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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 November 2002 (21.11.2002)

PCT

(10) International Publication Number
WO 02/093827 A1

(51) International Patent Classification[7]: H04L 9/18, H04K 1/06, H04N 7/167, G06F 3/14

(21) International Application Number: PCT/US02/15703

(22) International Filing Date: 15 May 2002 (15.05.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/859,212 15 May 2001 (15.05.2001) US

(71) Applicant: **SONY ELECTRONICS INC.** [US/US]; 1 Sony Drive, Park Ridge, NJ 07656 (US).

(72) Inventor: **PHAM, Steve**; 905 Westridege Drive, Milpitas, CA 95035 (US).

(74) Agents: **KULAS, Charles, J.** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, Eighth Floor, San Francisco, CA 94111 (US).

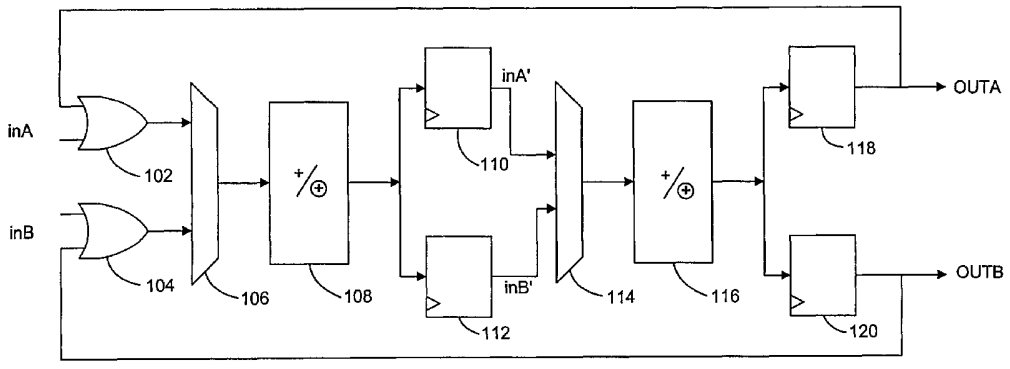
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, 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, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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: ENCRYPTION/DECRYPTION ENGINE FOR MULTIPLE DATA STREAMS



(57) Abstract: Buffers, or registers, (110), 112, 118, 120) are used at one or more places between processing stages(108, 116) in a device for decrypting a data stream (inA. inB). The device has multiple processing stages (108, 116) arranged in a circular manner so that data is repeatedly passed from a prior stage (108) to a next stage (116), and from a last stage (116) back to a first stage (108), until processing is completed. The use of one or more registers (110, 112, 118, 120) at one or more positions allows data to be stored so that the stream(inA) associated with the stored data can effectively be suspended. This allows data from another stream (in B) to be processed while the suspended stream (inA) is in a wait state.

WO 02/093827 A1

ENCRYPTION/DECRYPTION ENGINE FOR MULTIPLE DATA STREAMS

BACKGROUND OF THE INVENTION

This invention relates in general to encryption/decryption devices and more specifically to a decryption device capable of handling multiple independent data streams in a time-multiplexed fashion.

As information is increasingly handled in digital formats it becomes ever more important to provide security safeguards for these formats. For example, digital video has very demanding requirements in the need to restrict access. Formats such as the IEEE 1394 Standard for isochronous data transfer, Motion Picture Experts Group (MPEG) standards and high-definition television (HDTV) standards along with access, transfer and processing standards as promulgated by such organizations as Digital Transmission Licensing Administrator (DTLA – see, e.g., www.dtca.com) have imposed performance levels for devices using encryption and decryption on standardized digital formats. Because of the complex nature of encryption and decryption processing, and the extremely high bandwidth requirements of digital video, it is difficult to design circuits that can meet all of the requirements.

Fig. 1A shows a prior art encryption/decryption device.

In Fig. 1A, a data stream, such as an IEEE 1394-compliant data stream 10 is input into the left side of the device's circuitry as "chunks" of 64-bit words. Key 12 can be a variable-length word that is also input into the device as shown in Fig. 1A. The device includes several stages where each stage includes an exclusive or (XOR) 14 function followed by an addition operation 16. This process is repeated for a total of five stages as shown in Fig. 1A. At the end of the fifth stage, the result from adder 18 is looped back to the input of XOR 14.

Each cycle through the five stages completes a "round" through the device. Typically, multiple rounds are required. For example, a device may require ten rounds before either the encryption or decryption function is complete for the respective word.

This design can be referred to as a "circular arrangement" of multiple "processing stages." Each processing stage, such as 14 and 16, are arranged so that the output of a preceding stage is fed to the input of a succeeding stage. In other words, processing stage 14 performs its XOR operation on a data word and then passes the result to

processing stage 16 where an addition is performed. In this case, since the application is an encryption or decryption device, each stage also is provided with the key and each operation is a two-operand operation.

Note that applications other than encryption and decryption may use similar architecture.

It should be apparent that the ten rounds of processing through five stages where each stage includes multiple operations represents many cycles of processing for just a single 64-bit word. Naturally, a video stream is made up of many millions, trillions, or more, words of data that need to be processed in this multi-round manner.

Typically, the encryption process starts and ends at the boundary of a block of data. The block of data is called an "encryption frame." Processing of a next encryption frame can only commence after completion of processing of a current frame. In other words, it is not possible to interleave the processing of encryption frames. This means that a prior art approach, such as shown in Fig. 1A, does not allow for efficient concurrent processing of multiple data streams.

To further complicate efficient encryption/decryption of streams, it is typical in digital video applications that encryption frames are arbitrarily split into smaller data blocks. These data blocks can then be transferred over a communication link over varying periods of time and with varying intervals between block transmissions. This means that the start and end of an encryption frame of one data stream does not necessarily align with the frame from another stream. For this reason, the circuit of Fig. 1A is dedicated for real-time processing of a single data stream. To handle a second stream, another similar circuit would have to be employed.

Fig. 1B shows a time line where two prior art circuits of Fig. 1A are used.

In Fig. 1B, two input streams are processed as stream A and stream B. Each stream must be independently processed with two separate encryption circuits. The need for two circuits increases the complexity and size of the hardware necessary to process two streams, rather than just a single stream.

Stream A and B have frames divided into multiple blocks denoted as, for example, A0, A1, A2, etc. To complete the encryption/decryption of block A0 into block A0', block A0 and parts of block A1 are used. If there is a pause in reception of block A1 then the circuit must wait until block A1 is received to complete processing for block A0'.

The uninterruptible and serial processing of the device of Fig. 1A means that it is not possible for the device to process data from stream B when it is currently processing the encryption frame of stream A.

Thus, it is desirable to provide an invention that improves upon the prior art.

SUMMARY OF THE INVENTION

An encryption device providing for time-multiplexed processing of multiple data streams. In a digital video application the device is a decryption device for an isochronous data stream such as an IEEE 1394 - compliant data stream. The device uses multiple processing stages arranged in a circular fashion for processing data by passing the data through the stages multiple times, or rounds. When data reaches the last processing stage it is sent back to the first stage to begin a next round of processing. After several rounds of processing, the data is output.

Buffers, or registers, are used at one or more positions between processing stages. The use of one or more registers at a position allows data to be stored so that the stream associated with the stored data can effectively be suspended. This allows data from another stream to be processed while the suspended stream is in a wait state.

In one embodiment the invention provides a buffer coupled between at least two stages to provide for storing of at least one stage's output, and for later selectively providing the stored at least one stage's output to a successive stage.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1A shows a prior art encryption/decryption device;

Fig. 1B shows a time line where two prior art circuits of Fig. 1A are used;

Fig. 2A shows a block diagram of a generalized device of the present invention; and

Fig. 2B illustrates time-multiplexed processing of the circuit of Fig. 2A.

DESCRIPTION OF THE SPECIFIC EMBODIMENTS

Fig. 2A shows a block diagram of the generalized concept of the present invention.

In Fig. 2A, a multiple-stage digital processor is shown with the stages arranged in a circular manner. Stages 108 and 116 represent any type of digital processing stage. As will be apparent, any number of stages can be represented by stages 108 and 116.

Input is received at the left of the diagram at either of inputs in_A and in_B feeding XOR gates 102 and 104. The inputs are fed into multiplexer 106, which selectively applies one of the inputs to processing stage 108.

The output of processing stage 108 is selectively fed to one of two registers, or buffers, 110 and 112. Register 110 serves to store, and output, a value corresponding to in_A which is referred to as in_A' while register 112 receives, stores, and outputs in_B'.

Both outputs from registers 110 and 112 are fed to multiplexer 114. Multiplexer 114 selectively applies either in_A' or in_B' to processing stage 116. The output from processing stage 116 is sent, in turn, to a second set of registers 118 and 120. Again, register 118 corresponds to the A data stream while register 120 corresponds to the D data stream.

Register 118 outputs its value which is fed back through XOR gate 102 and multiplexer 106 to processing stage 108. Similarly, register 120's output is fed back to XOR gate 104 and multiplexer 106 to processing stage 108. When processing is complete for a given data word in either the A or B streams, then registers 118 and 120 output the result as OUT_A or OUT_B.

It should be apparent that the two processing stages have been split up by register banks at the outputs of each processing stage. Also, a multiplexer is used to select one of the two data words, corresponding to either the A or B data streams, at the input of each of the processing stages. The components of Fig. 2A are controlled by signals (not shown), as is noted in the art, to allow the selection of either A-stream or B-stream processing, as desired.

For example, to process A-stream data, multiplexer 106 selects the output of XOR gate 102 while new data is applied at in_A. This causes the in_A data to be processed by processing stage 108 and output to registers 110 and 112. Data at the input of register 110 is clocked so that a the processed in_A data word from processor stage 108 is stored in register 110. This value can be stored for any length of time to suspend processing of A-stream data.

While processing of A-stream data has been suspended, it is possible to continue to process a different stream, such as stream B. While A-stream data is held in register 110, B-stream data can be output from register 112 to processing stage 116. Thus, these registers allow processing of data in one stream to be suspended in favor of processing in another stream. Although the present example uses two register banks in a simplified diagram where there are two processing stages, it should be apparent that any number of register banks can be used interspersed among any number of processing stages. As discussed below, this will give different degrees of control, and a larger number of ways to multiplex, the data streams. Further, more than two registers can exist in each register bank. For example, instead of just two registers 110 and 112 accepting output from processing stage 108 and feeding multiplexer 114, there can be many registers for handling a corresponding number of data streams.

In Fig. 2A, a preferred embodiment of the invention alternately feeds A-stream data and B-stream data to each processing stage. This allows an interleaved, time multiplexed processing of two completely separate data streams. Thus, if one stream is stalled, the other stream can continue processing.

In this interleaved, time multiplexed mode, processing stage 108 is processing A-stream data while processing stage 116 is processing B-stream data. Assuming that the stages finished their processing at the same time, the A-stream data of processing stage 108 is stored in register 110 while the B-stream data of processing stage 116 is stored in register 120. Since this processing only represents one-half of a full round in this two-processing stage device, the second half of the round has processing stage 108 processing B-stream data from register 120 while processing stage 116 processes A-stream data output from register 110.

Fig. 2B illustrates time multiplexed processing in diagram form.

In Fig. 2B, the chart shows timing diagrams with respect to the six signals – in_A, in_A', OUT_A, in_B, in_B' and OUT_B. As can be seen from Fig. 2B, the A-stream data is applied to processing stage 108 in a first one-half cycle, or phase A, while the B-stream data is applied to processor stage 108 in the second-half cycle of each round, or phase B. This means that the output of processing stage 108 provides a result for the A-stream data at the end of phase A, and provides an output for the B-stream data at the end of phase B.

The in_A' row of the chart of Fig. 2B shows that register 110 has latched the A-stream data and holds it available for phase B in each round of processing. In other words, in round 10 processing (the first round), A'_{10} is available during phase B at the output of

register 110. Similarly, in round 9, A'_9 is available in phase B of round 9, etc. At the end of each round, the output of processing stage 116 is A-stream data. This data is latched into register 118 and is available as OUT_A. This is shown in the timing chart for the row labeled OUT_A. Similarly, B-stream data is processed by the second stage processor, processing stage 116, during phase A of each round so that OUT_B is available at the end of phase A of each round. This can be seen by referring to the row labeled OUT_B of Fig. 2B.

Thus, it should be apparent from the timing chart of Fig. 2B that the hardware shown in Fig. 2A is able to interleave, or time multiplex, two separate data streams without requiring any additional circuitry in the form of duplicate processing stages.

Although the invention has been discussed with regard to a specific embodiment thereof, it should be apparent that many variations and modifications to the preferred embodiment are possible without departing from the scope of the invention. For example, although functions for processing stages have been presented as addition, rotation, exclusive OR, it should be apparent that any type of processing can be performed by each stage and that different types of operations can be performed by different stages within the same circuit. The positioning of register banks within the multiple stages need not be symmetric with respect to the overall device. That is, a register bank can be placed one third of the way down the series of processing stages, at the end of all of the stages, etc.

Thus, the scope of the invention is to be determined solely by the appended claims.

WHAT IS CLAIMED IS:

1. A digital processing device, comprising:

a circular arrangement of two or more processing stages, wherein each processing stage receives as input one different processing stage's output, wherein any given processing stage performs a function on digital data received at the given processing stage's input to produce the given processing stage's output;

wherein the circular arrangement includes a first stage, wherein the first stage receives a digital data word;

wherein the circular arrangement includes a last stage, wherein the last stage outputs a processed digital data word;

processing control circuitry for controlling the processing stages so that the digital data word is received and processed by the first stage and, thereafter, by each successive stage in the circular arrangement so that when the processed digital data word is output by the last stage, the processed digital data word is transferred back to the first stage at least once before being output by the last stage;

at least one buffer for storing the output of one or more of the processing stages; and

buffer control circuitry for controlling storing the output of one or more of the processing stages into the at least one buffer so that processing of the digital data word is suspended.

2. The digital processing device of claim 1, wherein the digital data word is one or more bits in width.

3. The digital processing device of claim 1, wherein the function is an arithmetic operation.

4. The digital processing device of claim 1, wherein the function is a logical operation.

5. The digital processing device of claim 1, wherein the first stage includes a data key input for receiving a cryptographic key to be applied to the data during processing.

6. The digital processing device of claim 5, wherein the digital processing device achieves an encryption function.

7. The digital processing device of claim 5, wherein the digital processing device achieves a decryption function.

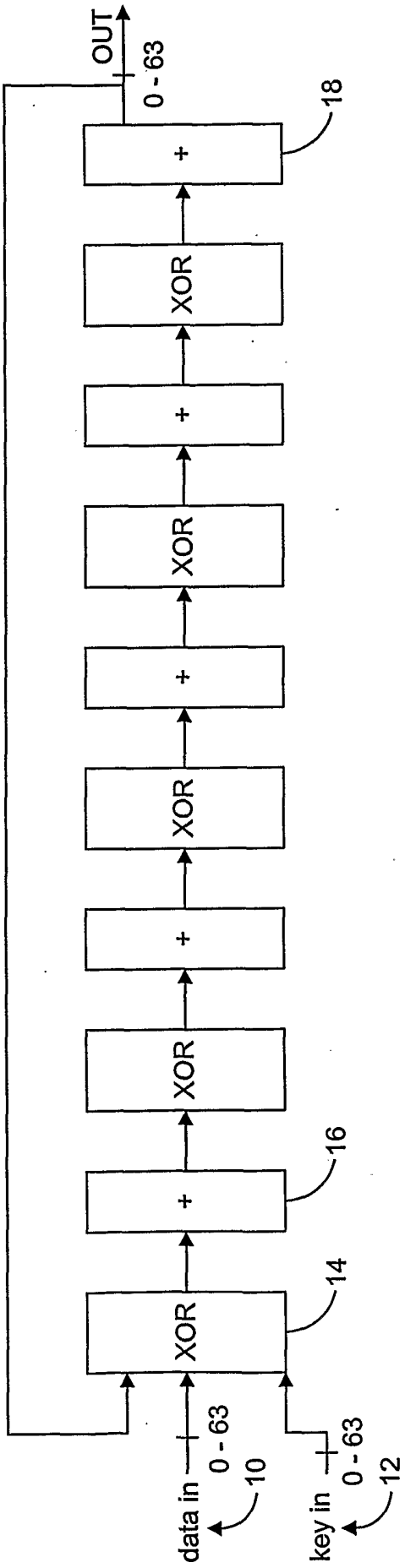
8. The digital processing device of claim 1, further comprising:
multiple buffers coupled to the output of one or more of the processing stages.

9. The digital processing device of claim 8, wherein a group of multiple buffers is coupled to the output of the last stage.

10. The digital processing device of claim 9, wherein a multiplexer is coupled to the outputs of two or more of the multiple buffers so that one selected output from the two or more multiple buffers can be selected.

11. The digital processing device of claim 1, wherein the digital data word is part of a stream of encrypted video information.

12. A digital decryption device with the ability to suspend processing of a current data word, wherein the digital decryption device includes a plurality of stages arranged in a circular manner so that each stage's output is successively fed to a next stage's input, wherein a first stage receives a data word to be decrypted and wherein a last stage both outputs a data word back to the first stage and makes the output data word available as output data from the digital decryption device, the digital decryption device further comprising:
a buffer coupled between at least two stages to provide for storing of at least one stage's output, and for later selectively providing the stored at least one stage's output to a successive stage.



Prior Art

Fig. 1A

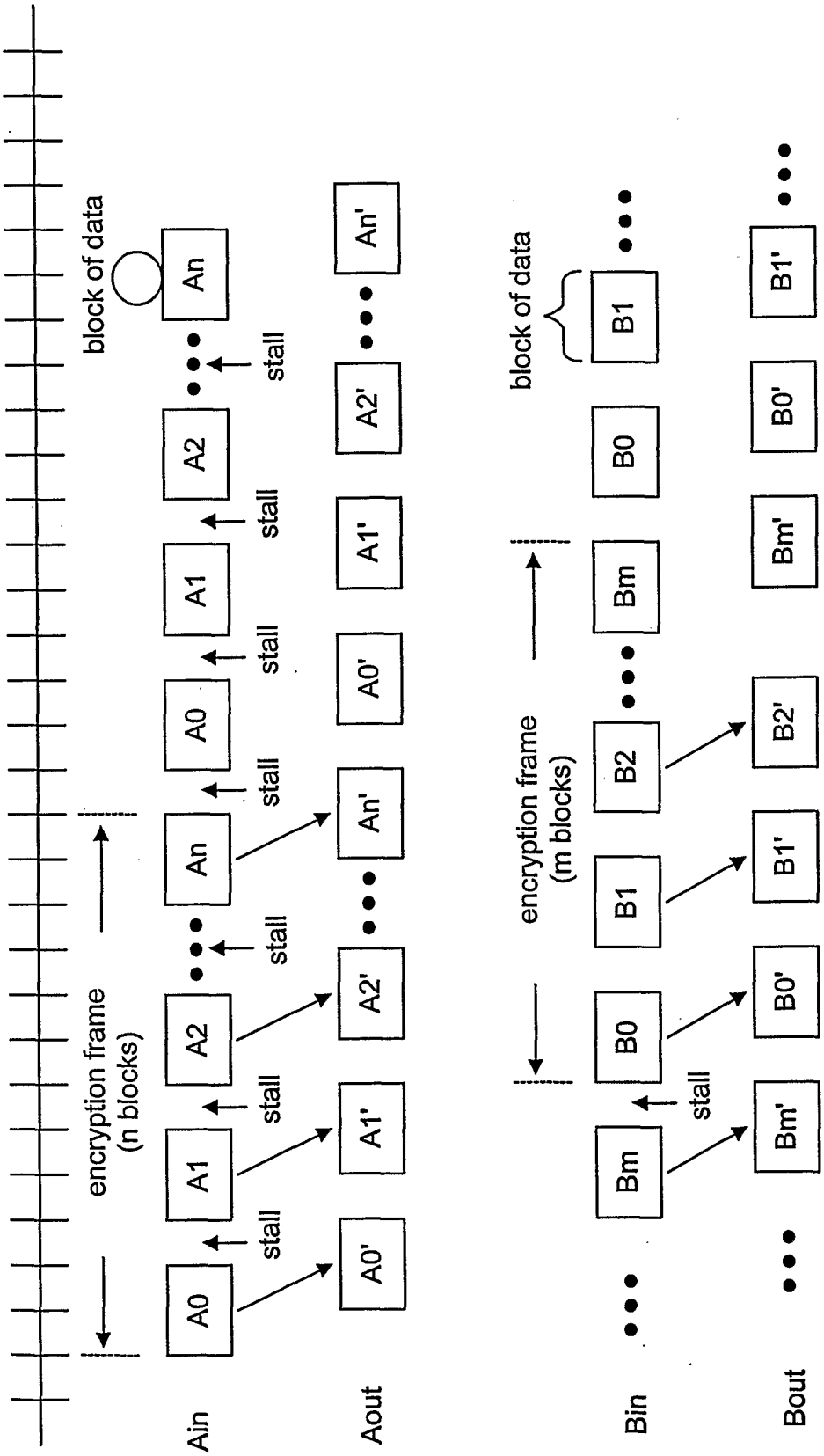

block of data
encryption frame
(n blocks)
Ain
Aout
A0
A1
A2
An
A0'
A1'
A2'
An'
stall
Bin
Bout
B0
B1
B2
Bm
B0'
B1'
B2'
Bm'

Fig. 1B

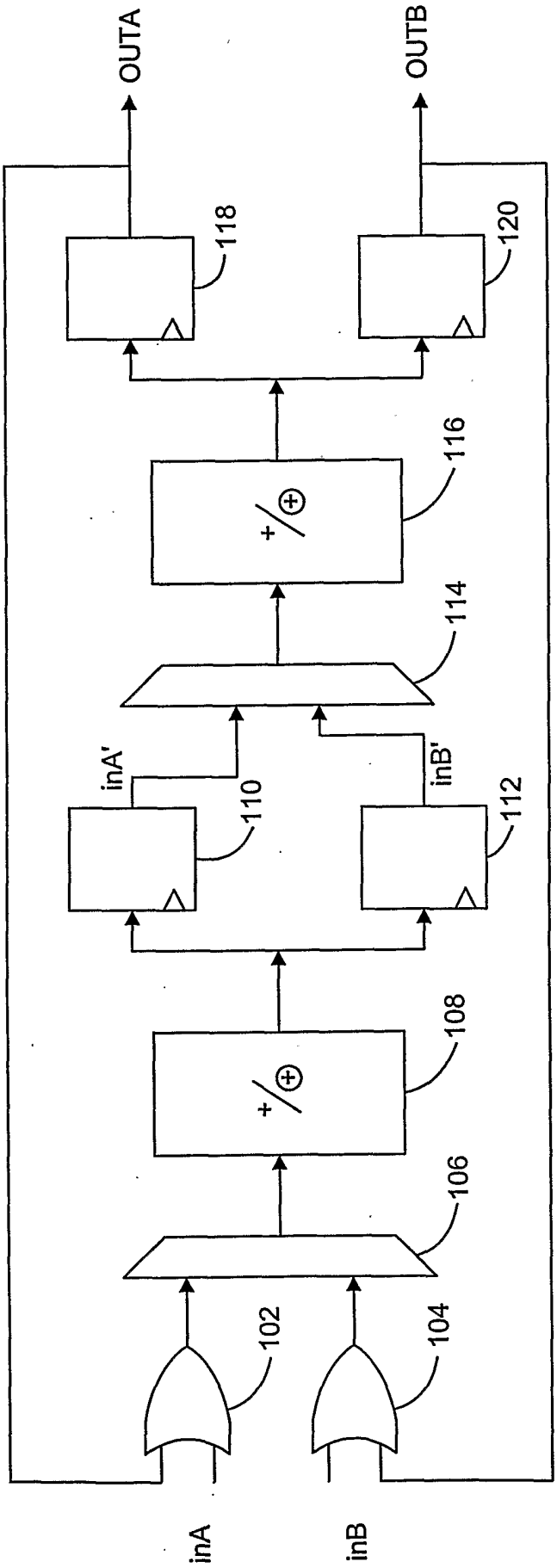

OUTA
OUTB
118
120
116
114
inA'
inB'
110
112
108
106
102
104
inA
inB

Fig. 2A

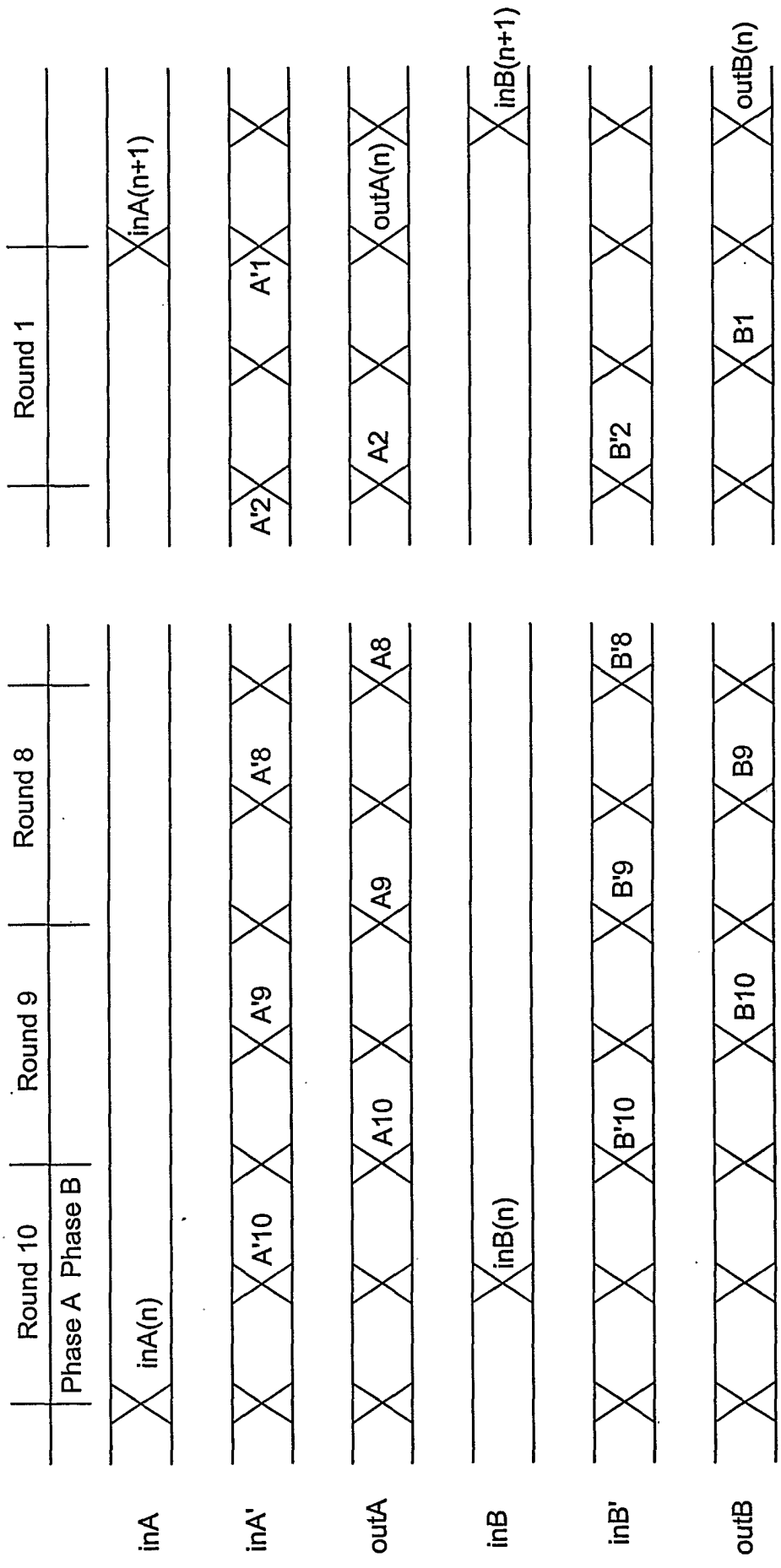

Round 10
Phase A
Phase B
Round 9
Round 8
Round 1
inA
inA(n)
inA(n+1)
inA'
A'10
A'9
A'8
A'2
A'1
outA
A10
A9
A8
A2
outA(n)
inB
inB(n)
inB(n+1)
inB'
B'10
B'9
B'8
B'2
outB
B10
B9
B1
outB(n)

Fig. 2B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/15703

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/18
US CL : 380/42

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : Please See Continuation Sheet

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,189,095 B1 (COPPERSMITH et al.) 13 February 2001 (13.02.2001), column 8, lines 50-58; column 10, lines 7-15; column 13, lines 51-56; column 14, lines 4-9 and 35-46;	1-9, 12
---		---
Y	column 15, lines 8-30 and 66-67; column 16, lines 1-7; column 17, lines 41-45; column 18, lines 31-67; column 19, lines 1-28 and 47-54; and figure 4, items M1-M4, c[0]-c[3].	10, 11
Y	US 6,195,368 B1 (GRATACAP) 27 February 2001 (27.02.2001), column 2, lines 19-24; column 6, lines 7-27; and column 27, lines 3-41.	10, 11

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

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

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 August 2002 (14.08.2002)	10 SEP 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer FOR Justin T. Darrow James R. Matthews Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

PCT/US02/15703

Continuation of B. FIELDS SEARCHED Item 1:
IPC (7) : H04L 9/18; H04K 1/06; H04N 7/167; G06F 3/14

US CL : 380/37, 42, 43, 205, 210, 212, 252; 708/135

Continuation of B. FIELDS SEARCHED Item 3:
EAST(USPAT; EPO; JPO; DERWENT; US-PGPUB)
search terms: processing, processor, word, byte, bit, bitsequence, sequence, frame, block, subblock, stream, first, initial, beginning, stage, module, repeat, multiple, buffer, register, arithmetic, add, subtract, multiply, divide, logic, "XOR", exclusive, gate, encrypt, encipher, encypher, scramble, cryptographic, key, value, ECM, EMM, control, management, message, decrypt, decipher, decypher, descramble, unscramble