution proposed by French et al. will not prevent malicious players from impersonating a genuine RFID capable gaming chip. In fact, the method described by French et al. does not address security issues at all; hence, intercepting the communication between the interrogating device and the gaming chip and subsequently resending the intercepted serial number through the means of an easily constructed mini-sender is made quite easy. This and other powerful attacks on RFID capable devices have proven that relying solely on the uniqueness of the chip serial number is not enough to ensure security and thus prevent chip replication.

Some security approaches devised in the past for chip memory content protection were essentially limited to string of security bits which could be irreversibly toggled by the RFID device. If this approach is successful in preventing writing into a specific memory location, it would not prevent reading from that memory location.

Summary of the invention

In summary, the present invention discloses system and methods that prevent gaming chip counterfeiting, RFID capable gaming chip tampering and RFID

capable gaming chip impersonation. Further, the present invention enforces RFID capable gaming chips validity assessment at gaming tables, cashier stations or at any other location within the casino where assessing the validity of the gaming chip is required.

Thus, it is an object of the present invention is to provide a security system for casino gaming chips authentication. In accordance with this object, there is provided a system for authenticating RFID-capable gaming chips in a casino, said system comprising at least one security server, at least one secure network, a casino management system and a plurality of magnetic couplers distributed within the casino, wherein said gaming chips are adapted to provide a response to a challenge issued by said magnetic couplers when said chips are located in the vicinity of said magnetic couplers, whereby said chip is authenticated when said response matches a computed response by said server.

In accordance with another aspect of the invention, there is provided a method for authenticating RFID-capable gaming chips within a casino, comprising the steps of:

(a) commissioning said chips at a commissioning station, including loading into said chip authentication information;
(b) providing a plurality of magnetic couplers distributed in said casino;
(c) issuing a challenge from said magnetic couplers to said chips when said chips are located in the vicinity of said magnetic couplers;
(d) receiving a response from said chip;
(e) comparing said response to a computed response; and
(f) authenticating said chip when said response matches said computed response.

In accordance with yet another aspect of the invention, there is provided a method for authenticating an RFID reader to a gaming chip within the casino comprising:

the gaming chip issuing a challenge to the RFID reader;

the gaming chip receiving a response from the RFID reader;
comparing said response to a computed response; and
authenticating the reader when said response matches said computed response.

Using such authentication it can be guaranteed that a gaming chip used within the casino will partly or entirely disclose the security critical information to an interrogating device only after successful assessment that the interrogating device is indeed legitimately empowered to access this security information. Similarly, using such authentication will help assessing that any RFID capable gaming chip used at a gaming table or at any other location within the casino actually contains legitimate security information introduced into the gaming chip memory during commissioning or at any other time by legitimate staff within the casino. This means that any tampering with the gaming chip memory content will be detected. A gaming chip authentication system as disclosed in the invention will impede malicious players from dissimulating fake gaming chips--that is, those gaming chips with a valid serial number but invalid security code or temporarily stolen security code—among valid gaming chips.

Another object of the present invention is to provide a gaming chip authentication security system that uses a set of secrets whereby each secret out of the set can be used only a predefined number of times. This may include for example using the secret only once. In this case the secret is considered to be one-time password and the term one-time password will be used for this type of secrets interchangeably.

Another object of the invention is to describe a method for changing the authentication secret on a regular basis following a predefined time schedule specified by legitimate casino staff.

The details of one or more embodiments of the invention are set forth in the accompanying drawings and the description below.

Brief description of the drawings

These and other objects and advantages of the invention will become apparent upon reading the detailed description and upon referring to the drawings in which:

Figure 1 is an overall view of a security system for gaming chip authentication as disclosed in the current invention.

Figure 2 is a schematic view of a gaming table with embedded magnetic couplers and communication channel between the table and the central server.

Figures 3A and 3B are transactional views of one embodiment of the methods described in this invention.

Figure 4 is a functional view of the information exchange that occurs between the reader and the chip.

Figures 5A and 5B are transactional views of another embodiment of the methods described in this invention.

Figures 6A and 6B are transactional views of yet another embodiment of the methods described in this invention.

Description of preferred embodiments of the invention

Embodiments of the security system for gaming chip authentication used in casino to ensure that the chip circulating within the casino and used at the gaming tables are genuine will typically encompass RFID capable gaming tables as described in International application no. PCT/CA2005/001338 filed on September 1, 2005 by the Applicant, which is hereby incorporated by reference.

The embodiments of the security system for gaming chip authentication rely on the existence of a data network within the casino to ensure that legitimate casino staff has properly commissioned the chip used within the casino. It assumed that the network is secure and data traveling though the network from one node to another suffers no additional delay except the propagation time. The embodiments of a system for gaming chip authentication as disclosed in the present invention do not rely on any specific or on any proprietary encryption algorithm to ensure that no security critical information contained within the chip memory has been modified by any entity external to the casino operating staff. This means that any standard asymmetric key encryption algorithm such as RSA or ECC or any standard symmetric key encryption such as DES or AES could be used interchangeably as long they offer the same level of bit security. However, a low footprint encryption algorithm will be preferably used since it will significantly alleviate the network traffic. The embodiments of a system for gaming chip authentication as disclosed in the present invention do not rely on any specific or on any proprietary RFID communication protocol or any RFID frequency. Hence any RFID integrated circuits such as those available off-the-shelves from integrated circuit suppliers such as EM-Microelectronic, Philips Semiconductors, Texas Instruments could be used interchangeably in these embodiments.

In one embodiment of the invention, a gaming table equipped with an RFID reader and interrogation zones communicates in a secure way with a security server in order to fetch gaming chip authenticating information. Such information is then

stored temporarily in the reader to speed up communication between the reader and the gaming chips. This temporarily stored information could possibly be used to successfully authenticate gaming chips even in the event of a complete network collapse. Authentication is done following a challenge response protocol whereby a digital signature is used to ensure the integrity of the messages sent by the parts intervening in the protocol

In another embodiment of the invention, the reader is allowed to process gaming chip-authenticating information but the reader is not allowed to store this information. This significantly reduces the amount of memory required at the reader side. But at the same time this requires careful network design since the traffic generated within the network could easily become overwhelming and could lead to a network collapse if no special care is taken.

In another embodiment of the invention, the gaming chip, in this document also subsequently called the "tag", is assumed to encompass a minimal cryptographic device beside a random number generator. The cryptographic device would preferably be of symmetric key type since these are easier to implement and require less area on the integrated circuit of the tag.

Referring to Figures 1 and 2, a security system for authenticating gaming chips 214 according to the present invention has a chip placement area 215 located within the casino preferably on gaming tables 209 (Black Jack table, Roulette table, etc.), a plurality of magnetic couplers 212 together with a plurality of readers 301 and a plurality of multiplexer for chip reading and writing, a secure network 101 together with a security server 102 and a casino management system 108.

Each gaming chip 302 has a memory 407 to store the information received from the security server via the reader 301. Upon arrival at the casino, or at any other time as the case may be, the gaming chips are commissioned. This means that

the gaming chips are registered in the casino database. The words gaming chip and tag will be used in the remaining part of this document interchangeably.

During the commissioning phase, all the parameters and all the necessary information needed for successful subsequent chip authentication is encoded into the chip memory 407. As illustrated in Figure 3 A, during this initialization phase, the tag generates a random number A that is concatenated to the tag's serial number 404 and sent 303a as a single chunk of information to the reader 301. The reader 301 uses its private key to build 307a a hash value H on the information. This hash value is transferred 303b to the security server 305. Again it is to be noted that the expressions "security server" and "host" will be used here interchangeably.

Upon receipt of the hash value H, the host 305 uses its private key to compute 306 a digital signature Z over the hash. This digital signature is then sent 303c to the reader which uses the security server's public key to verify 307b the signed message received 303c from the security server 305. Upon successful signature verification, the signed message is sent 303d to the tag 302, which then securely stores 304b the signed message into its memory 407.

Figure 3 B illustrates normal operation that follows the initialization phase. The transaction depicted on figure 3 B is a typical table game transaction. A reader (interrogator) 301 or a plurality thereof associated to a gaming table 107 or to a plurality thereof, initiates the transaction with a tag 302 by sending 303a an authentication request command to the tag. The tag generates 304c a random number B that is sent 303e back to the reader 305 together with the tag's serial number. Upon receipt of the random number B and the serial number 404, the reader sends 303b a retrieval command to the host 305 in order to retrieve the authentication information Z computed during the initialization phase and currently stored on the security server. Using the tag's serial number 404 the security server retrieves the digitally signed authentication information associated with the tag's

serial number and returns 303c it to the interrogator. Again, using the security server's public key, the interrogator verifies 307b the signature on the authentication information Z and subsequently computes 307c a cryptographic function F over the random number B, the tag's serial number and the authentication information Z. The reader then sends 303f the result of the computation to the tag. On his side, the tag computes 304e the same function F over the random number SN, the tag's serial number and the authentication information Z. Subsequently, the tag computes another cryptographic function G over the serial number, the authentication information Z and the serial number and sends 303g the result of this computation to the reader. Upon receipt of the result of the function G the reader computes the same function G over the random number B, the tag's serial number SN and the authentication information Z. When all the computations are done, the two parts compare the result of their proper computation with those received from the communication partner. If the calculated values are equal to those received, then the interrogator and the tag have mutually authenticated each other.

Figure 4 depicts a preferred embodiment of the present invention where the cryptographic engine 401 of the reader and the tag's memory 407 are displayed. The memory location pointer 409, which is used to record the most recently accessed valid memory location 410, is also displayed. The usefulness of the memory location pointer will be explicitly addressed during the description of the embodiment of the present invention depicted in Figure 5. Besides valid memory locations, the memory block 408 also displays memory locations 413 marked with an x in order to indicate that the content of these memory locations is not valid any more. The cryptographic functions F, G, H (414, 415, and 416) used throughout could be any cryptographic and persons skilled in the art will understand how to chose the best cryptographic function among those currently available or how to design other cryptographic functions that meet high security requirement. However, an embodiment of the present invention as depicted in Figure 4

encompasses feeding 4 independent values 403, 404, 405 and 406 as input to these cryptographic functions.

Figure 5 shows another preferred embodiment of the present invention. In this embodiment, the initialization parameter eventually defines how often the authentication process can be performed. Figure 5 A depicts the initialization process. In this process, the interrogator starts the initialization phase by sending 503a an initialization parameter to the tag. The tag responds with its serial number, which is subsequently forwarded 503c to the host by the reader along with a seed S generated by the reader. Upon receipt of the seed and the serial number, using its private key, the host generates 506b a signature Z over these two elements and subsequently sends the signature to the reader, which uses the host public key to verify 505a the signature generated by the host. Upon successful signature verification, the value Z is send 503e to the tag. The tag stores 504a the value Z. The tag then applies a cryptographic function F N times to the value Z and sends 503f P_0 the result of this operation to the reader. Without further processing, the reader forwards this value to the host, which then stores 506a P_0 in its database together with the tag's serial number SN. When a tag enters the field of the reader, the authentication sequence depicted in Figure 5 B requires that the reader first sends 503h the authentication request command along with a running index *i*. The tag responds to the request by applying 504 the cryptographic function F N-*I* times to the initial value Z. The value P_i calculated this way is then sent to the host through the reader. The host then applies 506c the same function F once to the previous response of the tag and compares 506d the obtained result with the value currently received from the tag. If these two values match then the current tag's response is stored 506e in the host's database along with the tag's serial number and access is granted. The host then sends back 503k the value *I* to the reader. Before the next authentication, the reader compares 505c the current value of I to zero. If *I* is greater than zero, then the tag is allowed to attempt a new authentication and the reader decreases the value of *I* before sending it to the tag for a new authentication. Otherwise, if I equals to zero

then the tag has reached its allowed authentication quota and must be re-commissioned.

Figure 6 depicts another embodiment of the current invention. Again, the initialization phase required for successful operation is illustrated in figure 6 A. The initialization phase starts with the reader sending 603a an initialization command to the tag. The tag answers 603b with its serial number, which is passed to the host without any further processing. The host then generates 605a and stores 605b an n-elements set of password strings ($S_1,\ldots,S_n$). These passwords are subsequently sent 603d 603e to the tag's secure memory through the reader without further processing. The host will then use the tag's serial as an index for its database.

When a tag enters the reader's field, the reader initiates an authentication process by sending 603f a random number *l* between 1 and n to the tag. The tag responds to this authentication request by retrieving the correct password using *i* as an access index 409 to valid locations 410 of one of its memory tables 408. The retrieved value is then sent 603g, 603h to the host trough the reader along with the tag's serial number. Using the tag's serial number, the host verifies that the password S_i received from the tag actually corresponds to the value stored in the database at position *i* for that given tag. If this is the case, access is granted and the host acknowledges 603i *l* to the reader. Upon receipt of the acknowledgment the reader marks the value of *i* as invalid and informs 603j the tag that it should invalidate the memory location 413 containing the value of *i*. Again as with the previously discussed embodiment, when the value of *i* reaches n, the tag has reached the predefined authentication quota and no other authentication is possible. Using this embodiment, several chips could be authenticated simultaneously since they could all share the same value of I while their respective serial number could be used to discriminate them on the host side.

The authentication process as described in this invention and in all the preferred embodiments described herein does not restrict communication between the security server and the chips only to communication through the gaming tables or cashier station. Indeed, chips may also be interrogated and requested to authenticate at other locations within the casino. For example, the casino could be equipped with readers and magnetic couplers coils located at employee portals 103 or at the casino exits 104 in order to prevent employee or player theft.

The embodiment of the present invention are not limited to passive RIFD chip as they will work equally with battery assisted RFID devices both active and semi-passive devices comprised.

CLAIMS

1. A system for authenticating RFID-capable gaming chips in a casino, said system comprising at least one security server, at least one secure network, a casino management system and a plurality of magnetic couplers distributed within the casino, wherein said gaming chips are adapted to provide a response to a challenge issued by said magnetic couplers when said chips are located in the vicinity of said magnetic couplers, whereby said chip is authenticated when said response matches a computed response by said server.

2. A system according to claim 1, wherein each of said gaming chips include a memory and pseudo-random number generator, and wherein each of said gaming chips has a unique serial number.

3. A system according to claim 1, wherein said challenge and said response are encrypted using symmetric cryptographic primitives.

4. A system according to claim 1, wherein said challenge and said response are encrypted using asymmetric cryptographic primitives.

5. A system according to claim 1, wherein said chips are provided with authentication information at a commissioning phase, said authentication information including a plurality of words, each word being used only once during authentication.

6. A system according to claim 1, wherein at least some of said magnetic couplers are located on or embedded in gaming tables.

7. A system according to claim 1, wherein said system further includes a commissioning station for commissioning said gaming chips when said chips first arrive at said casino, and at other predetermined times.

8. A method for authenticating RFID-capable gaming chips within a casino, comprising the steps of:

(a) commissioning said chips at a commissioning station, including loading into said chip authentication information;

(b) providing a plurality of magnetic couplers distributed in said casino;

(c) issuing a challenge from said magnetic couplers to said chips when said chips are located in the vicinity of said magnetic couplers;

(d) receiving a response from said chip;

(e) comparing said response to a computed response; and

(f) authenticating said chip when said response matches said computed response.

9. A method according to claim 8, wherein said step of providing a plurality of magnetic couplers includes the step of providing embedded active integrated circuits within the casino at gaming tables or embedded semi-passive integrated circuits or a combination thereof.

10. A method according to claim 8, wherein said response is encrypted using symmetric cryptographic primitives or asymmetric cryptographic primitives, or a combination thereof.

11. A method according to claim 8, wherein said computed response is computed in real-time.

12. A method according to claim 8, wherein said step (a) of commissioning is repeated at predetermined time intervals.

13. A method according to claim 8, wherein said authentication information is used a predefined number of time.

14. A method according to claim 8, wherein said method comprises computing and storing the authentication information in the gaming chip before the first authentication.

15. A method according to claim 8, wherein said method comprises computing the authentication on the fly during the authentication process.

16. A method for authenticating an RFID reader to a gaming chip within the casino comprising:
the gaming chip issuing a challenge to the RFID reader;
the gaming chip receiving a response from the RFID reader;
comparing said response to a computed response; and
authenticating the reader when said response matches said computed response.

17. A method of gaming chip authentication in accordance with claim 8 wherein the challenge value is pseudo-random value.

18. A method of gaming chip authentication in accordance with claim 8 wherein the challenge value is a binary string.

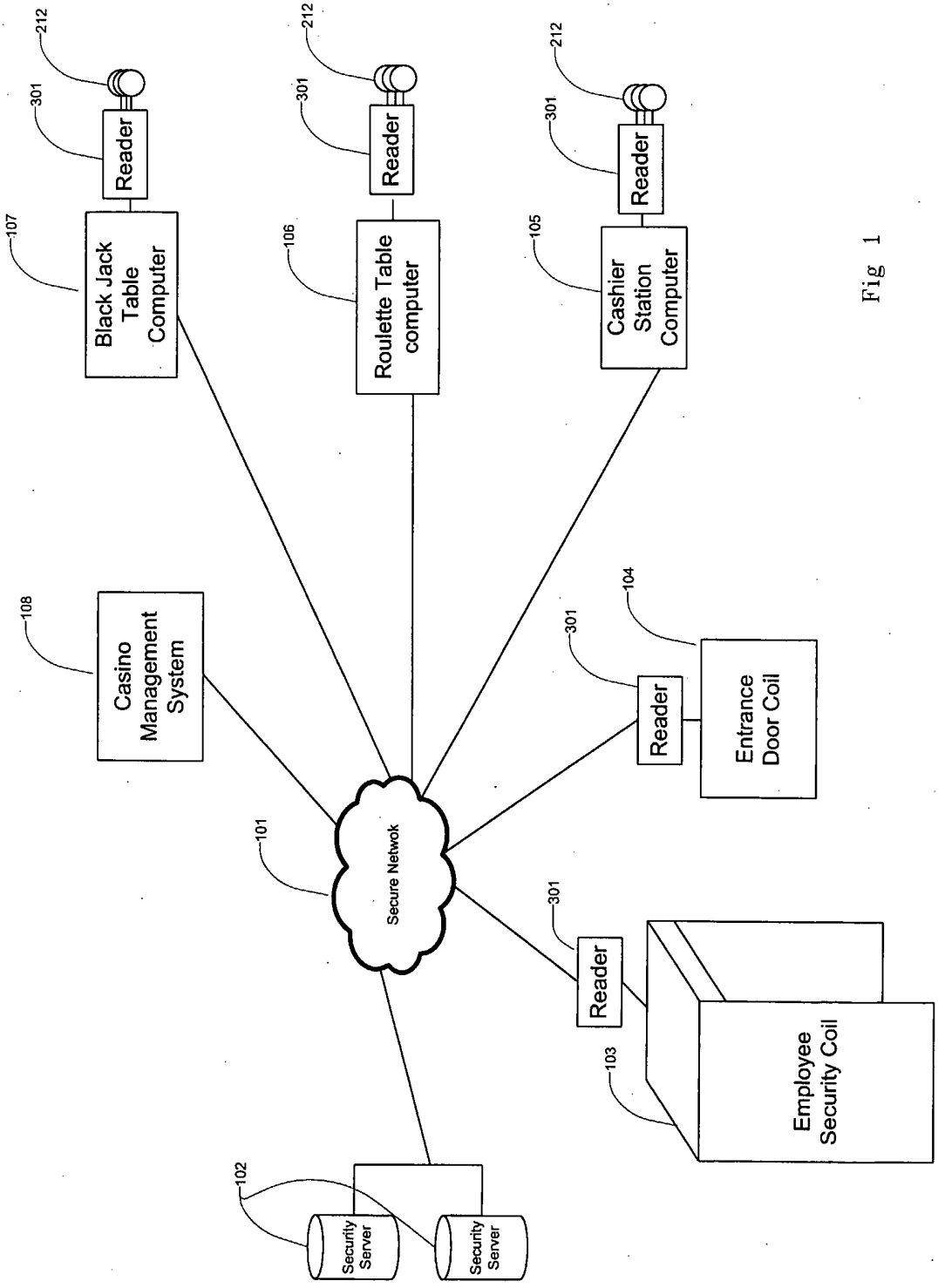

212
301
Reader
107
Black Jack Table Computer
212
301
Reader
106
Roulette Table computer
212
301
Reader
105
Cashier Station Computer
108
Casino Management System
104
301
Reader
Entrance Door Coil
101
Secure Netwok
301
Reader
103
Employee Security Coil
102
Security Server
Security Server

Fig 1

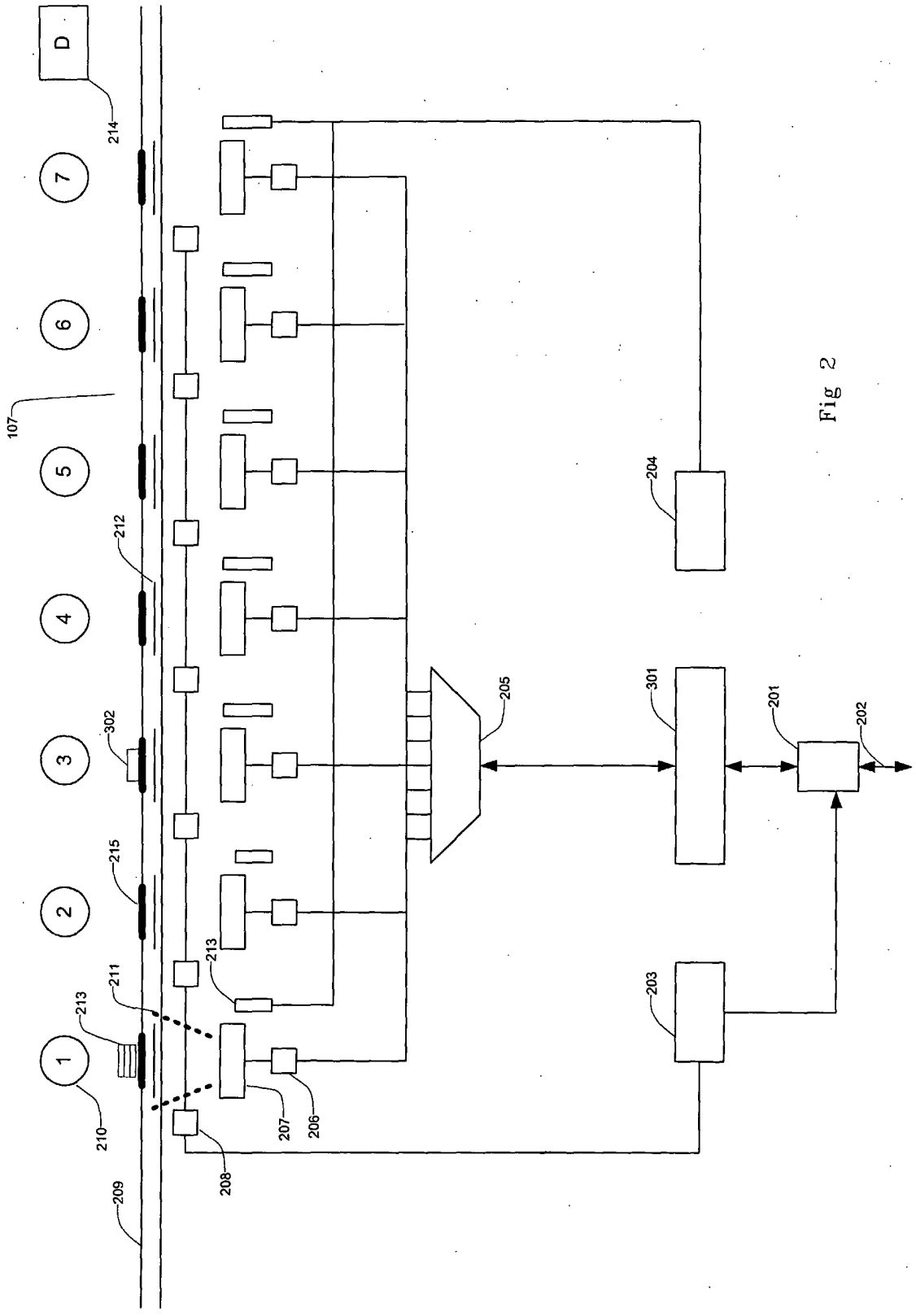

D
214
7
6
107
5
212
4
302
3
215
2
213
211
213
1
210
209
208
207
206
205
204
301
201
202
203

Fig 2

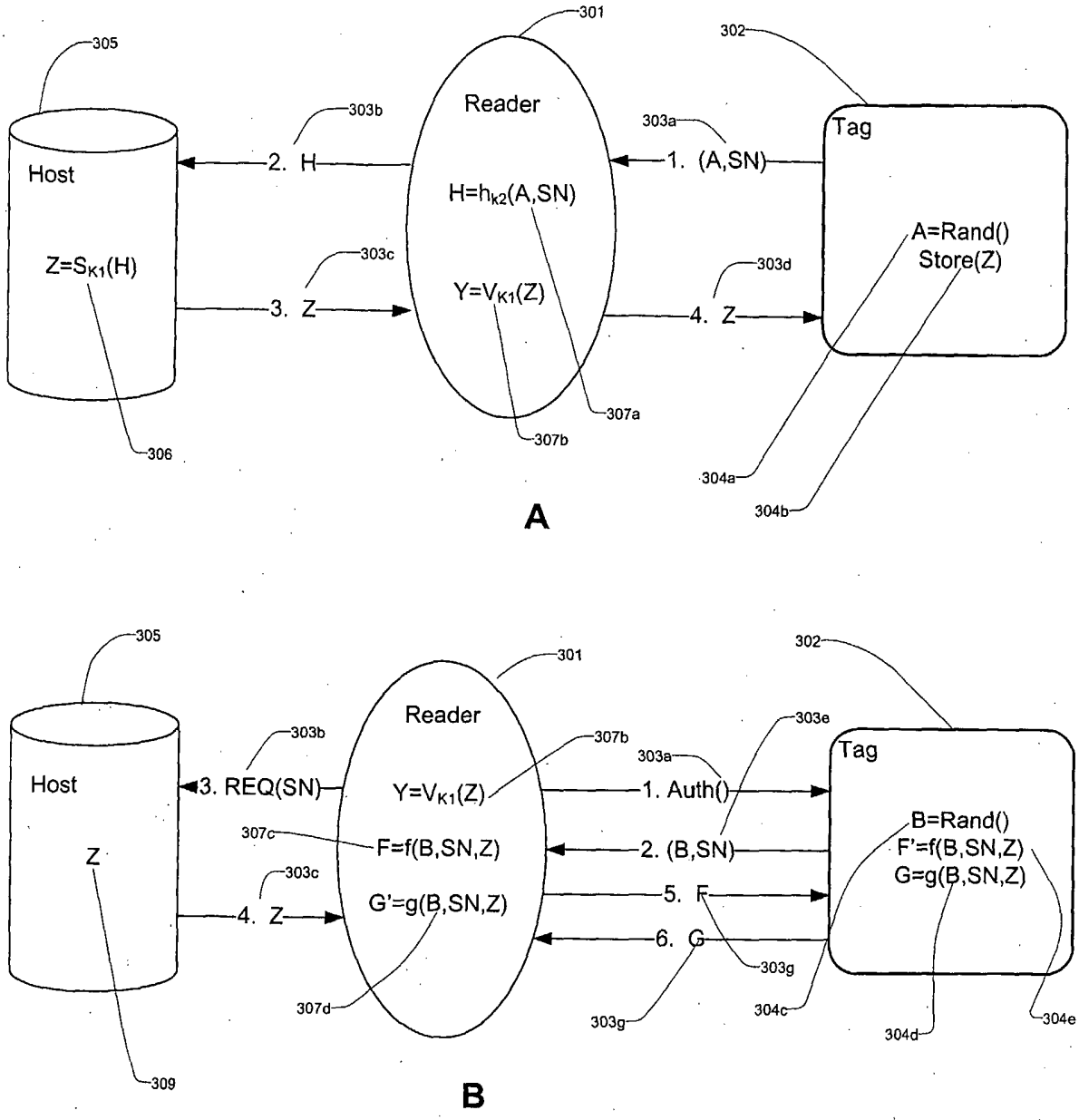

301
302
305
Reader
Tag
Host
303b
303a
2. H
1. (A,SN)
H=h_k2(A,SN)
A=Rand()
Store(Z)
Z=S_K1(H)
303c
303d
Y=V_K1(Z)
3. Z
4. Z
307a
307b
306
304a
304b
A
305
301
302
Reader
Tag
Host
303b
303e
307b
303a
3. REQ(SN)
Y=V_K1(Z)
1. Auth()
B=Rand()
F'=f(B,SN,Z)
G=g(B,SN,Z)
307c
F=f(B,SN,Z)
2. (B,SN)
Z
303c
5. F
4. Z
G'=g(B,SN,Z)
6. G
303g
307d
303g
304c
304d
304e
309
B

Fig 3

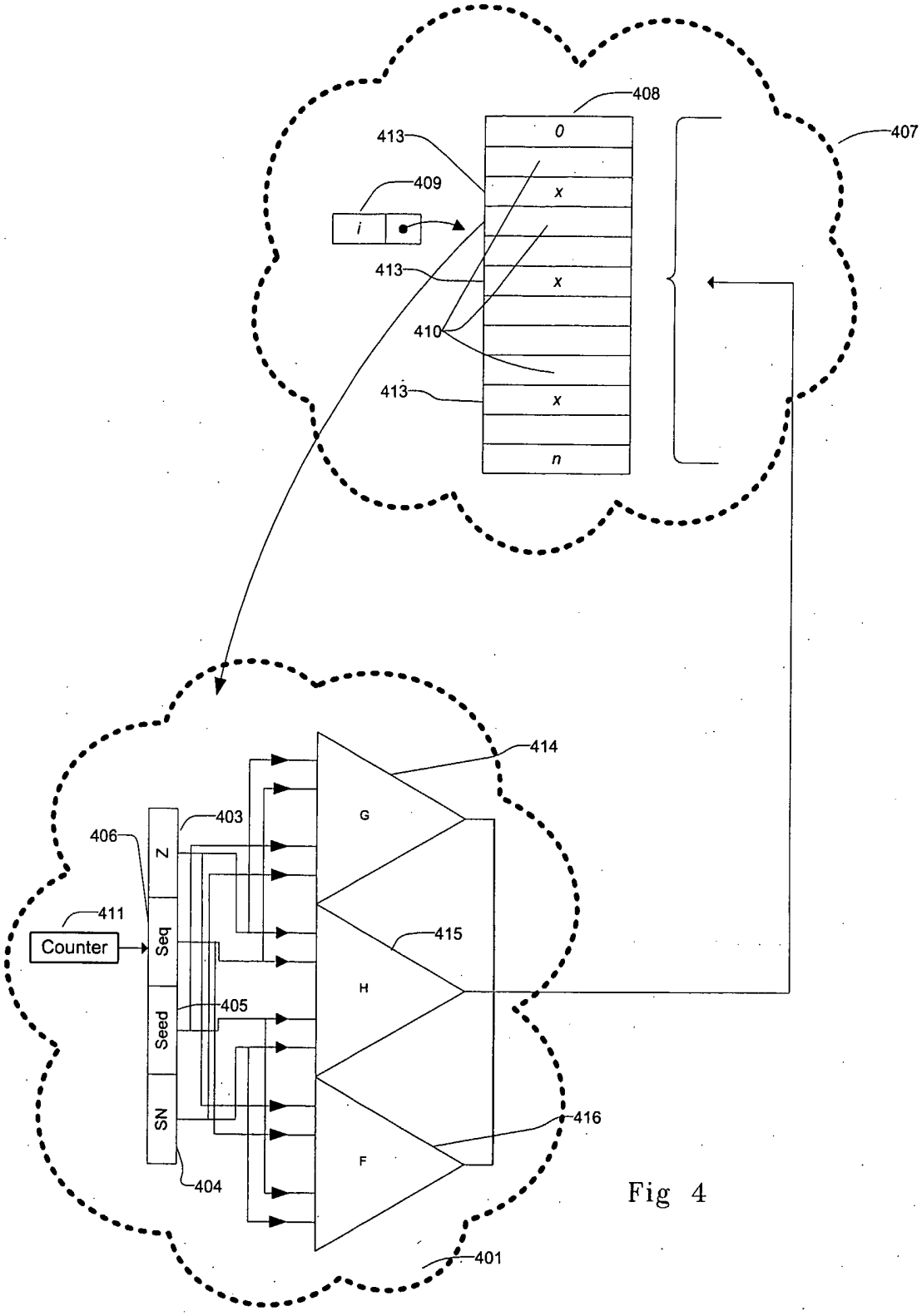
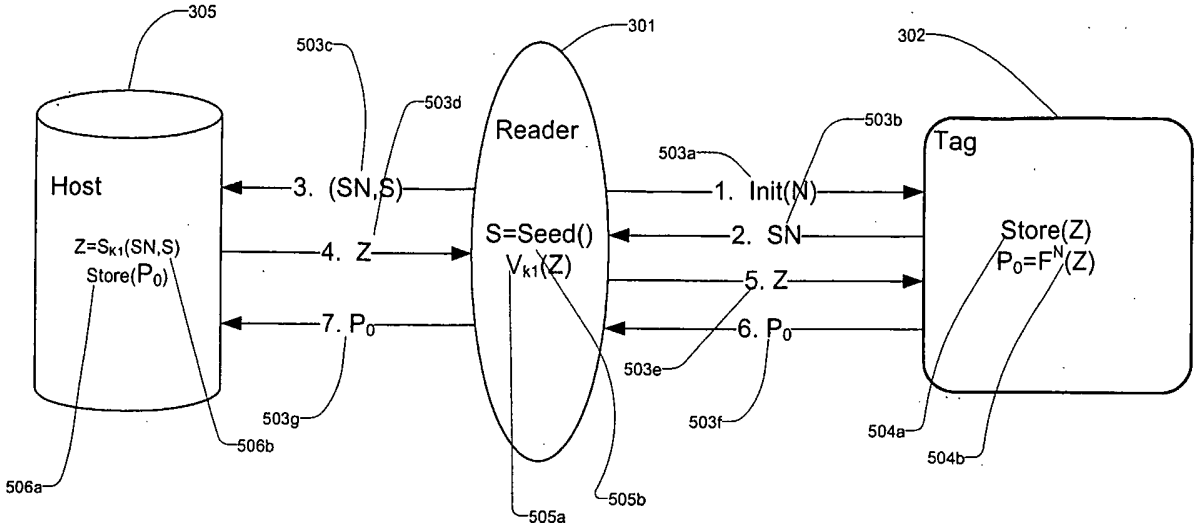
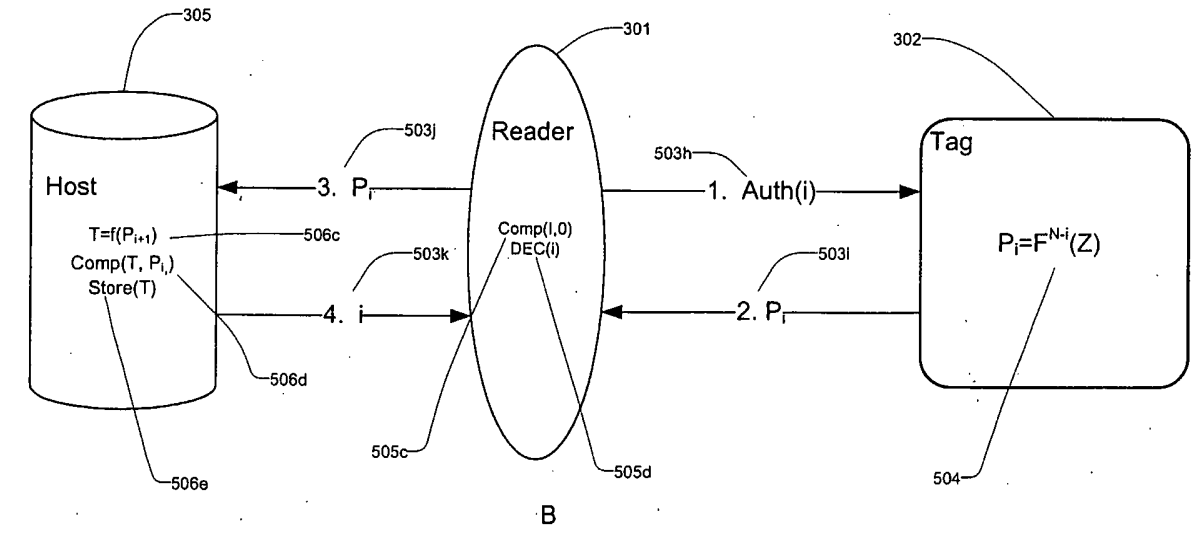

408
407
413
409
0
x
i
413
x
410
413
x
n
414
403
406
G
Z
411
Counter
Seq
415
H
405
Seed
SN
416
F
404
401

Fig 4

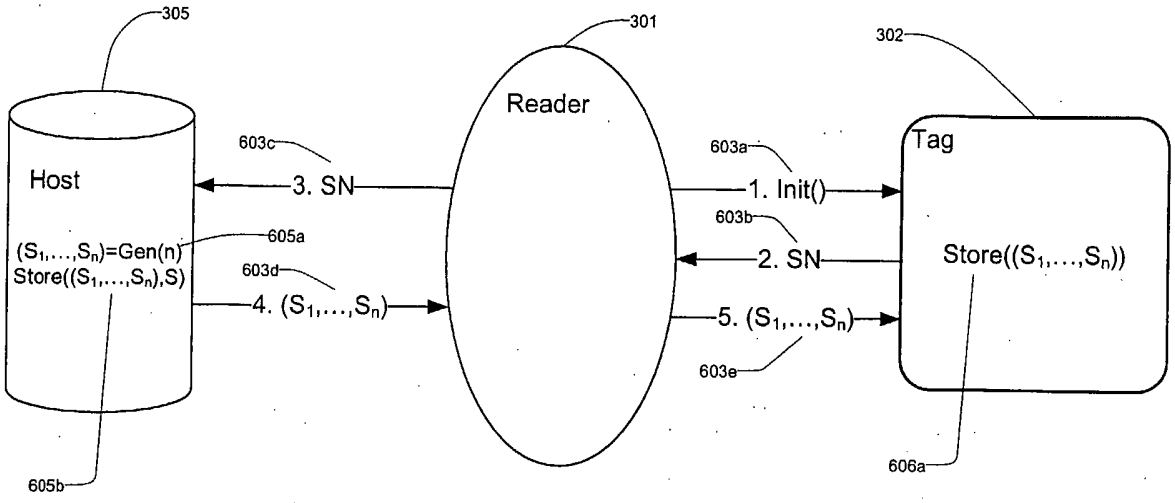

305
503c
503d
301
302
Reader
503b
503a
Tag
Host
3. (SN,S)
1. Init(N)
S=Seed()
$V_{k1}(Z)$
2. SN
Store(Z)
$P_0=F^N(Z)$
$Z=S_{k1}(SN,S)$
Store(P_0)
4. Z
5. Z
7. P_0
6. P_0
503e
503g
503f
504a
504b
506a
506b
505a
505b

A

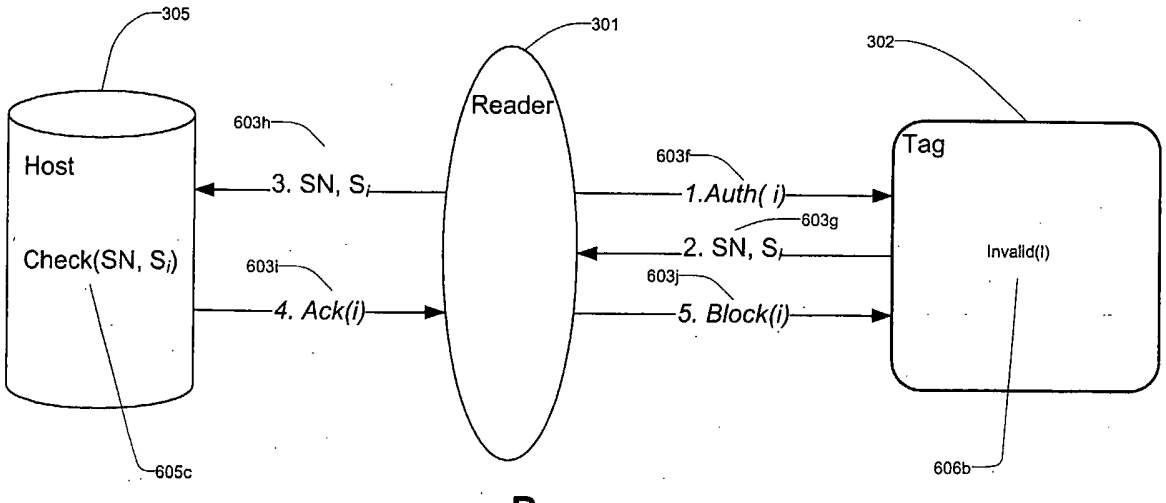

305
301
302
503j
Reader
503h
Tag
Host
3. P_i
1. Auth(i)
T=f(P_{i+1})
506c
Comp(I,0)
DEC(i)
$P_i=F^{N-i}(Z)$
503k
503l
Comp(T, P_i)
Store(T)
4. i
2. P_i
506d
505c
505d
506e
504

B

Fig 5


305
301
302
Reader
Host
Tag
603c
3. SN
603a
1. Init()
603b
2. SN
(S1,...,Sn)=Gen(n)
Store((S1,...,Sn),S)
605a
603d
4. (S1,...,Sn)
5. (S1,...,Sn)
603e
Store((S1,...,Sn))
605b
606a

A


305
301
302
Reader
Host
Tag
603h
3. SN, Si
603f
1.Auth(i)
603g
2. SN, Si
Check(SN, Si)
Invalid(I)
603i
4. Ack(i)
603j
5. Block(i)
605c
606b

B

Fig 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2005/001519

A. CLASSIFICATION OF SUBJECT MATTER
IPC[7]: G07F 17/32, G07F 1/06, G06K 19/07

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]: G07F, G06K

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

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Internet, Delphion, USPTO WEST, Canadian Patent Database: game/gaming, chip(s), RFID, radio frequency identification, authentication/authenticate, challenge, response, query.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 735 742 (FRENCH) 7 April 1998 (07-04-1998) entire document	1 to 18
Y	US 6 685 564 (OLIVER) 3 February 2004 (03-02-2004) entire document	1 to 18
Y	CA 2 500 779 (HUGHES ET AL) 22 April 2004 (22-04-2004) entire document	1 to 18

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent 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
18 November 2005 (18-11-2005)	25 November 2005 (25-11-2005)

Name and mailing address of the ISA/CA	Authorized officer
Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001(819)953-2476	Tara Derickx (819) 997-4502

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2005/001519

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	www.howstuffworks.com, *How RFIDs Work* 23 July 2004 (23-07-2004) located at the web archive location of: http://web.archive.org/web/20051116094736/http://electronics.howstuffworks.com/smart-label.htm/printable	1 to 18

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/CA2005/001519

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US5735742	07-04-1998	none	
US6685564	03-02-2004	US6186895 B1	13-02-2001
		US6464584 B2	15-10-2002
		US2004142743 A1	22-07-2004
CA2500779	22-04-2004	AU2003270786 A1	04-05-2004
		EP1547008 A1	29-06-2005
		US6842106 B2	11-01-2005
		WO2004034321 A1	22-04-2004

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2005/001519

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of the first sheet)

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

1. [ ] Claim Nos. :
because they relate to subject matter not required to be searched by this Authority, namely :

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

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

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows :

GROUP 1: *Claims 1 to 15* describe a system and method for authenticating RFID gaming chips in a casino.

GROUP 2: *Claims 16 to 18* describe a method for authenticating an RFID reader to a gaming chip within the casino.

1. [ ] As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. [X] As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. [ ] As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claim Nos. :

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

Remark on Protest
[ ] The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
[ ] The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
[ ] No protest accompanied the payment of additional search fees.