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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 February 2008 (21.02.2008)

PCT

(10) International Publication Number
WO 2008/021145 A1

(51) International Patent Classification:
H04L 9/06 (2006.01) *H04L 9/18* (2006.01)

(21) International Application Number:
PCT/US2007/017650

(22) International Filing Date: 8 August 2007 (08.08.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/837,683 15 August 2006 (15.08.2006) US
11/540,790 29 September 2006 (29.09.2006) US

(71) Applicant *(for all designated States except US)*: **LUCENT TECHNOLOGIES INC.** [US/US]; 600 Mountain Avenue, Murray Hill, NJ 07974-0636 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **PATEL, Sarvar** [US/US]; 34 Millers Lane, Montville, NJ 07045 (US).

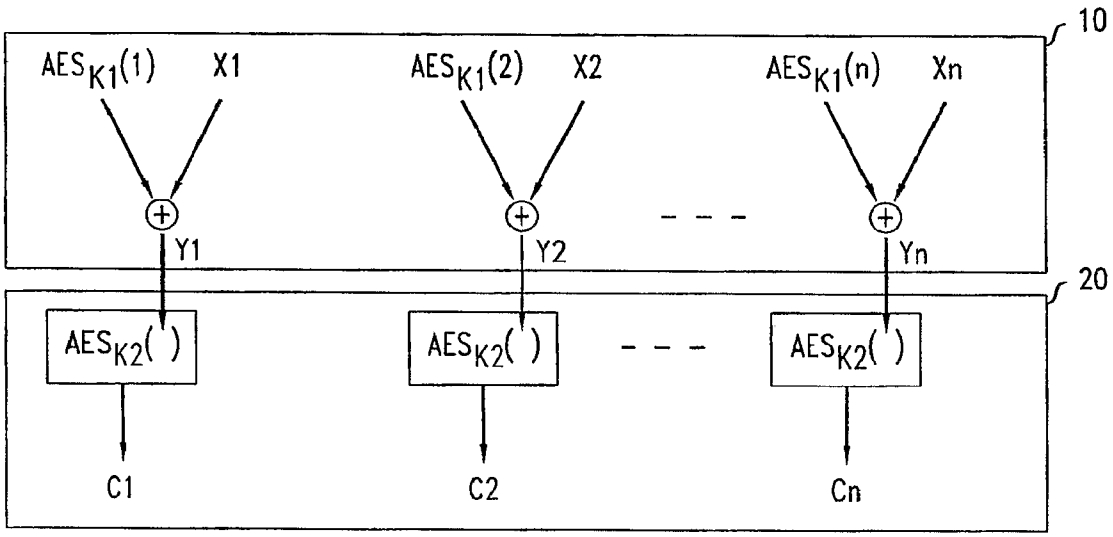
(74) Agent: **FINSTON, Martin, I.**; Lucent Technologies Inc., Docket Administrator - Room 2f-190, 600 Mountain Avenue, Murray Hill, NJ 07974 (US).

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

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

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

(54) **Title:** ENCRYPTION METHOD FOR MESSAGE AUTHENTICATION



(57) **Abstract:** In an encryption method, an input block of data is reversibly processed to produce a string that is at least partially randomized. The randomized string is then encrypted by a block cipher. In decryption, the input block of encrypted data is first decrypted with respect to the block cipher. Then the randomization is reversed.

WO 2008/021145 A1

ENCRYPTION METHOD FOR MESSAGE AUTHENTICATION

Cross Reference To Related Application

This application claims priority of Provisional Application Serial No. 60/837,683 which was filed August 15, 2006.

Field of the Invention

The invention relates to methods of secure encryption of messages.

Art Background

In many types of communication, there is a need to protect messages from tampering and unauthorized access. Encryption has long been used for such purposes. In advanced applications of encryption techniques, encryption keys are used not only to provide security for the encrypted messages, but also to protect the integrity of the messages. For example, a digital signature may be appended to a message prior to transmission, and a second version of the digital signature computed from the received message by the receiving party. If the two versions of the digital signature disagree, the receiving party will know that the integrity of the message was compromised by tampering.

To assure the integrity of a message, it is desirable to send the message, together with the appended digital signature, under the protection of a cipher that is non-malleable. The property of non-malleability assures that if even one bit of the encrypted message is changed as the result, e.g., of a malicious attack, the effects of the change will be distributed throughout the message upon decryption. Therefore, in particular, there will be a high probability that the digital signature is affected, and will fail to agree with the version locally computed by the receiving party.

One type of cipher used for encryption of messages is referred to as a block cipher. A block cipher takes blocks of binary data of fixed length as input strings, and produces blocks of binary data of fixed length as output strings. For example, Advanced Encryption Standard (AES) is a well-known block cipher that typically has input and output blocks of 128 bits.

One way to apply a block cipher such as AES is by Electronic Codebook (ECB) encryption. In ECB encryption, the message is divided into blocks of appropriate input length for the block cipher, and each block, in turn, is independently encrypted using the block cipher.

One weakness of ECB encryption is that it is susceptible to replay attacks. That is, an attacker may be looking for a recurrent string within the transmitted message. In ECB encryption, the recurrence of a plaintext string may lead to recurrence of the same encrypted string. In such a case, the recurrence may be recognized by the attacker.

Various attempts have been made to make encryption methods more robust against tampering, replay attacks, and other kinds of attack. One example of a more robust approach is described in U.S. Patent Serial No. 11/261,399, filed on October 28, 2005 by S. Patel et al. under the title, "Air-Interface Application Layer Security For Wireless Networks," and commonly assigned herewith. In that approach, a block cipher, for example, is used to generate a pair of pseudorandom strings A and B. The block X of plaintext is encrypted by forming the expression AX + B, where A and X are combined using polynomial multiplication. The combined use of the strings A and B provides non-malleability as well as robustness against reply attacks.

Although useful, such a polynomial encryption method is relatively costly because the multiplication operation for encryption and moreso its inverse for decryption are computationally intense.

Hence, there remains a need for robust encryption methods that are economical in their use of computational resources.

Summary of the Invention

We have found such a method. In a broad aspect, our method reversibly processes an input block of data to produce a string that is at least partially randomized. The randomized string is then encrypted by a block cipher. In decryption, the input block of encrypted data is first decrypted with respect to the block cipher. Then the randomization is reversed.

Brief Description of the Drawing

FIG. 1 is a flow diagram illustrating an encryption method according to the invention in one example embodiment.

FIG. 2 is a flow diagram illustrating a decryption method according to the invention in one example embodiment.

FIG. 3 is a flow diagram illustrating a method that may be used in a variation of the method of FIG. 1, for encrypting a partial string of input data.

FIG. 4 is a flow diagram illustrating a method that may be used in a variation of the method of FIG. 2, for decrypting a partial string of input data.

Detailed Description

The encryption method described here will have particular application for protecting the security and integrity of wireless transmissions of all kinds of content, including data traffic, voice traffic, and signaling data. Such transmissions may take place for example, and without limitation, between a wireless user terminal and a base station of the wireless network. However, the described method is not limited solely to wireless networks, but instead may also find suitable application in the domain of wireline communication. Likewise, it is appropriate for protecting communications between network entities of various kinds, including user terminals and network servers and switches.

In a particular example, a session key K is securely exchanged in advance between two parties to the protected communication. By well-known methods, the session key is used to generate two further keys K1 and K2. For example, K1 may be generated by the AES algorithm taking K as the input key and the integer 1, suitably padded with zeroes, as the argument: $K1 = AES_K(1)$. Similarly, we may have $K2 = AES_K(2)$. The key K1 is used with AES to generate pseudorandom strings of bits $AES_{K1}(1)$, $AES_{K1}(2)$, etc. By way of illustration, the arguments of AES for forming the pseudorandom strings may be the successive integers 1, 2, etc., suitably padded. However, any sequence of values may be used, as long as the same values are also known to the receiver for use in decryption.

With reference to FIG. 1, in a first encryption step 10, n blocks of input data X1, . . . , Xn are encrypted by AES according to: $Y1 = AES_{K1}(1) \oplus X1$, $Y2 = AES_{K1}(2) \oplus X2$,

. . . , $Yn = AES_{K1}(n) \oplus Xn$. In the preceding expressions, the symbol $\oplus$ signifies the logical exclusive or (XOR) operation. The result of these operations is to add at least partial randomization to the input blocks. The operations are reversible because a second XOR operation between each block and the corresponding pseudorandom string will restore the original input block.

If more economy but less security is desired, shorter pseudorandom strings can be used, and only a portion of each input block randomized in this fashion. Moreover, there are alternatives to block ciphers for generating the pseudorandom strings. For example, each of the pseudorandom strings described above may be a block from a long pseudorandom string generated by a stream cipher.

In a second encryption step 20, each of Y1, Y2, etc. is encrypted by AES, taking K2 as the input key, to produce a block of cipher text C1, C2, etc. That is, $C1 = AES_{K2}(Y1)$, $C2 = AES_{K2}(Y2)$, . . . , $Cn = AES_{K2}(Yn)$.

The decryption is the reverse of the above steps. For example, with reference to FIG. 2, C1 is decrypted in steps 30.1, 40.1 to X1′ by the following:

$Y1' = AES_{K2}^{-1}(C1)$

$X1' = AES_{K1}(1) \oplus Y1'$.

Similarly, steps 30.2, . . . , 30.n are applied to obtain Y2′, . . . , Yn′, from C2, . . . , Cn, and steps 40.2, . . . , 40.n are applied to obtain X2′, . . . , Xn′ from Y2′, . . . , Yn′.

Optionally, an efficient method can be used to encrypt and decrypt the last input block Xn in the event that it has fewer than the full block size of 128 bits. For purposes of illustration, we suppose that Xn has 64 bits. Then for encryption, with reference to FIG. 3, the XOR operation 50 is performed between Xn and the first 64 bits of $AES_{K1}(n)$. The resulting 64-bit string $\bar{Y}n$ is concatenated (step 60) with the last 64 bits of the preceding encrypted block C(n-1) to form a 128-bit string Zn. The resulting string is encrypted (step 70) in the normal way using $AES_{K2}(\bullet)$.

With reference to FIG. 4, for decrypting C(n-1) and Cn, the receiver first waits for the arrival and collection of the 192 bits consisting of: the first 64 bits of C(n-1), and the 128 bits of Cn resulting from the encryption 70 of the concatenation 60 of Xn (as randomized to form $\bar{Y}n$) with the last 64 bits of C(n-1). First, Cn, i.e., the last 128 bits

corresponding to the concatenated string are decrypted (step 80). Xn′ can then be recovered (step 90) from $\tilde{Y}n'$, i.e., from the last 64 of the decrypted bits. Then C(n-1) can be reassembled by concatenation (step 100) and decrypted to obtain X(n-1)′.

It should be noted that the methods described here may be carried out by a digital signal processor, a digital computer acting under the control of a software program, or other suitably conformed circuitry. After encryption, the message will be suitably conditioned and transmitted as a communication signal over an air interface or onto an optical or electronic transmission medium. Before decryption, the receiver will likewise receive the communication signal from the air interface or from the optical or electronic medium and will subject it to suitable conditioning.

Claims

What is claimed is:

1. A method, comprising obtaining at least one block of message data, at least partially randomizing the block of message data, encrypting the randomized block using a block cipher, and transmitting the encrypted block.

2. The method of claim 1, wherein the randomizing of the block of message data comprises providing a pseudorandom string, and performing an XOR operation between each of at least some bits of the block of message data and a respective bit of the pseudorandom string.

3. The method of claim 2, further comprising generating keys K1 and K2 from a session key, and wherein:

the pseudorandom string is provided by generating it from a cipher that takes K1 as an input key; and

the randomized block is encrypted using a block cipher that takes K2 as an input key.

4. A method, comprising receiving a transmitted signal and conditioning the received signal to obtain an encrypted message, decrypting at least one data block of the message from a block cipher, and derandomizing the decrypted block.

5. The method of claim 4, wherein the derandomizing of the block of message data comprises providing a pseudorandom string, and performing an XOR operation between each of at least some bits of the block of message data and a respective bit of the pseudorandom string.

6. The method of claim 5, further comprising generating keys K1 and K2 from a session key, and wherein:

the pseudorandom string is provided by generating it from a cipher that takes K1 as an input key; and

the received message block is decrypted using the inverse of a block cipher that takes K2 as an input key.

FIG. 1

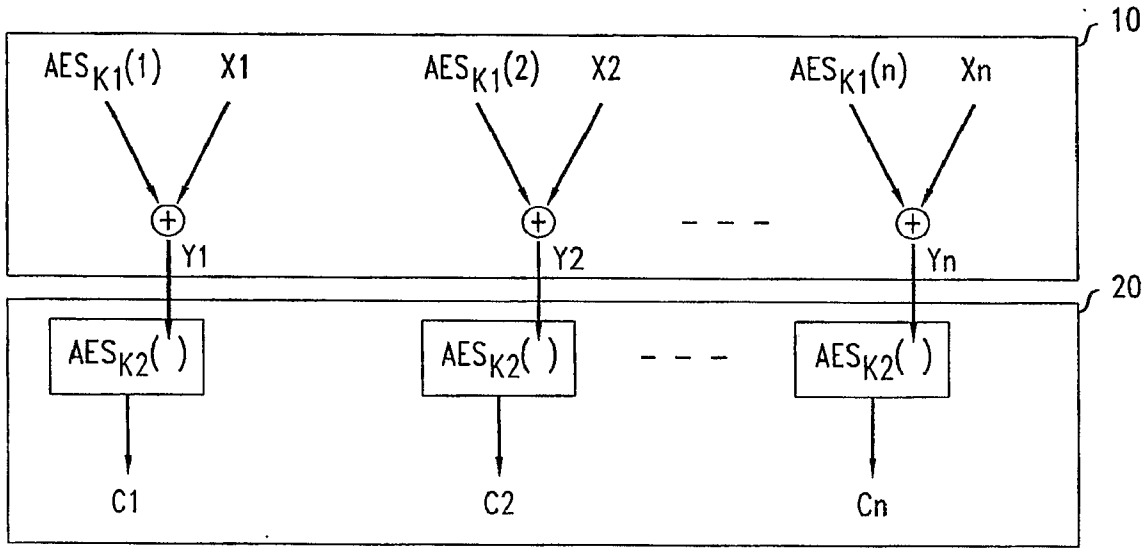

10
20
AES$_{K1}$(1)
X1
AES$_{K1}$(2)
X2
AES$_{K1}$(n)
Xn
Y1
Y2
Yn
AES$_{K2}$( )
AES$_{K2}$( )
AES$_{K2}$( )
C1
C2
Cn

FIG. 2

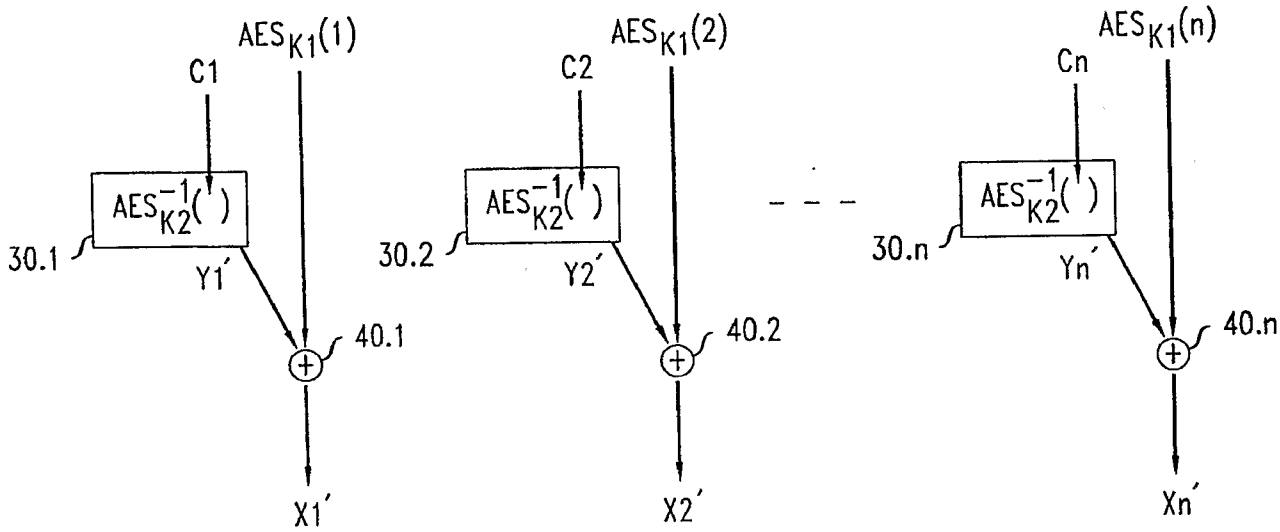

AES$_{K1}$(1)
C1
AES$^{-1}_{K2}$( )
30.1
Y1′
40.1
X1′
AES$_{K1}$(2)
C2
AES$^{-1}_{K2}$( )
30.2
Y2′
40.2
X2′
AES$_{K1}$(n)
Cn
AES$^{-1}_{K2}$( )
30.n
Yn′
40.n
Xn′

FIG. 3

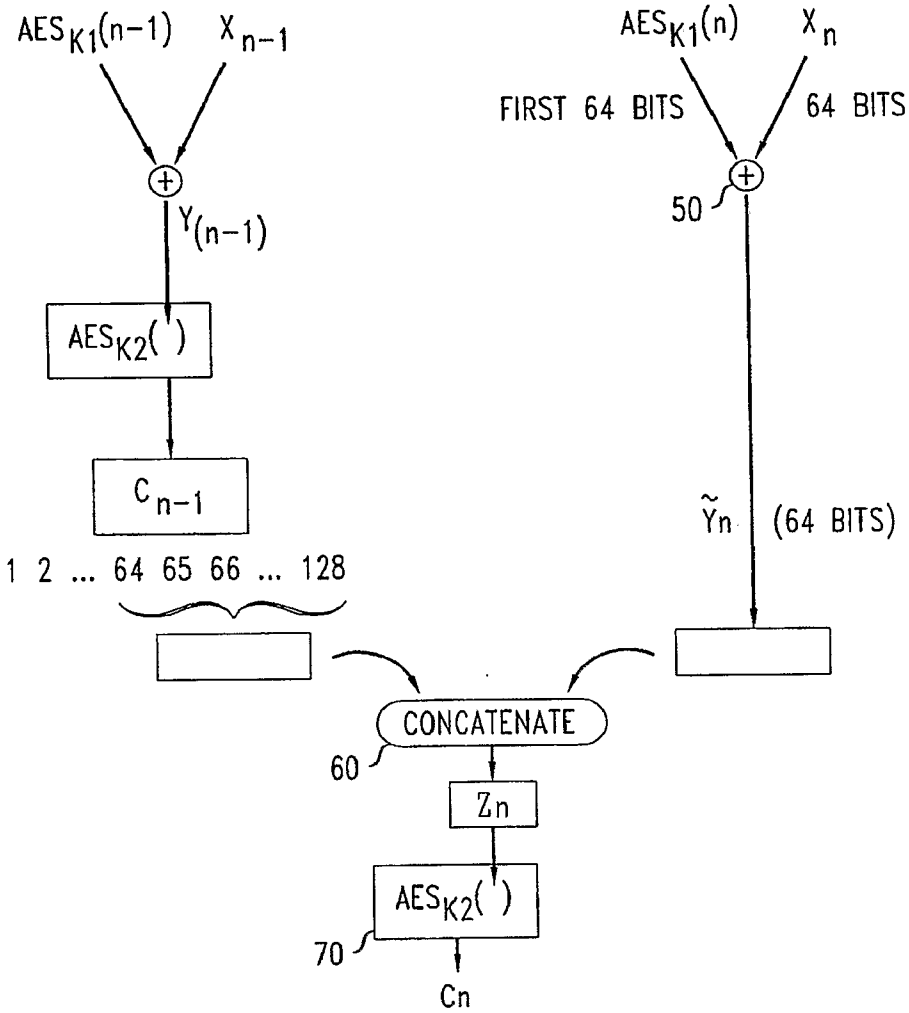
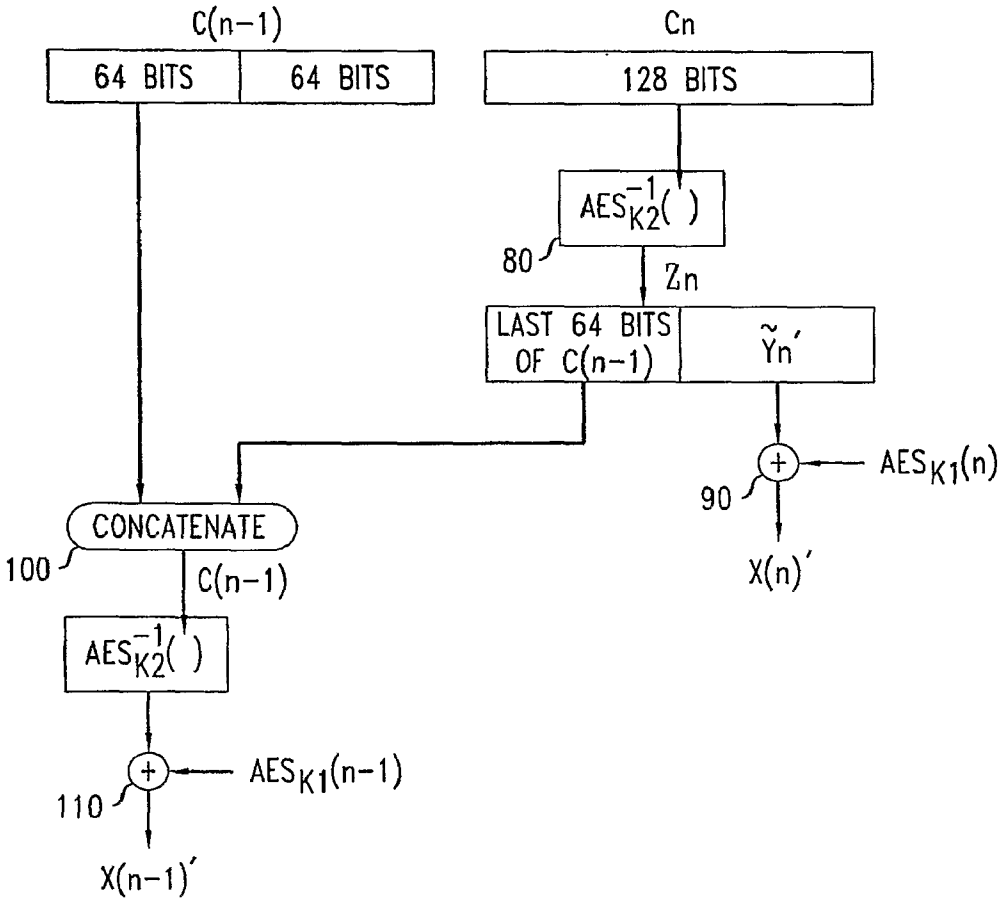

AES K1(n-1)
X n-1
Y(n-1)
AES K2( )
C n-1
1 2 ... 64 65 66 ... 128
AES K1(n)
X n
FIRST 64 BITS
64 BITS
50
Ỹn
(64 BITS)
CONCATENATE
60
Zn
AES K2( )
70
Cn

FIG. 4


C(n-1)
64 BITS
64 BITS
Cn
128 BITS
$AES_{K2}^{-1}(\ )$
80
Zn
LAST 64 BITS OF C(n-1)
$\tilde{Y}n'$
$AES_{K1}(n)$
90
X(n)'
CONCATENATE
100
C(n-1)
$AES_{K2}^{-1}(\ )$
$AES_{K1}(n-1)$
110
X(n-1)'

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/017650

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/06 H04L9/18

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)
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, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 077 554 A (FERRE HERRERO ANGEL JOSE [ES]) 21 February 2001 (2001-02-21) abstract paragraph [0030] - paragraph [0061] figures 2-7	1-6
X	BRUCE SCHNEIER ED - SCHNEIER B: "Applied Cryptography Second Edition" APPLIED CRYPTOGRAPHY. PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C, NEW YORK, JOHN WILEY & SONS, US, 1996, page 193-194, 200-201, XP002460342 ISBN: 0-471-11709-9 page 193, line 20 - last line ; figure 9.3 page 200, line 1 - page 201, line 4; figure 9.9	1-6

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

"E" earlier document but published on or after the international filing date

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 November 2007	12/12/2007

Name and mailing address of the ISA/	Authorized officer
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	Dujardin, Corinne

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/017650

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/169465 A1 (ITANI NORIKO [JP]) 4 August 2005 (2005-08-04) abstract paragraph [0065] - paragraph [0070] paragraph [0133] - paragraph [0140] figures 1,2,19,20	1,2,4,5
X	JP 2001 211166 A (MICRO TECHNOLOGY KK) 3 August 2001 (2001-08-03) abstract	1,2,4,5

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2007/017650

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1077554 A	21-02-2001	AT 282915 T	15-12-2004
		AU 3523799 A	23-11-1999
		DE 69921984 D1	23-12-2004
		WO 9957845 A1	11-11-1999
		US 7050580 B1	23-05-2006
US 2005169465 A1	04-08-2005	JP 2005217842 A	11-08-2005
JP 2001211166 A	03-08-2001	NONE	