

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
4 March 2004 (04.03.2004)

PCT

(10) International Publication Number
WO 2004/019547 A1

(51) International Patent Classification⁷: **H04L 7/04**, 7/10

(21) International Application Number:
PCT/US2003/025905

(22) International Filing Date: 19 August 2003 (19.08.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/405,203 22 August 2002 (22.08.2002) US

(71) Applicant (for all designated States except US): **THOMSON LICENSING S.A.** [FR/FR]; 46, Quai A. Le Gallo, F-92648 Boulogne (FR).

(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, 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), 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).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **SCHULTZ, Mark, Alan** [US/US]; 4437 Somerset Way S., Carmel, IN 46033 (US). **CHIDAMBARAM, Dinakaran** [IN/US]; 9252 Yale Drive #C, Indianapolis, IN 46240 (US).

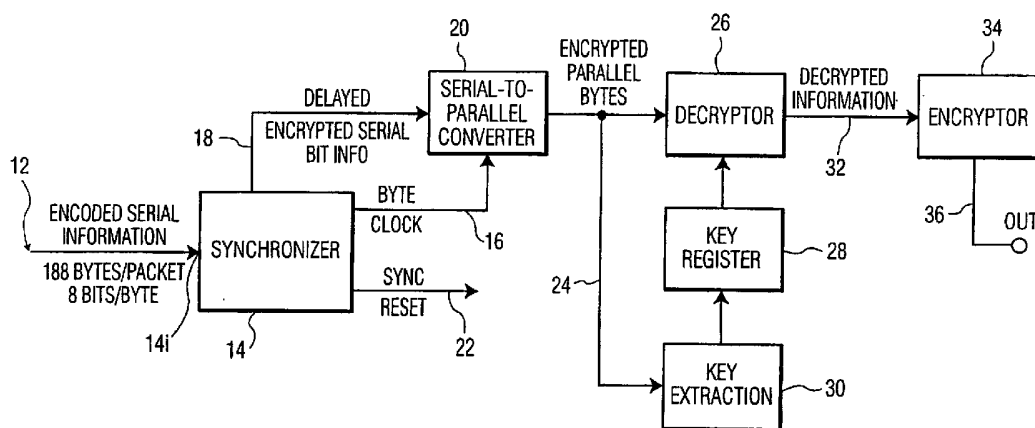
(74) Agents: **TRIPOLI, Joseph, S.** et al.; c/o Thomson Licensing Inc., Two Independence Way, Suite #200, Princeton, NJ 08540 (US).

Published:

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

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: FAST SYNCHRONIZATION IN SMART CARDS



10

(57) Abstract: A method of processing a digital data stream containing packets of information, where each packet includes a synchronization portion defining a value, and a packet identification portion. The method comprises receiving packets of the data stream containing the synchronization portion and the packet identification portion and periodically enabling a detector for detecting the value in a portion of a packet of the data stream. A synchronization signal is generated in response to the detection for synchronizing processing of the packets. In response to the synchronization signal, a subsequent portion of the packet is compared with stored information intended to correspond to the packet identification portion, to determine whether the synchronization signal resulted from detection of the synchronization portion associated with the packet. If the comparison fails to reveal a match, the detector is re-enabled for further detection of the value.

FAST SYNCHRONIZATION IN SMART CARDSCross-Reference to Related Applications

5 [0001] This application claims the benefit of the priority of U.S. Provisional Application 60/405,203 filed August 22, 2002 in the name of Schultz et al.

[0002] This application is related to commonly assigned patent application entitled "Smart Card With NRSS Delay Line For Data Alignment" filed on August 15, 2003 in the name of Schultz et al. (Docket Number PU020388).

10

Field of the Invention

[0003] This invention relates to smart cards, and more particularly to rapid synchronization to synchronization bytes of multi-byte information packets.

Background of the Invention

15

[0004] Delivery of various forms of information and entertainment is often conditional, in that the information or entertainment is available only if the recipient pays the owner of the information, or is otherwise an authorized recipient. Smart cards can be used to provide the authorization necessary for such conditional delivery. In general, custody of the smart card represents the authorization required to interface with a delivery system.

20

[0005] In the context of delivery of serial video using an MPEG standard transport stream, the video as delivered from a source may be encrypted, and the smart card performs the decryption needed to convert the video to usable form. The decryption is performed by a decryption device or circuit located on the smart card. In order for decryption to take place, the decryptor on the smart card requires a proper key. The necessary decryption keys accompany the video stream, and can be extracted therefrom. These decryption keys are transmitted relatively infrequently, say every half-second or so. Thus, under least-optimum timing conditions, decryption might not start for one-half

25

second after the key became available to the smart card. The key may be changed at the source every few seconds for improved security. There may be different keys for various different ones of the available video streams, and/or for different ones of the smart-card/delivery-device pairs.

- 5 [0006] In order to obtain the decryption key from the delivered encrypted information stream, the smart card must correctly decode the set of bytes containing the key information from among the bytes of each packet of information. As an example, a serial bit stream of MPEG transport stream video might be made up of successive packets of information, where each packet of information consists of 188 bytes, each of 8 bits.
- 10 Within each 188-byte packet, the first 8-bit byte is a synchronization byte having a value of forty-seven (47). Four packet identification (PID) bytes immediately follow the packet synchronization byte. These packet identification bytes carry information relating to the type of information in the packet, the type of coding, error detection and correction (EDAC) and the like. Since each packet contains 188 bytes, there are 187 bytes between
- 15 successive synchronization bytes, and 183 bytes between the end of the packet identification bytes and the next following synchronization byte. These 183 bytes are used for transport of the information, which in the example is video information.
- [0007] FIGURE 1 is a simplified block diagram of a portion of a smart card 10 including a decryption block, a key extraction block, and a prior art synchronizing arrangement. In
- 20 FIGURE 1, encrypted serial information is applied by way of an input port 12 to a port 14i of a prior-art synchronizer 14. The encrypted serial information is in the form of packets of 188 bytes, where each byte is of eight bits. Within each packet, the first byte is a synchronization byte, which has a particular value. In the case of a MPEG transport stream, the particular value of the synchronization byte is forty-seven (47). In this
- 25 transport stream, four packet identification (PID) bytes immediately follow the synchronization byte.

[0008] Synchronizer 14 of FIGURE 1 generates a byte clock on an output signal path 16,

which is used to clock a serial-to-parallel converter illustrated as a block 20. Encrypted serial information, delayed relative to the encrypted serial information applied to input port 12, is produced on an output signal path 18 of synchronizer 14, and is applied to serial-to-parallel converter 20. Serial-to-parallel converter 20 produces on a signal path
5 24 a stream of eight-parallel-bit bytes in response to the byte clock. A packet synchronization or reset signal generated on an output path 22 of synchronizer 14 is used for a timing reference in a triple DES decryption engine. The NRSS system delay through the smart card is a constant clock delay even though there may be gaps between the 188-byte packets. When decryption is active, the reset or sync signal of the next
10 packet helps to establish if a gap exists or no gap is found between packets, which adjusts the processing for terminating the present or current packet and the beginning of processing of the incoming packet.

[0009] The encrypted stream of parallel-bit bytes produced by serial-to-parallel converter 20 of FIGURE 1 is applied to a key extraction arrangement illustrated as a
15 block 30. The key information is transmitted in a number of bytes found in the serial bit stream entering port 12 of smart card 10, on an infrequent basis, such as every half-second. Block 30 monitors the parallel-bit byte stream and, when key information is available, extracts the key, and processes it, if necessary, as by decrypting, and applies the resulting decrypted key to a memory or register illustrated as a block 28. In
20 operation, a decryptor, illustrated as a block 26, receives the encrypted parallel-bit bytes from converter 20, and decrypts the information using the key which is available in register 28. Decryptor block 26 produces decrypted video information on a signal path 32. In order to maintain security of the decrypted video, the video may again be encrypted in a block illustrated as 34 with an encryption code which a utilization or
25 display apparatus can decode. The re-encrypted video is produced at a smart card output port or path 36.

[0010] FIGURE 2 is a simplified block diagram of a prior-art synchronizer which may be

used in block 14 of FIGURE 1. In FIGURE 2, the encrypted serial information is applied by way of input port 14i of synchronizer 14 to the input port 210i of an eight-bit delay line or register 210. Delay line 210 makes each of the stored eight bits available on a set 212 of output lines 212a, 212b, . . . 212g, 212h. The eight-bit-period delayed encrypted serial information is output from block 210 at an output port 210o, and is applied by way of signal path 18 to serial-to-parallel converter 20.

[0011] Also in FIGURE 2, an AND gate 214 includes eight input ports 1, 2, . . . , 7, 8, each of which is connected to one of the eight bit lines of set 212. More particularly, input ports 1 and 2 of AND gate 214 are connected to bit lines 212g and 212h, respectively, and input ports 7 and 8 of AND gate 214 are connected to bit lines 212a and 212b, respectively. AND gate 214 includes a further input port designated EN9. This further input port is used as an enable (EN) input port, enabling the remaining input ports in response to a selected logic level applied over a bit line 216, and disabling the gate in response to the other logic level. In one version, positive logic is used, and the enabling logic level is logic high.

[0012] During operation, AND gate 214 of FIGURE 2 monitors/detects the value of the bits traversing 8-bit delay line 210. AND gate 214 is configured to, when enabled, respond to the value of a synchronizing byte, which in one version has a bit value of forty-seven (47). Thus, when the total value of the bits traversing delay line 210 equals 47 and AND gate 214 is enabled, AND gate 214 responds by producing a packet synchronizing (sync) or reset signal on signal path 22. The sync signal on signal path 22 is applied to a three (3)-bit counter illustrated as a block 218, which resets to zero (or to full count, as desired) and then counts eight clock cycles. Since a byte corresponds to eight bits or clock cycles, the full count of counter 218 occurs once per byte, and may be considered to be a byte clock. The byte clock signal produced by counter 218 is applied by way of path 16 to serial-to-parallel converter 20, to aid in producing the parallel-bit bytes. Thus, converter 20 accepts eight bits, and produces one byte every eight bit clock

cycles.

[0013] The sync signal or reset pulse produced on path 22 by AND gate 214 of FIGURE 2 is also applied to a reset input port 228r of a counter 228, together with the byte clock from counter 218. Counter 228 counts a number of bytes corresponding to the number of bytes between successive packet synchronizing pulses. More particularly, in an exemplary arrangement in which there are 188 bytes in each packet, one of which is the synchronization byte, there are 187 byte intervals between two successive synchronization bytes. At full count, counter 228 generates a logic high or logic 1 at its output port 228o, which is applied to the enable input port EN9 of AND gate 214, to thereby enable AND gate 214 to detect the next synchronization byte. In the same manner, during counts other than a full count, output port 228o of counter 228 produces a logic low or 0 signal, which disables AND gate 214. Disabling the AND gate for all periods other than the expected arrival time of the synchronization byte tends to reduce the incidence of response of AND gate 214 to occasional byte values of 47, which may occur during operation.

[0014] The operation of the arrangement of FIGURE 2 makes it clear that, so long as the initial response of AND gate 214 is to a true synchronization byte, the synchronization system 14 is unlikely to respond to synchronization-level bytes which occur during the video portions of the signal, since the AND gate is disabled during the video portions of the signal. However, the first detection of a synchronization-value byte may occur in response to a video-content portion of the signal, rather than in response to a synchronization byte. In this event, the reset pulse will occur during the video interval, and the synchronization block 14 will not become aware of this error until the 187-byte-interval counter 228 reaches its full count. In such a situation, the reaching of a full count of counter 228 enables AND gate 214 during the video-content portion of the signal. In general, the video content at that location will no longer have the synchronization byte value, which is 47 in the example. In this event, synchronization has not been achieved,

and a period of about one packet duration has already expired.

[0015] Considering that the decrypting key must be obtained and processed before decryption of the video content can be started, and packet synchronization must be achieved before that or those of the bytes containing the decrypting key can be identified, and further considering that the encrypting key byte is available only intermittently, rapid synchronization is desirable to provide timely response of the smart card to a user's request.

Summary of the Invention

[0016] According to an aspect of the invention, a method of processing a digital data stream containing packets of information, where each packet includes a synchronization portion defining a value, and a packet identification portion. The method comprises receiving packets of the data stream containing the synchronization portion and the packet identification portion and periodically enabling a detector for detecting the value in a portion of a packet of the data stream. A synchronization signal is generated in response to the detection for synchronizing processing of the packets. In response to the synchronization signal, a subsequent portion of the packet is compared with stored information intended to correspond to the packet identification portion, to determine whether the synchronization signal resulted from detection of the synchronization portion associated with the packet. If the comparison fails to reveal a match, the detector is re-enabled for further detection of the value.

[0017] According to another aspect of the invention, an apparatus for processing a digital data stream containing packets of information, where each packet includes a synchronization portion defining a value, and a packet identification portion. The apparatus is operable for receiving packets of the data stream containing the synchronization portion and the packet identification portion. A detector having a controllable input is responsive to the value in the data stream for producing a synchronization signal, whereby the detector produces a synchronization signal in

response to the synchronization portion of a packet in the data stream and also in response to an information item having the value. A counter responsive to the synchronization signal, counts a predetermined number of bytes associated with the received packets of the data stream, and produces an enable signal for controlling the controllable input of the detector for enabling detection at a time corresponding to the predetermined number of bytes after the synchronization signal, thereby enabling the detector to respond to a further synchronization portion associated with a packet in the data stream, and whereby, if the detector responds to an information item rather than to a synchronization portion, at least the predetermined number of byte periods must pass before resynchronization can begin. A comparator responsive to the synchronization signal is operable for matching a subsequent portion of the packet data stream following the detected value, with stored information intended to correspond to the packet identification portion, and, in the absence of a match, generating and applying an input enable signal to the controllable input, thereby enabling the detector to further search for and detect a received the value prior to the expiry of a period of the predetermined number of bytes.

[0018] A smart card according to an aspect of the invention is for decrypting encrypted N-byte information packets, where the information packets include a synchronization byte defining a value, a first plurality of packet identification bytes following the synchronization byte, and, from time to time, a decryption key. The card comprises a key-controlled decryption arrangement coupled to receive the encrypted N-byte information packets, for decrypting the information to produce decrypted information, and a delay device for delaying the information for the number of bits in a byte of the information, and for providing simultaneous access to each of the bits in the information so delayed. A controllable gate is coupled to the delay device, for responding to the value with (or by generating) a synchronization signal or reset pulse, whereby the gate produces a synchronization signal in response to the synchronization byte and also in

response to an information byte having the value. A key extraction arrangement is coupled to receive the information, for, when synchronized to the packets by the synchronization signal, extracting the key, thereby allowing the decryption arrangement to decrypt the information. The smart card also includes a byte clock generator; and a
5 serial-to-parallel converter coupled to an output port of the delay device and to the byte clock generator, for converting the information output from the delay device from serial-bit to byte form at the rate of the byte clock. A byte counter is coupled to receive the synchronization signal, for counting N-1 bytes, and for producing an enable signal for controlling the controllable gate at a time N-1 bytes after the synchronization signal,
10 thereby enabling the controllable gate to respond to a further synchronization byte, whereby, if the controllable gate responds to an information byte rather than to a synchronization byte, at least N-1 byte periods must pass before resynchronization can begin. An identification packet comparator is coupled to the serial-to-parallel converter, for matching with stored information at least one of the first plurality of packet
15 identification bytes following the synchronization signal generated by the controllable gate, and, in the absence of a match, for generating and applying a gate enable signal to the controllable gate, thereby enabling the controllable gate to search for the value prior to the expiry of a period of N-1 bytes.

[0019] In one embodiment of the invention, the encrypted serial information comprises
20 MPEG serial transfer format video with 188-byte packets, 8 bits per byte, and starting with a synchronization byte having a value of 47. In this embodiment, there are four packet identification bytes which immediately follow the synchronization byte.

Brief Description of the Drawing

25 [0020] FIGURE 1 is a simplified diagram of a decryptor for encrypted serial information in the form of successive packets;

[0021] FIGURE 2 is a simplified block diagram of a prior art synchronizing portion of

the arrangement of FIGURE 1; and

[0022] FIGURE 3 is a simplified block diagram of a synchronizing portion of the arrangement of FIGURE 1 according to an aspect of the invention.

5

Description of the Invention

[0023] In FIGURE 3, elements corresponding to those of FIGURE 2 are designated by like reference alphanumerics. FIGURE 3 differs from FIGURE 2 in having an OR gate 310 connected in signal path 216 between output port 228o of counter 228 and the enable input port EN9 of AND gate 214. More particularly, port 228o of counter 228 is
10 connected to an input port 310₁ of OR gate 310, and the output port 310o of OR gate 310 is connected to port EN9 of AND gate 214. OR gate 310 has no effect on the enabling and disabling of AND gate 214 by counter 228, so that when counter 228 reaches a full count of 187 byte intervals, it produces an enable signal which enables AND gate 214 for the next following byte, and maintains AND gate 214 disabled otherwise.

15 [0024] OR gate 310 of FIGURE 3 has its second input port 310₂ connected to the output port 312o of an AND gate 312. AND gate 312 effectively provides a second input port, designated 312i₁ by which AND gate 214 can be enabled. More particularly, if the output port 312o of AND gate 312 is logic high, that logic high level will be coupled through OR gate 310 to the enable input port EN9 of AND gate 214 regardless of the
20 state of output port 228o of counter 228. A block illustrated as 314 in FIGURE 3 stores the bit patterns of the packet identification (PID) bytes which are of interest to the smart card 10 of FIGURE 1, and makes the patterns available to a comparator arrangement illustrated as a block 316. As mentioned, in an embodiment of the invention involving MPEG video, the PID bytes immediately follow the sync byte. Comparator 316 is
25 enabled for comparison of the stream of data bytes arriving by way of path 24 with at least one, and preferably a set of two or more, of the PID bytes within the data stream. Comparator 316 is enabled by a enable (EN) signal applied from the output port 320o of

a window generator 320. Window generator 320 responds to at least the second count of the counter 228 following the sync or reset signal, and preferably to the second, third, fourth, and fifth counts, to enable comparison block 316 during the first, or preferably the first through fourth counter-228 counts following the sync bit which resets counter 228.

5 During the window interval, comparison block 316 compares the stream of parallel-bit bytes applied from path 24 with the PID byte(s). If a match is found, the output port 316o of comparator 316 remains at an inactive (logic low) level. With port 316o at an inactive level, AND gate 312 is disabled, and the logic level at its output port remains at an inactive logic level. Thus, in the presence of a match between the stored PID bytes

10 and the current data bytes, the PID comparison arrangement including memory 314, comparator 316, and gates 310 and 312 has no effect on the prior-art portion of the synchronizer, namely the FIGURE 2 synchronizer. In the event of a lack of a match between the stored PID bytes and the current data bytes, output port 316o of comparator 316 produces an active logic state, such as a logic high level. The active logic state

15 propagates through AND gate 312 if the gate is enabled by having its ON/OFF input port (and therefore its input port 312i₂) at an active logic state. The active logic level produced by comparison block 316 in the absence of a match between the stored PID bytes and the current data bytes propagates through AND gate 312 if enabled, and also propagates through OR gate 310 to the enable input port EN9 of AND gate 214, thereby

20 enabling AND gate 214 to continue searching for/detecting a synchronization byte. Thus, if comparison block 316 fails to match any one of the PID bytes, synchronization is deemed to not be achieved, and gate 214 is re-enabled to search for another sync byte.

[0025] Other embodiments of the invention will be apparent to those skilled in the art. For example, the window generator 320 may enable comparison block 316 during a

25 single byte interval or plural byte intervals, and the enabled intervals may immediately follow the sync byte(s) or be separated therefrom, and may even enable the comparison block during plural subintervals in each packet interval, as desired. The synchronization

signal within the information stream may be a single byte having a value or may include further bytes. The number of PID bytes may be of any desired value, as can the number of bytes in a packet. Accordingly, various modifications and changes can be made without departing from the spirit of the invention. All such modifications and changes
5 are considered to be within the scope of the appended claims

CLAIMS

1. A method of processing a digital data stream containing packets of information, each packet including a synchronization portion defining a value, and a packet identification portion, said method comprising:

5 receiving packets of said data stream containing said synchronization portion and said packet identification portion;

periodically enabling a detector for detecting said value in a portion of a packet of said data stream, and generating a synchronization signal in response to said detection for synchronizing processing of said packets; and

10 in response to said synchronization signal, comparing a subsequent portion of said packet with stored information intended to correspond to said packet identification portion, to determine whether said synchronization signal resulted from detection of said synchronization portion associated with said packet; and, if not, enabling said detector for further detection of said value.

15

2. The method of claim 1, wherein the step of periodically enabling said detector comprises enabling said detector according to a given bit count associated with said packet.

20

3. The method of claim 1, wherein the step of comparing a subsequent portion of said packet with stored information comprises: comparing a predetermined number of bits in said packet immediately following said detected portion of said packet having said value, with said stored information.

25

4. The method of claim 3, wherein the comparing a predetermined number of bits in said packet immediately following said detected portion of said packet further comprises: determining if there is a match between at least one of the next four bytes in

said packet following said detected portion of said packet having said value, and said stored information.

5 5. The method of claim 1, wherein, the step of periodically enabling said detector further comprises disabling said detector upon producing said synchronization signal, counting the next N-1 bytes in said data stream in response to said produced synchronization signal, and enabling said detector after said N-1 bytes.

10 6. The method of claim 4, wherein, when no match exists, said detector is enabled until a next detection of said value occurs.

 7. Apparatus for processing a digital data stream containing packets of information, each packet including a synchronization portion defining a value, and a packet identification portion, said apparatus comprising:

15 means for receiving packets of said data stream containing said synchronization portion and said packet identification portion;

 a detector having a controllable input and responsive to said value in said data stream for producing a synchronization signal, whereby said detector produces a synchronization signal in response to said synchronization portion of a packet in said data stream and also in response to an information item having said value;

20 a counter responsive to said synchronization signal, for counting a predetermined number of bytes associated with said received packets of said data stream, and for producing an enable signal for controlling said controllable input of said detector for enabling detection at a time corresponding to said predetermined number of bytes

25 after said synchronization signal, thereby enabling said detector to respond to a further synchronization portion associated with a packet in said data stream, and whereby, if said detector responds to an information item rather than to a synchronization portion, at least

said predetermined number of byte periods must pass before resynchronization can begin;
and

a comparator responsive to said synchronization signal for matching a
subsequent portion of said packet data stream following said detected value, with stored
5 information intended to correspond to said packet identification portion, and, in the
absence of a match, generating and applying an input enable signal to said controllable
input, thereby enabling said detector to further search for and detect a received said value
prior to the expiry of a period of said predetermined number of bytes.

10 8. The apparatus of claim 7, wherein said digital data stream containing
packets of information comprise N-byte information packets, and wherein said
predetermined number of bytes comprise N-1 bytes.

9. The apparatus of claim 8, wherein said information packets are encrypted,
15 and wherein a key-controlled decryptor receives said encrypted N-byte information
packets, for producing decrypted information.

10. The apparatus of claim 9, wherein a byte clock generator is responsive to
said synchronization signal for resetting said clock, and a serial-to-parallel converter is
20 coupled to said receiving means and to said byte clock generator, for converting said
information in said data stream from serial bit to byte form at the rate of said byte clock.

11. The apparatus of claim 7, wherein said receiving means includes a delay device for delaying the number of bits in a byte of said information packets in said data stream.

5

12. The apparatus of claim 7, wherein said apparatus is disposed in a smart card.

13. A method of processing a digital data stream containing packets of information, said packets including a synchronization portion defining a value, and a packet identification portion, said method comprising:

10

receiving packets of said data stream containing said synchronization portion and said packet identification portion;

15

enabling a detector for detecting said value in a portion of said data stream and generating a synchronization signal for synchronizing processing of said data stream, said enabling occurring according to a given bit count associated with said data stream; and

20

in response to a synchronization signal, comparing a portion of each packet with stored information intended to correspond to said packet identification portion, to determine whether said synchronization signal resulted from detection of said synchronization portion associated with said data stream; and if not, selectively enabling said detector for further detection of said value.

25

14. A smart card for decrypting encrypted N-byte information packets, where said information packets include a synchronization byte defining a value, a first plurality of packet identification bytes following said synchronization byte, and, from time to time, a decryption key, said card comprising:

key-controlled decryption means coupled to receive said encrypted N-byte information packets, for decrypting said information to produce decrypted information;

5 a delay device for delaying said information for the number of bits in a byte of said information, and for providing access to each of the bits in the information so delayed;

a controllable gate coupled to said delay device, for responding to said value with a synchronization signal, whereby said gate produces a synchronization signal in response to said synchronization byte and also in response to an information byte having said value;

10 key extraction means coupled to receive said information, for, when synchronized to said packets by said synchronization signal, extracting said key, thereby allowing said decryption means to decrypt said information;

a byte clock generator;

15 a serial-to-parallel converter coupled to an output port of said delay device and to said byte clock generator, for converting the information output from said delay device from serial bit to byte form at the rate of said byte clock;

20 a byte counter coupled to receive said synchronization signal, for counting N-1 bytes, and for producing an enable signal for controlling said controllable gate at a time N-1 bytes after said synchronization signal, thereby enabling said controllable gate to respond to a further synchronization byte, whereby, if said controllable gate responds to an information byte rather than to a synchronization byte, at least N-1 byte periods must pass before resynchronization can begin;

25 identification packet comparison means coupled to said serial-to-parallel converter, for matching with stored information at least one of said first plurality of packet identification bytes following said synchronization signal generated by said controllable gate, and, in the absence of a match, for generating and applying a gate enable signal to said controllable gate, thereby enabling said controllable gate to search

for said value prior to the expiry of a period of N-1 bytes.

15 15. The smart card of claim 14, wherein said identification packet comparison means further does not respond in the presence of a match between said stored
5 information and said at least one of the next four bytes following said synchronization signal.

10 16. The smart card of claim 14, wherein said identification packet comparison means matches with stored information at least two of the next four bytes following said
synchronization signal generated by said controllable gate, and, in the absence of a match, generates and applies a gate enable signal to said controllable gate.

15 17. The smart card of claim 14, wherein said number N of bytes in a packet is 188, and said number N-1 is 187.

18. The smart card of claim 17, wherein the number of said first plurality of packet identification bytes in each packet is four.

20 19. The smart card of claim 18, wherein said four packet identification bytes immediately follow said synchronization signal generated by said controllable gate.

20. The smart card of claim 18, wherein said encrypted information is MPEG serial transport stream video.

25 21. The smart card of claim 20, wherein said information is video.

22. The smart card of claim 14, wherein said first plurality of packet identification bytes in each packet immediately follows said synchronization byte.

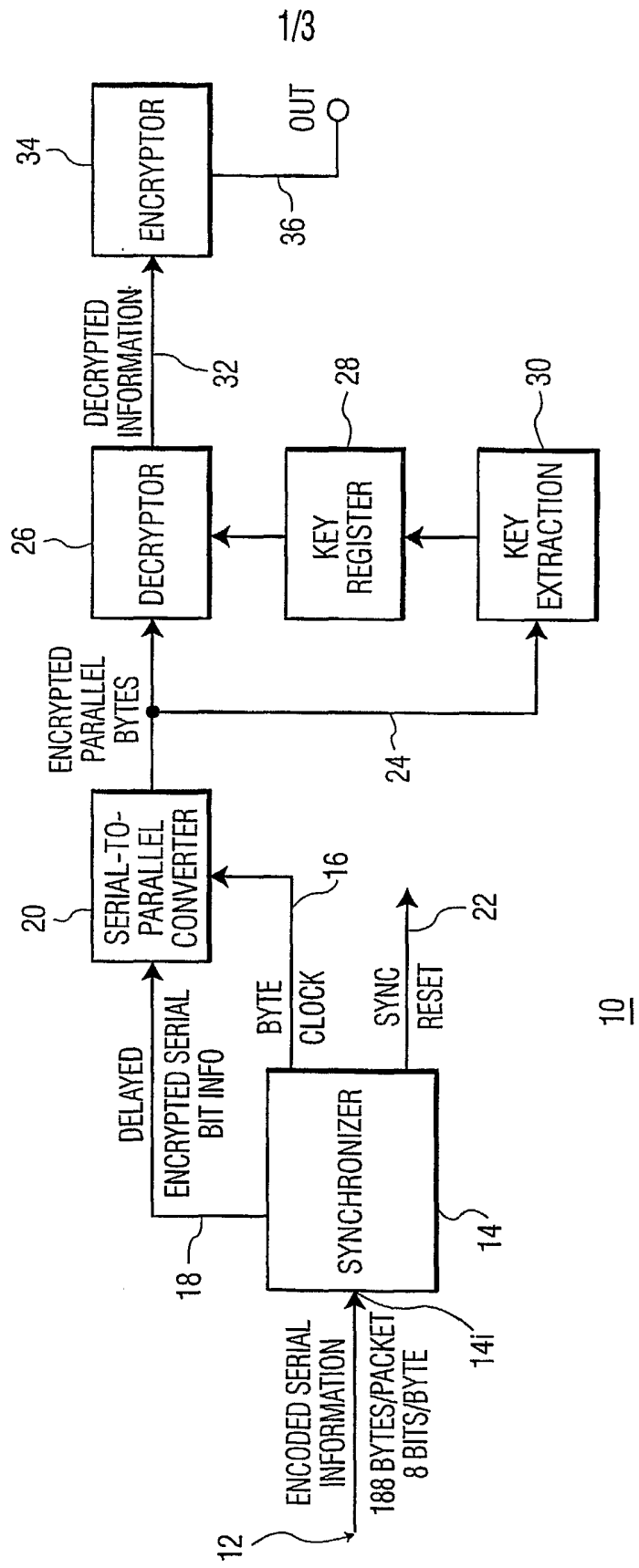


FIG. 1

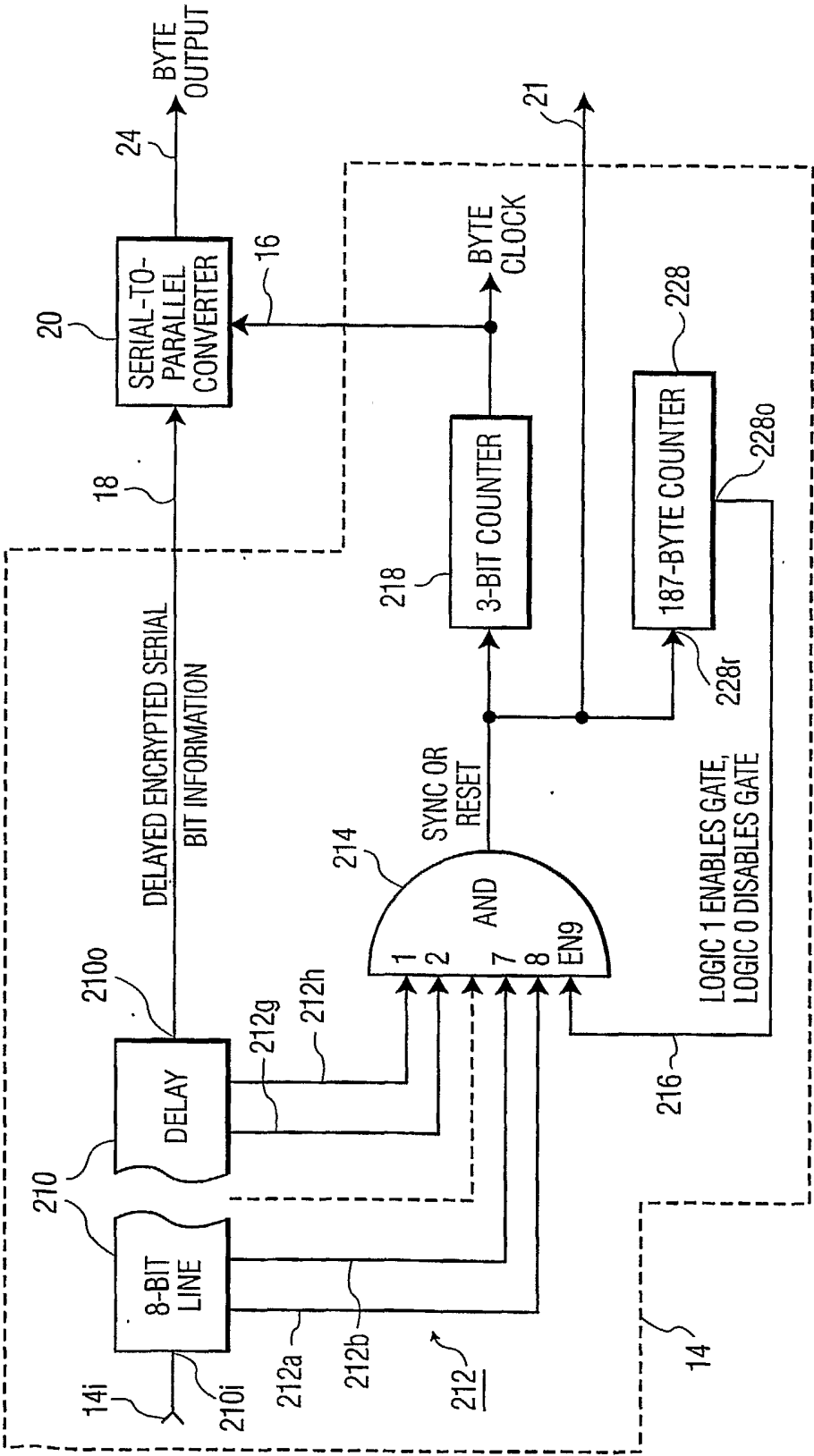


FIG. 2
PRIOR ART

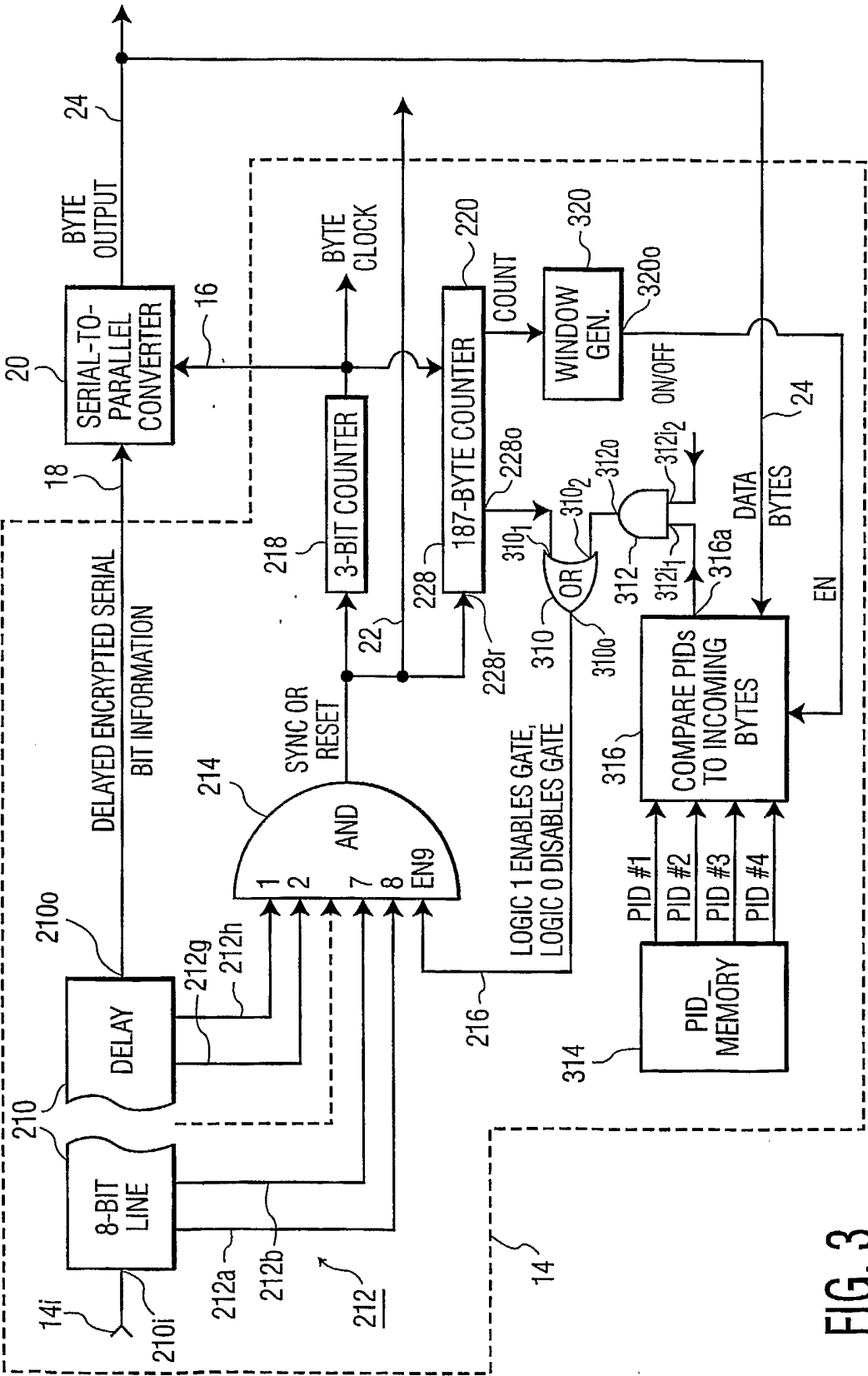


FIG. 3

INTERNATIONAL SEARCH REPORT

Internatio Application No

PCT/US 03/25905

A. CLASSIFICATION OF SUBJECT MATTER
 IPC 7 H04L7/04 H04L7/10

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 H04L

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

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

EPO-Internal, WPI Data, IBM-TDB, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 154 468 A (AKIWUMI-ASSANI SAMUEL O ET AL) 28 November 2000 (2000-11-28) column 1, line 38 - line 57 column 6, line 18 -column 8, line 14 column 9, line 12 - line 20 ----	1-22
A	US 6 118 819 A (KIM HYEONG-GEUN) 12 September 2000 (2000-09-12) column 3, line 12 - line 31 ----	1-22
A	US 5 703 887 A (HEEGARD CHRIS ET AL) 30 December 1997 (1997-12-30) column 1, line 63 -column 2, line 14 ----- -/--	1-22

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

☒ 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.

G document member of the same patent family

Date of the actual completion of the international search

9 December 2003

Date of mailing of the international search report

29/12/2003

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

Agudo Cortada, E

INTERNATIONAL SEARCH REPORT

Internatio Application No
PCT/US 03/25905

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4 763 339 A (TAYLOR THEODORE E ET AL) 9 August 1988 (1988-08-09) column 1, line 16 - line 18 column 1, line 36 - line 50 column 3, line 9 - line 16 column 4, line 8 - line 11 -----	1-22

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internatio Application No

PCT/US 03/25905

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 6154468	A	28-11-2000	EP 0868797 A1 WO 9818233 A1 JP 2000507785 T	07-10-1998 30-04-1998 20-06-2000
US 6118819	A	12-09-2000	KR 180501 B1 JP 10117189 A	01-05-1999 06-05-1998
US 5703887	A	30-12-1997	CA 2165604 A1 JP 8256336 A	24-06-1996 01-10-1996
US 4763339	A	09-08-1988	GB 2156189 A ,B HK 21890 A JP 60236536 A SG 73989 G	02-10-1985 30-03-1990 25-11-1985 20-04-1990