

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
18 December 2003 (18.12.2003)

PCT

(10) International Publication Number  
WO 03/104973 A1

- (51) International Patent Classification<sup>7</sup>: **G06F 7/72**
- (21) International Application Number: PCT/IB03/02583
- (22) International Filing Date: 4 June 2003 (04.06.2003)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:  
0213242.1 7 June 2002 (07.06.2002) GB
- (71) Applicant (for all designated States except US): **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL];  
Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

- (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, SC, SD, SE, SG, SK, SL, 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).

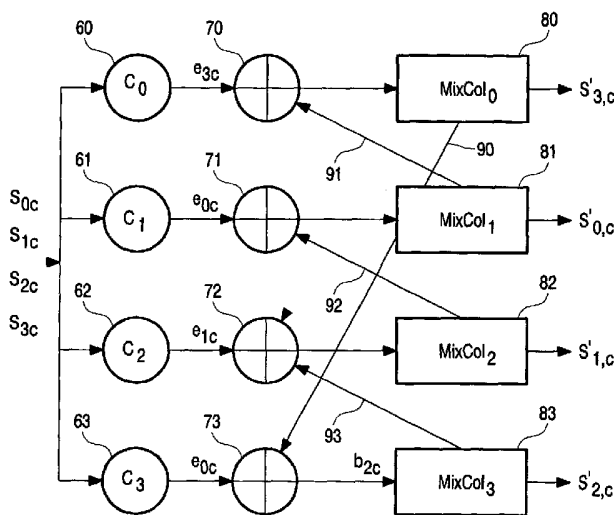
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): **HUBERT, Gerardus, T., M.** [NL/NL]; c/o Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB).
- (74) Agent: **TURNER, Richard, C.**; Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB).

**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: AES MIXCOLUMN TRANSFORM



(57) **Abstract:** A simplified logic circuit for performing the AES Rijndael MixColumns transform exploits the common relationship between each of the successive rows of the transform matrix and its preceding row. A logic circuit for performing multiplication of an  $(m \times n)$  matrix by a  $(1 \times n)$  or by a  $(m \times 1)$  matrix, where  $m$  is a number of rows and  $n$  is a number of columns, and where each successive row,  $m$ , of  $n$  elements is a predetermined row permutation of a preceding row comprises:  $n$  multiplication circuits;  $n$  logic circuits;  $n$  registers for receiving logical output from the logic circuits; feedback logic for routing the contents of each register to a selected one of inputs of the logic circuits in accordance with a feedback plan that corresponds to the common relationship between successive matrix rows; and control means for successively providing as input to each of the  $n$  multiplication circuits each element in the  $(1 \times n)$  or  $(m \times 1)$  matrix.

WO 03/104973 A1

## DESCRIPTION

**AES MIXCOLUMN TRANSFORM**

5

The present invention relates to methods and apparatus for implementation of the Advanced Encryption Standard (AES) algorithm and in particular to methods and apparatus for performing the matrix multiplication operation that constitutes the AES MixColumn transformation in each of the encryption and decryption rounds of the algorithm.

The invention has particular, though not exclusive, application in cryptographic devices such as those installed in smart cards and other devices where processor and memory resources are somewhat limited and many operations of the cryptographic algorithm are performed in dedicated ASIC or FPGA hardware.

The AES algorithm has wide application in the encryption of data to be transmitted in a secure fashion. One application is in the transmittal of personal and/or financial information from a smartcard to a card reader device. Confidential data stored on the card must not be retrieved from the card except in encrypted form to ensure that the data so retrieved cannot be intercepted and read by an unauthorised third party. Only the authorised reader is able to decrypt the data retrieved from the card.

Similarly, data supplied by the card reader to be stored in the card must be passed to the card in encrypted form, and decrypted by the card for storage and subsequent retrieval.

While the AES algorithm is relatively straightforward to implement in a conventional computer system deploying state of the art processor and memory circuits, in a smartcard application, the processor and memory resource is very limited, and many functions must be executed in dedicated hardware, such as ASICs or FPGAs.

There is therefore a requirement for hardware implementations of the procedures required in the AES algorithm which implementations require the minimum use of hardware resource.

5 It is an object of the present invention to provide suitable circuitry for effecting the MixColumn transform deployed in the standard AES (Rijndael) cryptographic algorithm, both for encryption and decryption.

According to one aspect, the present invention provides a logic circuit for multiplication of an  $(m \times n)$  matrix by a  $(1 \times n)$  or by a  $(m \times 1)$  matrix, where  
10  $m$  is a number of rows and  $n$  is a number of columns, and wherein each successive row  $m$ , of  $n$  elements is a predetermined row permutation of a preceding row, the circuit comprising:

$n$  multiplication circuits each having an input and an output which returns the value of said input multiplied by a predetermined multiplicand;

15  $n$  logic circuits, each for executing a predetermined logical combination of a first input and a second input to provide a logical output, the first input being coupled to the output of a corresponding one of the  $n$  multiplication circuits;

$n$  registers for receiving said logical output;

20 feedback logic for routing the contents of each register to a selected one of the second inputs in accordance with a feedback plan that corresponds to the predetermined row permutation; and

control means for successively providing as input to each of the  $n$  multiplication circuits each element in the  $(1 \times n)$  or  $(m \times 1)$  matrix.

25

Embodiments of the present invention will now be described by way of example and with reference to the accompanying drawings in which:

Figure 1 is a flow diagram illustrating implementation of an encryption operation using the AES block cipher algorithm; and

30 Figure 2 is a schematic diagram of a functional logic block for performing the MixColumns transform.

The AES algorithm for encryption of plaintext to ciphertext is shown in figure 1. The AES algorithm may be implemented using a 128-bit, a 192-bit or a 256-bit key operating on successive 128-bit blocks of input data. The present invention is applicable to all of these implementations. Figure 1 will now be described in the context of the basic implementation using a 128-bit key.

An initial 128-bit block of input plaintext 10 is XOR-combined 11 with an original 128-bit key 12 in an initial round 15. The output 13 from this initial round 15 is then passed through a number of repeated transform stages, in an encryption round 28 which includes the SubBytes transform 20, the ShiftRows transform 21 and the MixColumns transform 22 in accordance with the defined AES algorithm.

The output from the MixColumns transform 22 is XOR-combined 23 with a new 128-bit round key 26, which has been derived 25 from the initial (original) key 12. The output from this XOR-combination 23 is fed back to pass through the encryption round 28 a further number of times, the number depending upon the particular implementation of the algorithm.

For each successive iteration through the encryption round 28, a new round key 26' is derived from the existing round key 26 according to the AES round key schedule.

The number of iterations ( $N_r - 1$ ) of the encryption round 28 is nine where a 128-bit encryption key is being used, eleven where a 192-bit encryption key is being used, and thirteen where a 256-bit encryption key is being used.

After the requisite number ( $N_r - 1$ ) of encryption rounds 28, a final round,  $N_r$ , is entered under the control of decision box 24. The final round 30 comprises a further SubBytes transform 31, a further ShiftRows transform 32, and a subsequent XOR-combination 33 of the result with a final round key 36 generated 35 from the previous round key. The output therefrom comprises the ciphertext output 39 of the encryption algorithm.

The present invention relates particularly to the performing of the MixColumns transform 22. Through the rounds 28, 30, the 128-bit blocks

being processed are conveniently represented as 16 8-bit blocks in a  $4 \times 4$  matrix, as  $s_{\text{row}, \text{column}}$ , according to the pattern,

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

5

In the MixColumns transform 22, the columns of this state are considered as polynomials over  $GF(2^8)$  and multiplied modulo  $(x^4 + 1)$  with a predetermined fixed polynomial  $a(x)$ , given by:

10

$$a(x) = a_3x^3 + a_2x^2 + a_1x + a_0,$$

in which, represented as hexadecimal values,

15

$$a_3 = 03 \text{ h}$$

$$a_2 = 01 \text{ h}$$

$$a_1 = 01 \text{ h}$$

$$a_0 = 02 \text{ h.}$$

20

The polynomial is co-prime to  $x^4 + 1$  and is therefore invertible.

For encryption, the MixColumns transform can therefore be expressed as

$$s_{r,c} \rightarrow s'_{r,c}, \text{ for each of the columns in } s.$$

25

$$\begin{pmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{pmatrix} = \begin{pmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{pmatrix} \begin{pmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{pmatrix}$$

The evaluation of this matrix multiplication is:

5

$$s'_{0,c} = \{02\} * s_{0,c} \oplus \{03\} * s_{1,c} \oplus s_{2,c} \oplus s_{3,c}$$

$$s'_{1,c} = s_{0,c} \oplus \{02\} * s_{1,c} \oplus \{03\} * s_{2,c} \oplus s_{3,c}$$

$$s'_{2,c} = s_{0,c} \oplus s_{1,c} \oplus \{02\} * s_{2,c} \oplus \{03\} * s_{3,c}$$

10  $s'_{3,c} = \{03\} * s_{0,c} \oplus s_{1,c} \oplus s_{2,c} \oplus \{02\} * s_{3,c}$

During decryption, the inverse of this operation is required. It is given by the following matrix multiplication.

15

$$\begin{pmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{pmatrix} = \begin{pmatrix} b_0 & b_3 & b_2 & b_1 \\ b_1 & b_0 & b_3 & b_2 \\ b_2 & b_1 & b_0 & b_3 \\ b_3 & b_2 & b_1 & b_0 \end{pmatrix} \begin{pmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{pmatrix} = \begin{pmatrix} 0E & 0B & 0B & 09 \\ 09 & 0E & 0E & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{pmatrix} \begin{pmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{pmatrix}$$

The evaluation of this matrix multiplication is:

20  $s'_{0,c} = \{0E\} * s_{0,c} \oplus \{0B\} * s_{1,c} \oplus \{0D\} * s_{2,c} \oplus \{09\} * s_{3,c}$

$$s'_{1,c} = \{09\} * s_{0,c} \oplus \{0E\} * s_{1,c} \oplus \{0B\} * s_{2,c} \oplus \{0D\} * s_{3,c}$$

$$s'_{2,c} = \{0D\} * s_{0,c} \oplus \{09\} * s_{1,c} \oplus \{0E\} * s_{2,c} \oplus \{0B\} * s_{3,c}$$

$$s'_{3,c} = \{0B\} * s_{0,c} \oplus \{0D\} * s_{1,c} \oplus \{09\} * s_{2,c} \oplus \{0E\} * s_{3,c}$$

It is noted that the MixColumns transform matrix has the special property that each successive row is a shifted or rotated version of the preceding row. In general, each element in a row appears in every row but in a different position in the row, and specifically, for the MixColumns transform  
5 matrix the different position of each element for each row constitutes a single position right shift or rotation.

According to the present invention, it has been recognised that this property allows the multiplication of each column of the state  $\mathbf{s}$  to be achieved with significantly reduced hardware.

10 Figure 2 illustrates an exemplary embodiment of hardware logic 50 adapted for the multiplication of an  $m \times n$  matrix by a  $1 \times n$  matrix, in which the relationship between each successive row of  $n$  elements of the  $m \times n$  matrix is a predetermined row shift. For the AES MixColumns transform,  $m = 4$ ,  $n = 4$  and the predetermined relationship is a single right shift.

15 The logic 50 comprises four 8-bit multiplication circuits 60 ... 63, four 8-bit XOR gates 70 ... 73 and four feedback / output registers 80 ... 83, shown as MixCol<sub>0</sub> ... MixCol<sub>3</sub>. Each multiplication circuit 70 ... 73 is adapted for multiplication of an input by one of the matrix coefficients  $c_0, c_1, c_2, c_3$ . Each of  
20 the XOR gates 70 ... 73 may be implemented using any appropriate combination of logic elements required to execute the appropriate logical combination of two inputs, as described hereinafter.

For encryption rounds, the values of  $c_0 \dots c_3$  are, respectively,  $a_0 \dots a_3$  as defined above. For decryption rounds, the values of  $c_0 \dots c_3$  are,  
25 respectively,  $b_0 \dots b_3$  as defined above. The output of each multiplication circuit 60 ... 63 is coupled to a first input of a corresponding XOR gate 70 ... 73. The output of each XOR gate 70 ... 73 is coupled to a corresponding MixCol register 80 ... 83. The output of each MixCol register 80 ... 83 is coupled to the second input of one of the XOR gates 70 ... 73 according to a  
30 feedback plan 90 ... 93 that corresponds to the row shift function that defines the relationship between successive rows of the matrix. In the present case, the feedback plan 90 ... 93 implements the right row shift function between

successive rows of the matrices  $a_{r,c}$  (encryption) and  $b_{r,c}$  (decryption) – more generally the matrix  $c_{r,c}$ .

During operation of the circuit 50,  $s_{0c}$ ,  $s_{1c}$ ,  $s_{2c}$ ,  $s_{3c}$  are sequentially offered to the multiplication logic 60 ... 63 on successive cycles. At the outset of each column multiplication, the registers MixCol<sub>0</sub> to MixCol<sub>3</sub> are pre-set to zero.

*After the 1<sup>st</sup> cycle:*

$$\text{MixCol}_0 = c_{0.s_{0c}}$$

$$10 \quad \text{MixCol}_1 = c_{1.s_{0c}}$$

$$\text{MixCol}_2 = c_{2.s_{0c}}$$

$$\text{MixCol}_3 = c_{3.s_{0c}}$$

*After the 2<sup>nd</sup> cycle:*

$$15 \quad \text{MixCol}_0 = c_{0.s_{1c}} \oplus c_{1.s_{0c}}$$

$$\text{MixCol}_1 = c_{1.s_{1c}} \oplus c_{2.s_{0c}}$$

$$\text{MixCol}_2 = c_{2.s_{1c}} \oplus c_{3.s_{0c}}$$

$$\text{MixCol}_3 = c_{3.s_{1c}} \oplus c_{0.s_{0c}}$$

20 *After the 3<sup>rd</sup> cycle:*

$$\text{MixCol}_0 = c_{0.s_{2c}} \oplus c_{1.s_{1c}} \oplus c_{2.s_{0c}}$$

$$\text{MixCol}_1 = c_{1.s_{2c}} \oplus c_{2.s_{1c}} \oplus c_{3.s_{0c}}$$

$$\text{MixCol}_2 = c_{2.s_{2c}} \oplus c_{3.s_{1c}} \oplus c_{0.s_{0c}}$$

$$\text{MixCol}_3 = c_{3.s_{2c}} \oplus c_{0.s_{1c}} \oplus c_{1.s_{0c}}$$

25

*After the 4<sup>th</sup> cycle:*

$$\text{MixCol}_0 = c_{0.s_{3c}} \oplus c_{1.s_{2c}} \oplus c_{2.s_{1c}} \oplus c_{3.s_{0c}}$$

$$\text{MixCol}_1 = c_{1.s_{3c}} \oplus c_{2.s_{2c}} \oplus c_{3.s_{1c}} \oplus c_{0.s_{0c}}$$

$$\text{MixCol}_2 = c_{2.s_{3c}} \oplus c_{3.s_{2c}} \oplus c_{0.s_{1c}} \oplus c_{1.s_{0c}}$$

$$30 \quad \text{MixCol}_3 = c_{3.s_{3c}} \oplus c_{0.s_{2c}} \oplus c_{1.s_{1c}} \oplus c_{2.s_{0c}}$$

Rearranging these outputs, according to the feedback plan 90 ... 93 gives the outputs:

$$\begin{aligned} \text{MixCol}_1 &= s'_{0,c} \\ 5 \quad \text{MixCol}_2 &= s'_{1,c} \\ \text{MixCol}_3 &= s'_{2,c} \\ \text{MixCol}_0 &= s'_{0,c} \end{aligned}$$

which is the required result.

10

It will be noted that, generally speaking, the number of rows,  $m$ , in the matrix determines the number of cycles required, while the number of columns,  $n$ , determines the number of logic groups (multipliers 60 ... 63, XOR gates 70 ... 73, and registers 80 ... 83) required.

15 The multiplication logic 60 ... 63 can be implemented using any suitable logic. In a preferred embodiment, the logic is provided for both encryption and decryption combining certain logic according to the following schedule.

For  $c_0 \times s_{0,c}$ , there the output from the respective multiplication logic 60 ... 63 is defined as  $e_{\text{cycle, bit}}$ , and  $d = 0$  for encryption and  $d = 1$  for decryption:

20

$$\begin{aligned} e_{07} &= s_6 \text{ XNOR NAND}(d, s_{45}) \\ e_{06} &= s_5 \text{ XNOR NAND}(d, s_{347}) \\ e_{05} &= s_4 \text{ XNOR NAND}(d, s_{236}) \\ e_{04} &= s_{37} \text{ XNOR NAND}(d, s_{125}) \\ 25 \quad e_{03} &= s_{27} \text{ XNOR NAND}(d, s_{0157}) \\ e_{02} &= s_{17} \text{ XNOR NAND}(d, s_{0567}) \\ e_{01} &= s_0 \text{ XNOR NAND}(d, s_{67}) \\ e_{01} &= s_7 \text{ XNOR NAND}(d, s_{56}) \end{aligned}$$

30

Similarly, for  $c_1 \times s_{1,c}$ :

$$e_{17} = s_7 \text{ XNOR NAND}(d, s_4)$$

$$\begin{aligned}
e_{16} &= s_6 \text{ XNOR NAND}(d, s_{37}) \\
e_{15} &= s_5 \text{ XNOR NAND}(d, s_{267}) \\
e_{14} &= s_4 \text{ XNOR NAND}(d, s_{1567}) \\
e_{13} &= s_3 \text{ XNOR NAND}(d, s_{056}) \\
5 \quad e_{12} &= s_2 \text{ XNOR NAND}(d, s_{57}) \\
e_{11} &= s_1 \text{ XNOR NAND}(d, s_6) \\
e_{10} &= s_0 \text{ XNOR NAND}(d, s_5)
\end{aligned}$$

Similarly, for  $c_2 \times s_{2,c}$ :

$$\begin{aligned}
10 \quad e_{27} &= s_7 \text{ XNOR NAND}(d, s_{45}) \\
e_{26} &= s_6 \text{ XNOR NAND}(d, s_{347}) \\
e_{25} &= s_5 \text{ XNOR NAND}(d, s_{236}) \\
e_{24} &= s_4 \text{ XNOR NAND}(d, s_{125}) \\
15 \quad e_{23} &= s_3 \text{ XNOR NAND}(d, s_{015}) \\
e_{22} &= s_2 \text{ XNOR NAND}(d, s_{0567}) \\
e_{21} &= s_1 \text{ XNOR NAND}(d, s_{67}) \\
e_{20} &= s_0 \text{ XNOR NAND}(d, s_{56})
\end{aligned}$$

20 Similarly, for  $c_3 \times s_{3,c}$ :

$$\begin{aligned}
e_{37} &= s_{67} \text{ XNOR NAND}(d, s_4) \\
e_{36} &= s_{56} \text{ XNOR NAND}(d, s_{37}) \\
e_{35} &= s_{45} \text{ XNOR NAND}(d, s_{267}) \\
25 \quad e_{34} &= s_{347} \text{ XNOR NAND}(d, s_{1567}) \\
e_{33} &= s_{23} \text{ XOR } s_7 \text{ XNOR NAND}(d, s_{056}) \\
e_{32} &= s_{12} \text{ XOR } s_7 \text{ XNOR NAND}(d, s_{57}) \\
e_{31} &= s_{01} \text{ XNOR NAND}(d, s_6) \\
e_{30} &= s_{07} \text{ XNOR NAND}(d, s_5)
\end{aligned}$$

30

where:

- $a_{57} = a_5 \text{ XOR } a_7$   
 $a_{07} = a_0 \text{ XOR } a_7$   
 $a_{34} = a_3 \text{ XOR } a_4$   
 $a_{567} = a_7 \text{ XOR } a_{56}$   
5  $a_{125} = a_{12} \text{ XOR } a_5$   
 $a_{1567} = a_{17} \text{ XOR } a_{56}$   
 $a_{37} = a_3 \text{ XOR } a_7$   
 $a_{67} = a_6 \text{ XOR } a_7$   
 $a_{23} = a_2 \text{ XOR } a_3$   
10  $a_{056} = a_0 \text{ XOR } a_{56}$   
 $a_{267} = a_2 \text{ XOR } a_{67}$   
 $a_{27} = a_2 \text{ XOR } a_7$   
 $a_{56} = a_5 \text{ XOR } a_6$   
 $a_{12} = a_1 \text{ XOR } a_2$   
15  $a_{347} = a_{34} \text{ XOR } a_7$   
 $a_{0157} = a_{01} \text{ XOR } a_{57}$   
 $a_{17} = a_1 \text{ XOR } a_7$   
 $a_{45} = a_4 \text{ XOR } a_5$   
 $a_{01} = a_0 \text{ XOR } a_1$   
20  $a_{236} = a_{23} \text{ XOR } a_6$   
 $a_{0567} = a_{07} \text{ XOR } a_{56}$

This requires 23 XOR gates, 32 XNOR gates and 32 NAND gates.

- Other embodiments are intentionally within the scope of the  
25 accompanying claims.

## CLAIMS

1. A logic circuit for multiplication of an ( $m \times n$ ) matrix by a ( $1 \times n$ ) or by a ( $m \times 1$ ) matrix, where  $m$  is a number of rows and  $n$  is a number of  
5 columns, and wherein each successive row  $m$  of  $n$  elements is a predetermined row permutation of a preceding row, the circuit comprising:

$n$  multiplication circuits (60...63) each having an input and an output which returns the value of said input multiplied by a predetermined multiplicand;

10  $n$  logic circuits, (70...73) each for executing a predetermined logical combination of a first input and a second input to provide a logical output, the first input being coupled to the output of a corresponding one of the  $n$  multiplication circuits;

$n$  registers (80...83) for receiving said logical output;

15 feedback logic for routing the contents of each register to a selected one of the second inputs in accordance with a feedback plan that corresponds to the predetermined row permutation; and

control means for successively providing as input to each of the  $n$  multiplication circuits each element in the ( $1 \times n$ ) or ( $m \times 1$ ) matrix.

20

2. The logic circuit of claim 1 in which the feedback logic provides a feedback plan corresponding to said predetermined row permutation that is a row shift.

25 3. The logic circuit of claim 2 in which the row shift is a single element right shift.

4. The logic circuit of claim 1 in which the  $n$  logic circuits are each adapted to execute an XOR-combination of said first input and said second  
30 input.

5. The logic circuit of claim 1 in which each of the predetermined multiplicands corresponds to one of the elements in the AES Rijndael MixColumns transform function.

5 6. The logic circuit of claim 5 in which the number  $m = 4$ , the number  $n = 4$ , the multiplicand for the first multiplication circuit = 02, the multiplicand for the second multiplication circuit = 03, the multiplicand for the third multiplication circuit = 01, and the multiplicand for the fourth multiplication circuit = 01.

10

7. The logic circuit of claim 5 in which the number  $m = 4$ , the number  $n = 4$ , the multiplicand for the first multiplication circuit = 0E, the multiplicand for the second multiplication circuit = 0B, the multiplicand for the third multiplication circuit = 0D, and the multiplicand for the fourth multiplication  
15 circuit = 09.

8. The logic circuit of claim 6 or claim 7 in which the four multiplicands are switchable between the values in claim 6 and the values in claim 7.

20

9. The logic circuit of claim 1 in which the control means is adapted to successively provide as input to each of the  $n$  multiplication circuits each successive element in the  $(1 \times n)$  or  $(m \times 1)$  matrix over each of  $n$  or  $m$  cycles of operation respectively.

25

10. The logic circuit of claim 1 in which each of the  $n$  multiplication circuits, each of the  $n$  logic circuits, and each of the  $n$  registers are at least eight bits wide.

30

11. The logic circuit of claim 1 in which the control means further includes means for providing as output from said logic circuit the contents of the  $n$  registers after each  $n$ th cycle.

12. The logic circuit of claim 1 in which the control means further includes means for resetting each of the registers prior to the first calculation cycle.

5

13. The logic circuit of claim 1 in which each successive row  $m$  of  $n$  elements is a predetermined row permutation of the immediately preceding row.

10

14. An AES MixColumns transform circuit incorporating the logic circuit of any one of claims 1 to 13.

15

15. An AES encryption and/or decryption engine incorporating the logic circuit of any one of claims 1 to 13 for performing the MixColumns transform.

16. Apparatus substantially as described herein with reference to the accompanying drawings.



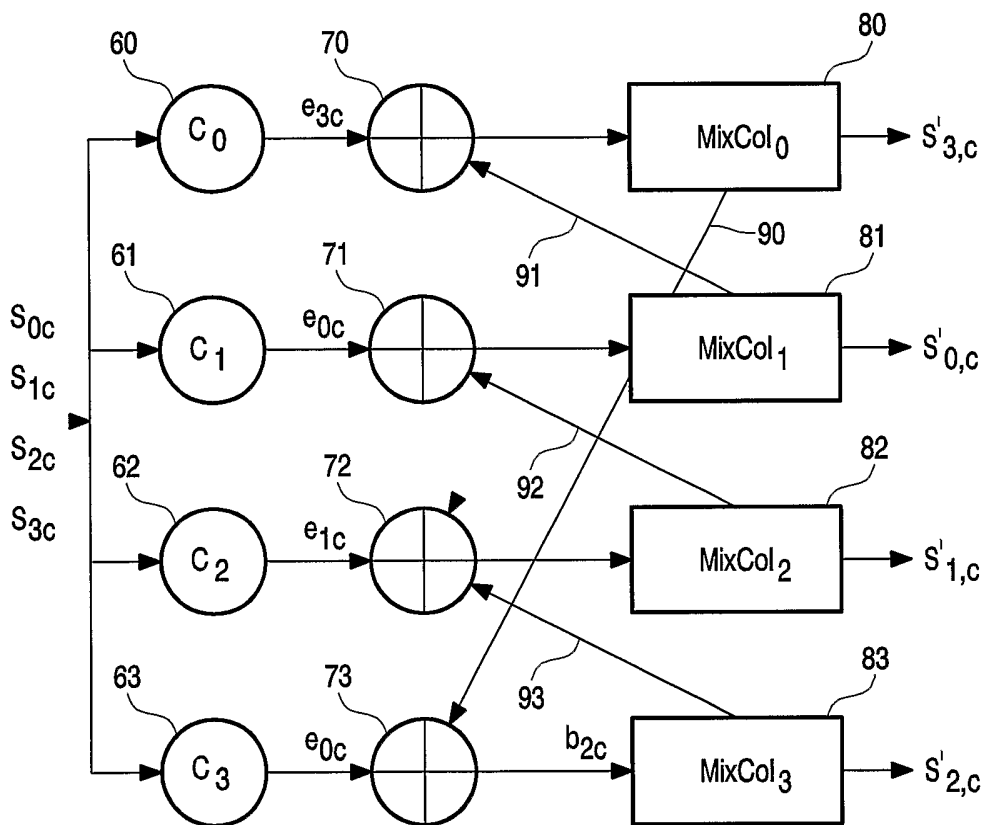


FIG.2

INTERNATIONAL SEARCH REPORT

International Application No  
PCT/IB 03/02583

<b>A. CLASSIFICATION OF SUBJECT MATTER</b> IPC 7 G06F7/72		
According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) IPC 7 G06F		
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, PAJ, WPI Data		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category <sup>a</sup>	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MCLOONE M ET AL: "High performance single-chip FPGA Rijndael algorithm implementations" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. 3RD INTERNATIONAL WORKSHOP, CHES 2001, PARIS, FRANCE, MAY 14 - 16, 2001 PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE, BERLIN: SPRINGER, DE, vol. 2162, 14 May 2001 (2001-05-14), pages 65-76, XP002203795 ISBN: 3-540-42521-7 page 70, line 8-12; figure 5 --- -/--	1-16
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C.		
<input type="checkbox"/> Patent family members are listed in annex.		
<sup>a</sup> Special categories of cited documents :		
*A* document defining the general state of the art which is not considered to be of particular relevance *E* earlier document but published on or after the international filing date *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) *O* document referring to an oral disclosure, use, exhibition or other means *P* document published prior to the international filing date but later than the priority date claimed *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. *&* document member of the same patent family		
Date of the actual completion of the international search 30 October 2003		Date of mailing of the international search report 06/11/2003
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 Prins, L

INTERNATIONAL SEARCH REPORT

International Application No.  
PCT/IB 03/02583

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>STALLINGS W: "THE ADVANCED ENCRYPTION STANDARD"                      CRYPTOLOGIA, UNITED STATES MILITARY ACADEMY, WEST POINT, NY, US,                      vol. 26, no. 3, July 2001 (2001-07), pages 165-188, XP001094868                      ISSN: 0161-1194                      page 175, line 9 -page 178, line 2                      -----</p>	1-16