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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 February 2013 (28.02.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/028056 A1

(51) International Patent Classification:
H04L 9/00 (2006.01) *H04L 9/06* (2006.01)

(21) International Application Number:
PCT/MY2012/000157

(22) International Filing Date:
28 June 2012 (28.06.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 2011003915 19 August 2011 (19.08.2011) MY

(71) Applicant *(for all designated States except US)*: **MIMOS BERHAD** [MY/MY]; Technology Park of Malaysia, Bukit Jalil, 57000 Kuala Lumpur (MY).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MOHAMED NOOR BEG, Ahmad Raif** [MY/MY]; Mimos Berhad, Technology Park of Malaysia, Bukit Jalil, 57000 Kuala Lumpur (MY). **TENGKU AZIZ, Raja Mohd Fuad** [MY/MY]; Mimos Berhad, Technology Park of Malaysia, Bukit Jalil, 57000 Kuala Lumpur (MY). **JUHARI, Mohammad Firdaus** [MY/MY]; Mimos Berhad, Technology Park of Malaysia, Bukit Jalil, 57000 Kuala Lumpur (MY).

(74) Agent: **MOHAN, K.**; Adastra Intellectual Property Sdn Bhd, A-28-10, Menara UOA Bangsar, No. 5, Jalan Bangsar Utama 1, 59000 Kuala Lumpur (MY).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, 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, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

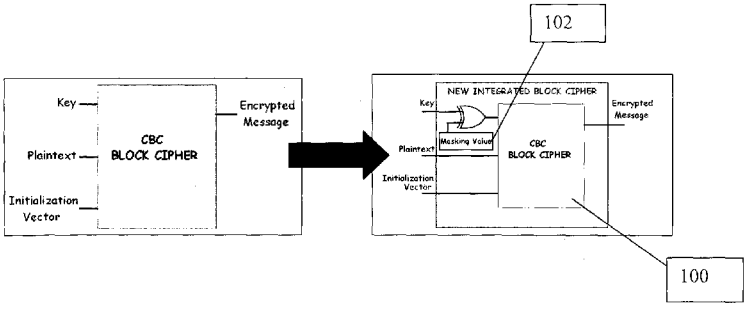
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

WO 2013/028056 A1

(54) Title: METHOD AND SYSTEM FOR PROVIDING A SECURED INTERNET PROTOCOL BASED COMMUNICATION



(57) Abstract: The present invention discloses a method and system for use in an IP based network, whereby a highly secured communication between two participating devices can be achieved. Instead of masking a key after encyrption to be shared between devices to establish communication, the present invention masks the original key at an earlier level, preferably at key input prior to using it for encryption and decryption. The key is masked using X-OR operation (102) integrated in the CBC block (100) thus generating a secondary key which is then used for encryption and decryption process.

METHOD AND SYSTEM FOR PROVIDING A SECURED INTERNET PROTOCOL BASED COMMUNICATION

FIELD OF THE INVENTION

Embodiments of the present invention are directed generally to a method and system for use in a network, and more particularly a method and system for use in providing a secured internet protocol based communication between at least two participating devices within a network.

BACKGROUND OF THE INVENTION

Managing a network signifies the need to gather network information that flows into and from a respective device, in order to efficiently monitor network traffic and detecting the problems which may arise on said network. Information gathered can be used to, among other variety of tasks, perform routine trouble- shooting tasks, such as locating a server that is down, or that is receiving a disproportionate number of work requests. Evidently, these tasks can only be carried out with the aid of effective network traffic monitoring.

One of the various quintessential tasks in network traffic monitoring is managing Internet Protocol security, whereby

the primary objective of this task is to ensure communications between devices over Internet Protocols (IP) network is effectively protected. Typically, across an IP based network, IP packets are transferred and received between devices or agents, subject to mutual authentication between said devices. Devoid of Internet security systems, these devices or agents may be exposed to perilous network attacks. At present, Internet protocol communications are being secured by a protocol suite known as the Internet Protocol security (IPsec).

During operation, IPsec generates authentication and cryptographic keys for secure establishment between participating devices within the network. Currently the widely used IPsec keys are known as static keys, in which they are used classically over a long period of time with respect to communication establishments within a network, in contrast with ephemeral keys. Although static keys play a significant role in ensuring safe and protected communication between devices, there are several disadvantages have been observed since its introduction to the industry.

Challenges or tribulations which are typically associated with the use of static keys include being vulnerable to attacks, as in many cases static keys are not random enough

thus allowing attackers to launch password guessing attacks; and replay protection are not feasible using static keys. Another vital disadvantage is that once key is leaked, the communication between two devices within a respective network will be substantially compromised. One primary factor of how these keys can be leaked lies in the administrator itself. Administrators are the ones who have knowledge on which encryption algorithm is used as well as the full length details of the encryption keys. Therefore, the keys can be leaked to eavesdroppers due to the administrator's negligence.

Recognizing the shortcomings of the existing static keys deployment within an IP based network, it is highly desirable to have a method and system that can resolve the glaring issues as discussed and thus prevent the communications between devices being compromised.

The present invention is a method and system that is a step ahead the prior art, whereby with the present invention, the static keys are masked prior to using it for encryption, thus even though the attacker or sniffer has knowledge of the encryption keys, they cannot use this key for decryption as data is encrypted using a masked version of the keys. Accordingly, the IP security intensity is greater and

therefore communication between devices within an IP based network will not be compromised.

Still other embodiments and advantages of the present invention will become readily apparent to those skilled in the art from the following detailed description, wherein embodiments of the invention are described by way of illustration.

SUMMARY OF THE INVENTION

In one embodiment, there is provided a method and system for static key masking, whereby one of the main steps is to mask the original key using X-OR operator.

In another embodiment of the present invention, at the implementation levels, the key masking block is provided as part of cipher block, thereby resulting to the secondary key and the key transformation process being invisible for the insiders or administrators.

In one embodiment, the method and system of the present invention includes utilities that are configured to manage the Security Association Database (SAD) and Security Policy Database (SPD).

In another embodiment, the method and system of the present invention includes using standard crypto libraries of linux's kernel 2.6x.

In one embodiment, there is disclosed a method for use in an Internet Protocol Security (IPsec) System in providing a secured Internet Protocol based communication between two devices within a network, said method comprising the steps of: performing an X-OR operation to mask an original key to be shared between two devices; and generating a secondary key based on said X-OR operation to be used in encryption and decryption; wherein the X-OR operation comprises the step of generating a secret value for use in generating the secondary key.

In another embodiment, there is disclosed a security system for use in an Internet Protocol (IP) based network, for providing a secured communication between two devices within a network, said system comprising: a CBC block cipher (100) integrated with an XOR block for XOR operation to generate a masked key based on an original key and a register (102) for generating secret values to be used in generating said masked key; a security association database (SAD); a security policy database (SPD); at least one device which is configured to manage said SAD and SPD; and a standard crypto library.

As will be realized in the following description, the invention is capable of other and different embodiments and its several details are capable of modifications in various respects, all without departing from the scope of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

Features of the invention will be apparent from the following description when read with reference to the accompanying drawings:

FIG 1 shows the overall view of the method and system of the present invention;

FIG 2 shows an example of a scenario, a communication between two devices, Alice and Bob devoid of any security system;

FIG 3 shows another example of a scenario, a communication between two devices, Alice and Bob, with the deployment of a conventional security system;

FIG 4 shows an example of SAD Database listing;

FIG 5 shows another example of a scenario, a communication between two devices, Alice and Bob, with Eve and an acquaintance of Alice which can be a potential key leaker;

FIG 6 shows the implementation of the present invention;

FIG 7 shows another view in the implementation of the present invention;

FIG 8 shows the a part of the present invention, whereby it is shown that the X-OR block is integrated at key input; and

FIG 9 shows another view in the implementation of the present invention.

DETAILED DESCRIPTION

In the following description, reference is made to the accompanying drawings where, by way of illustration, specific embodiments of the invention are shown. It is to be understood that other embodiments may be used as structural and other changes may be made without departing from the scope of the present invention. Also, the various embodiments and aspects from each of the various embodiments may be used in any suitable combinations. Accordingly, the drawings and detailed description are to be regarded as

illustrative in nature and not as restrictive.

FIG 1 shows the overall view of the method and system of the present invention, in accordance with a preferred embodiment. As shown in FIG 1, the system of the present invention includes a Security Association Database (SAD) module (60), an operating system (OS) (70), IPsec packet processor (80), a key masking block (102) and a block cipher (100) which is preferably in the form of CBC block-cipher. The method and system of the present invention provides the integration of key masking method block in the encryption hardware implementation, in one embodiment.

The principle of functionality of an IPsec system will now be described so as to elucidate the mechanism of the present invention.

In a basic tri-party communication, there is Alice, who wants to send a message to Bob, having Eve as an IP-packet sniffer or potential attacker. This situation is illustrated in FIG 2. In the first scenario, the communication between Alice and Bob is not secured or protected by any encryption system. Therefore, Eve has access to all information sent by Alice to Bob. In a second scenario, Alice connects with Bob through a secure channel, as shown in FIG 3. Therefore, all messages sent to Bob are encrypted using the same key that

they share. The "Shared Key" is usually in the form of SAD (Security Association Database) that is situated at both Alice and Bob. An example of the SAD is shown FIG 4. This time, Eve is not able to decrypt the message sent as she can only see rubbish messages flowing through the communication channel. In the next scenario which is illustrated in FIG 5, Nora is introduced whereby she is an acquaintance to Alice thus has the access to Alice's SAD. In the event that Eve has the encryption or has a similar decryptor as Bob's, Eve may be able to access all information sent to Bob if she has the encryption key. The feasibility to obtain such key will be higher if Nora leaks the key to Eve. Based on the situations or scenarios discussed above, it is evident that the communications between Alice and Bob are highly compromised due to the existence of Eve and the possibility of the key being leaked by Nora. This also shows that any insider can leak the key to Eve, and Eve can use this information together with a network analysis tool to decipher the encrypted messages in real time.

The method and system of the present invention will now be described, particularly on how it can resolve the security hole which may be created in various network communication instances, as described above.

In one embodiment, the present invention masks the keys at hardware level or the device level; preferably, said key is masked at the key input level. With the key being masked at this early, level, Alice and Bob will not have the knowledge of the mechanism of masking that device uses thus adding more security to the IPSEC implementation. Now referring to FIG 6, a simple X-OR operation is performed based onthe original key with a secret value. It is preferred that this secret value is at the same dimension as the original key.

Still referring to FIG 6, KMM by X-ORing is provided thus a key with a secret value is generated. This is a secondary key generated to be used in the encryption process. Further, the XOR function is embedded within the CBC block cipher (100) to ensure its invisibility towards any insider.

As seen in FIG 7 and FIG 8, in accordance with an embodiment of the present invention, there is provided a CBC block-cipher (100) structure with an addition of X-OR block at the key input. There is further provided a register which is configured to generate the secret value. The KTP inside the encryption system and method in accordance with the present invention is represented by an XOR operator and a register.

Now referring to FIG 9, in effect, the register generates a secret value which is used in the X-OR operation with key to

generate a second or masked key. The secondary key is then used in encryption and decryption, which may be based on various algorithms such as 128-bits AES, RSA and DES.

While the invention has been particularly shown and described with reference to the illustrated embodiments, those skilled in the art will understand that changes in form and detail may be made without departing from the scope of the invention.

CLAIMS

1. A method for use in an Internet Protocol Security (IPsec) System in providing a secured Internet Protocol based communication between two devices within a network, said method comprising the steps of:

performing an X-OR operation to mask an original key to be shared between two devices; and

generating a secondary key based on said X-OR operation to be used in encryption and decryption;

wherein the X-OR operation comprises the step of generating a secret value for use in generating the secondary key.

2. The method as claimed in Claim 1 wherein the secret value is at the same dimension as the original key.

3. The method as claimed in Claim 1 wherein the method further comprising the step of providing an XOR module or block at the key input of a CBC block cipher.

4. The method as claimed in Claim 3 wherein the method further comprising providing a register for generating secret values adjacent to the XOR block.

5. A security system for use in an Internet Protocol (IP) based network, for providing a secured communication between

two devices within a network, said system comprising:

a CBC block cipher (100) integrated with an XOR block for XOR operation to generate a masked key based on an original key and a register (102) for generating secret values to be used in generating said masked key;

a security association database (SAD) (60);

a security policy database (SPD);

at least one device which is configured to manage said SAD and SPD; and

a standard crypto library.

6. The security system as claimed in Claim 5 wherein the device installed with XOR comprises a CBC block-cipher and a register for generating secret values to generate the masked key.

7. The security system as claimed in Claim 5 wherein the masked key is a secondary key to be used in encryption and decryption so as to establish communication between the devices.

8. The security system as claimed in Claim 1 wherein the device installed with an XOR is configured to encrypt the key XORED with a constant value and with a predetermined bit length, preferably similar to the key bit length.

9. The security system as claimed in Claim 4 wherein the constant value is in the form of a register or memory module.

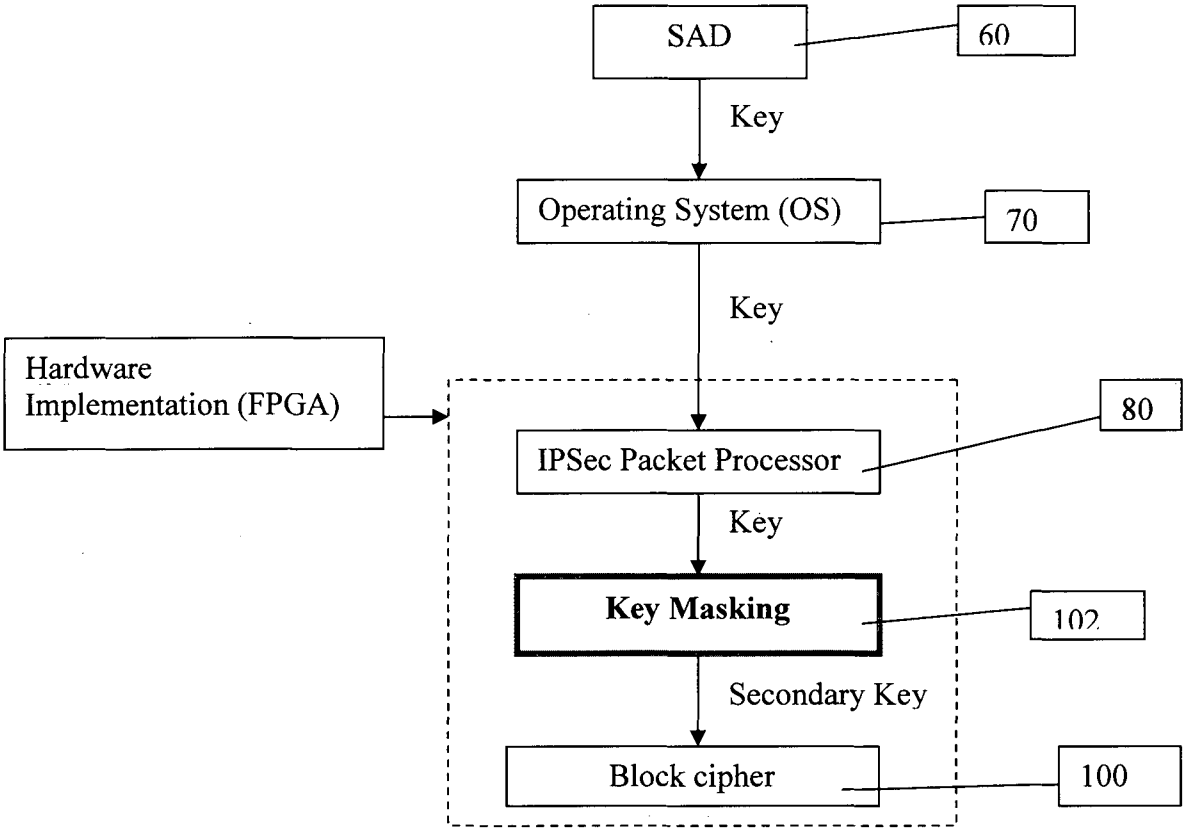

SAD
60
Key
Operating System (OS)
70
Key
Hardware Implementation (FPGA)
80
IPSec Packet Processor
Key
Key Masking
102
Secondary Key
Block cipher
100

FIG 1

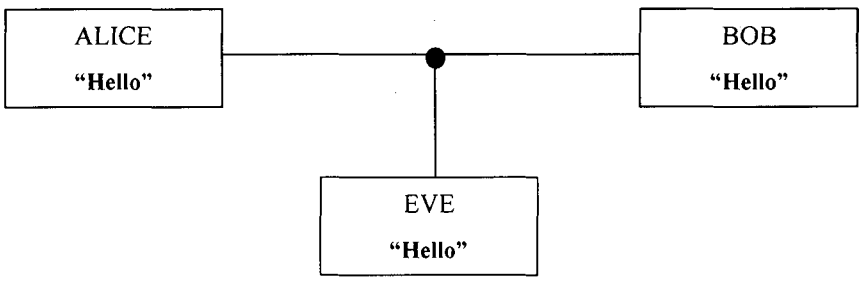

ALICE
"Hello"
BOB
"Hello"
EVE
"Hello"

FIG 2

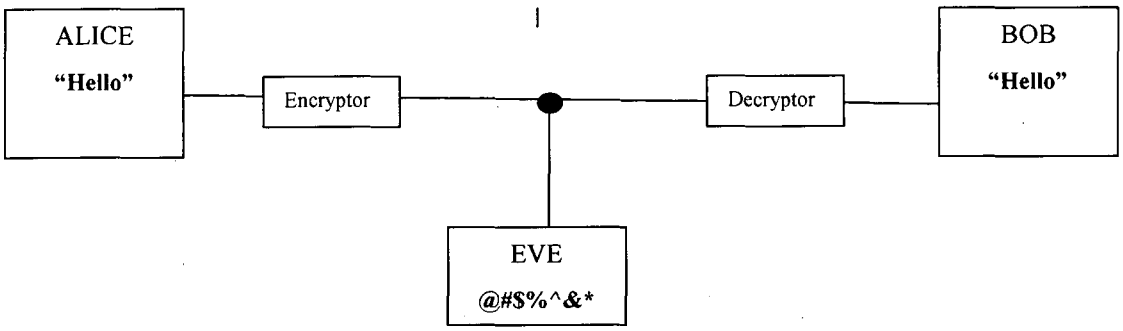


FIG 3

```
sbin/setkey -c <<-HERE
        flush;
        spdflush;

add $client $server esp 0x2000 -m tunnel
  -E rijndael-cbc  0x643C98696633487374B0DC5119495CFF
  -A hmac-sha1     0x2AE8944A625558EC238E1F2946E87CCD12345678;

add $server $client esp 0x2001 -m tunnel
  -E rijndael-cbc  0x3D1B58BA507ED7AB2EB141F241B71EFB
  -A hmac-sha1     0x79E2A9E37545E146515F007C5BD062C212345678;
dump;
HERE
```

FIG 4

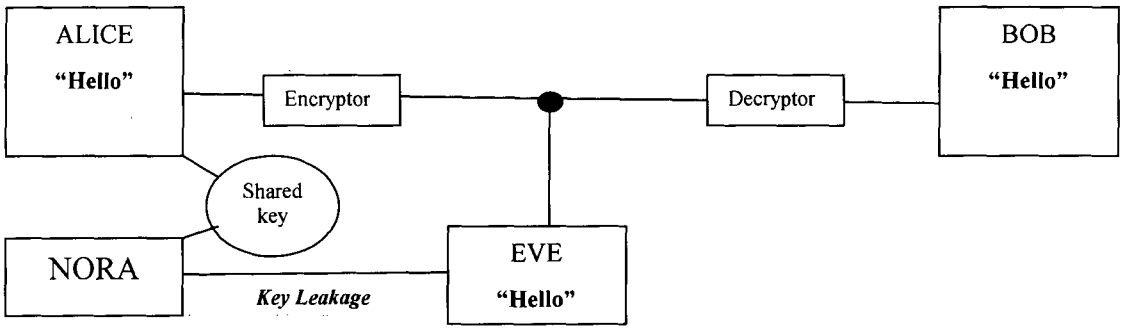


FIG 5

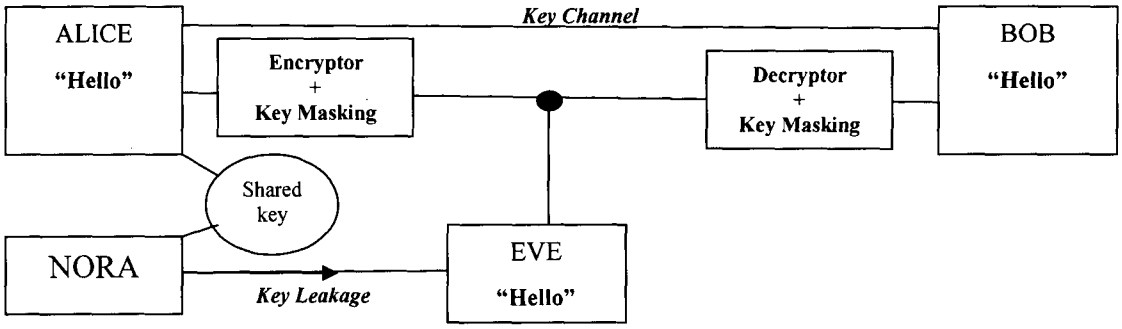


FIG 6

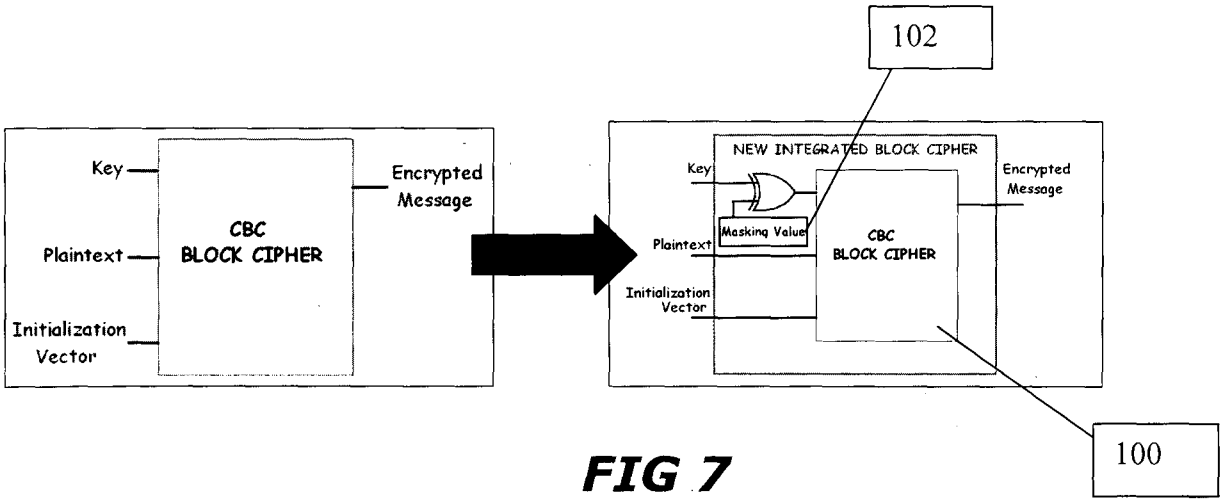


FIG 7

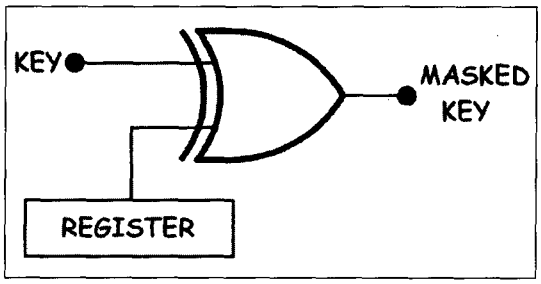

KEY
MASKED KEY
REGISTER

FIG 8

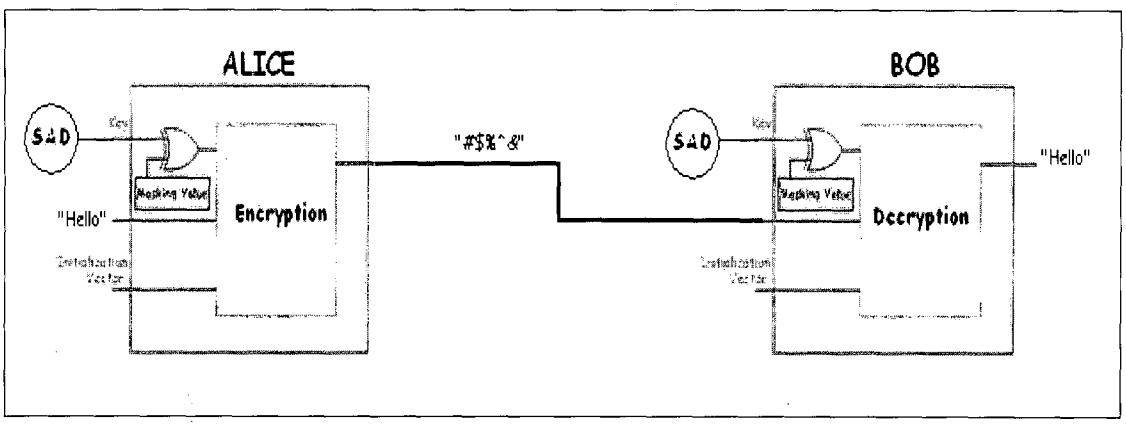

ALICE
BOB
SAD
Key
Masking Value
"Hello"
Encryption
"#$%^&"
SAD
Key
Masking Value
Decryption
"Hello"

FIG 9

INTERNATIONAL SEARCH REPORT

International application No
PCT/MY2012/000157

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/00 H04L9/06
ADD.

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 practicable, search terms used)
EPO-Internal, WPI Data, PAJ, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FR 2 893 796 A1 (ATMEL CORP [US]) 25 May 2007 (2007-05-25) page 13, line 22 - page 16, line 11 page 2 -----	1-9
X	EP 1 398 901 A1 (TOSHIBA KK [JP]) 17 March 2004 (2004-03-17) abstract figures 5-8 paragraph [0045] - paragraph [0050] -----	1-9
X	EP 1 267 514 A2 (FUJITSU LTD [JP]) 18 December 2002 (2002-12-18) figures 19,27,29 paragraph [0071] - paragraph [0131] -----	1-9
	-/--	

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

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 November 2012	10/12/2012

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, Fax: (+31-70) 340-3016	Bec, Thierry

INTERNATIONAL SEARCH REPORT

International application No
PCT/MY2012/000157

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 7 580 519 B1 (GOH JOON-KIT [SG]) 25 August 2009 (2009-08-25) abstract figures 1E,1F column 5, line 55 - column 10, line 58 column 28, line 30 - line 43 -----	1-9
A	KENNETH G PATERSON ET AL: "Cryptography in Theory and Practice: The Case of Encryption in IPsec", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20060424:152503, 24 April 2006 (2006-04-24), pages 1-23, XP061001581, [retrieved on 2006-04-24] the whole document -----	1-9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/MY2012/000157

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2893796 A1	25-05-2007	CN 101371480 A	18-02-2009
		EP 1955465 A2	13-08-2008
		FR 2893796 A1	25-05-2007
		JP 4990908 B2	01-08-2012
		JP 2009516964 A	23-04-2009
		KR 20080073345 A	08-08-2008
		US 2008019503 A1	24-01-2008
EP 1398901 A1	17-03-2004	DE 60302512 D1	05-01-2006
		DE 60302512 T2	22-06-2006
		EP 1398901 A1	17-03-2004
		JP 4357815 B2	04-11-2009
		JP 2004101981 A	02-04-2004
		US 2004091107 A1	13-05-2004
EP 1267514 A2	18-12-2002	DE 60222052 T2	21-05-2008
		EP 1267514 A2	18-12-2002
		EP 1772985 A1	11-04-2007
		JP 4596686 B2	08-12-2010
		JP 2002366029 A	20-12-2002
		US 2003048903 A1	13-03-2003
US 7580519 B1	25-08-2009	NONE	