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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 December 2013 (27.12.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/189619 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/EP2013/057260

(22) International Filing Date:
5 April 2013 (05.04.2013)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **NEC EUROPE LTD.** [DE/DE]; Kurfürsten-Anlage 36, 69115 Heidelberg (DE).

(72) Inventors: **GAJEK, Sebastian**; Schloss-Wolfsbrunnenweg 15/III, 69118 Heidelberg (DE). **SEEDORF, Jan**; Breslauer Straße 53, 69124 Heidelberg (DE). **DAGDELEN, Oezguer**; Rodensteinstraße 22, 64625 Bensheim (DE).

(74) Agent: **ULLRICH & NAUMANN**; Schneidmühlstr. 21, 69115 Heidelberg (DE).

(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, BN, 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, PA, 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))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

— *upon request of the applicant, before the expiration of the time limit referred to in Article 21(2)(a)*

(54) Title: METHOD AND SYSTEM FOR MODIFYING AN AUTHENTICATED AND/OR ENCRYPTED MESSAGE

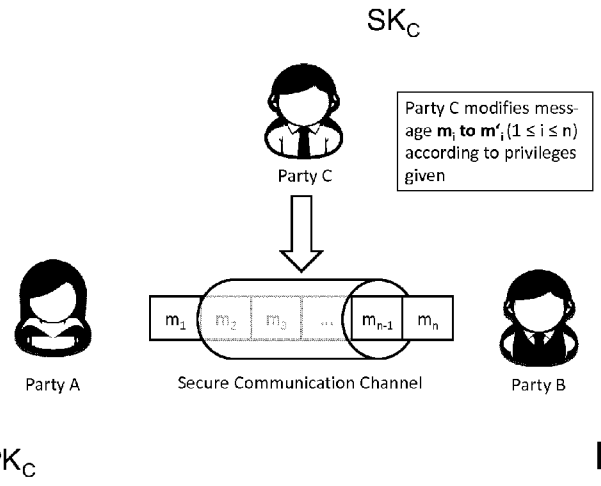


Fig. 1

(57) Abstract: The present invention relates to a method for modifying an authenticated and/or encrypted message by a modifying party exchanged between a sending party and a receiving party based on a secure communication protocol, comprising the steps of a) Dividing a clear message into non-modifiable parts and modifiable parts by the sending party, b) Including modifiable part information into the message by the sending party, c) Authenticating and/or encrypting the message by the sending party, d) Providing en- and decryptability and/or authenticability of the message to the modifying party in such a way that the modifying party can only modify the modifiable parts of the message, e) Modifying one or more modifiable parts by the modifying party, and f) Providing an authenticated and/or encrypted modified message according to the secure communication protocol to the receiving party. The present invention relates also to a system for modifying an encrypted message.

WO 2013/189619 A1

METHOD AND SYSTEM FOR MODIFYING AN AUTHENTICATED AND/OR ENCRYPTED MESSAGE

The present invention relates to a method for modifying an authenticated and/or encrypted message by a modifying party exchanged between a sending party and a receiving party based on a secure communication protocol.

The present invention relates also to a system for modifying an authenticated and/or encrypted message by a modifying party exchanged between a sending party and a receiving party based on a secure communication protocol.

Securing communication in distributed networks like the internet or mobile communication networks, e.g. 3G or LTE is a building block for a large number of applications. Conventional methods for securing communication are based for example on the SSL, IPSEC or SSH protocol. These protocols have been developed or designed decades ago when the underlying network topology was end-to-end oriented, meaning a client-to-server communication. A key requirement was to assess the confidentiality of the message and the message integrity. Any modification of messages was regarded as security breach.

One of the problems of using such protocols is, that they limit the flexibility of applications. Communication today is coupled more loosely. For example, in cloud-computing multiple parties interact with different services which are again distributed on different physical machines. For instance, the cloud provider contracts some web accelerator to embed a message template on the behalf of the cloud into the communication between a mobile device and the cloud provider. Usage of conventional security protocols does not allow the web accelerator to engage in the corresponding communication. To overcome this problem, service providers disseminate their secret key material, for example in form of long term keys, to intermediates.

However, this raises great security problems: Intermediates may easily impersonate the service provider and cause damage, for example by exploiting information of users of the service provider or the like. Since conventional secure

protocols are designed in such a way that minor modifications to a message yield to a message rejection, even minor changes are delicate and require much care.

In the non-patent literature of Agrawal and Boneh, Homomorphic MACs: MAC-Based Integrity for Network Coding, in: ACNS 2009, LNCS 5536, pp. 292-305 a homomorphic message authentication code for network coding is described. Intermediate nodes in the underlying network may combine authenticated messages while preserving authenticity. In the non-patent literature of Boneh and Freeman, in: PKC'11 linearly homomorphic signatures for small fields are described. Even further a generized method for obtaining homomorphic signatures from previous signature schemes are described. Even further the homomorphism was extended to polynomial function as described in Boneh and Freeman, Homomorphic Signatures for Polynomial Functions, in: EUROCRYPT'12. One of the drawbacks of the above mentioned methods is that these methods are only useful for asymmetric settings due to the use of digital signatures where a signer and a verifier have different key material. However, digital signatures are useless when modifying encrypted messages.

In the non-patent literature of Ahn, Boneh, Camenisch, Hohenberger, Shealt, Waters: Computing on Authenticated Data, in: TCC 2012:1-20 an orthogonal method for computing on encrypted data is described. Message tags are derived for a message being valid relative to a predicate over a previous set of messages. In the non-patent literature of Rosario Gennaro, Daniel Wichs: Fully Homomorphic Message Authenticators, IACR Cryptology ePrint Archive 2012: 290 (2012) fully homomorphic message authenticators are defined using an underlying primitive fully-homomorphic encryption mechanism. However, one of the drawbacks is, that one is limited to compute a polynomial function over the messages while preserving the validity of accumulated message tags.

It is therefore an objective of the present invention to provide a method for modifying an encrypted message without leading to a rejection of that message by a receiver when a message was modified in an allowable way.

It is a further objective of the present invention to provide a method and a system enabling a modifying party to be held back from modifying message parts which the modifying party is not allowed to modify.

It is a further objective of the present invention to provide a method and a system for modifying an encrypted message which can be easily implemented, preferably in conventional protocols and enable an enhanced flexibility for applications.

According to the invention the objectives are accomplished by a method of claim 1 and a system of claim 12.

According to claim 1 a method for modifying an authenticated and/or encrypted message by a modifying party exchanged between a sending party and a receiving party based on a secure communication protocol is defined.

According to claim 1 the method is characterized by

a) Dividing a clear message into non-modifiable parts and modifiable parts by the sending party,
b) Including modifiable part information into the message by the sending party,
c) Authenticating and/or encrypting the message by the sending party,
d) Providing en- and decryptability and/or authenticability of the message to the modifying party in such a way that the modifying party can only modify the modifiable parts of the message,
e) Modifying one or more modifiable parts by the modifying party and
f) Providing an authenticated and/or encrypted modified messagoe according to the secure communication protocol to the receiving party.

According to claim 12 a system for modifying an authenticated and/or encrypted message by a modifying party exchanged between a sending party and a receiving party based on a secure communication protocol, preferably for performing with a method according to one of the claims 1-11, is defined.

According to claim 12 the system is characterized in that the sending party is operable to divide a clear message into non-modifiable parts and modifiable parts,

to include modifiable part information into the message, and to authenticate and/or to encrypt the message by the sending party, that the modifying party is operable to be provided with en- and decryptability and/or authenticability of the message in such a way that the modifying party can only modify the modifiable parts of the message, and to modify one or more modifiable parts by the modifying party and that the receiving party is operable to receive the authenticated and/or encrypted modified message according to the secure communication protocol and preferably is operable to check security integrity according to the secure communication protocol of a received message.

According to the invention it has been recognized that the method and the system according to the invention can easily be integrated in existing flagship protocols, such as TLS.

According to the invention it has further been recognized that a modifying party is prevented from modifying message parts for which the modifying party does not have the permission to change them.

According to the invention it has further been recognized that by including modifiable part information into the message, the modifying party can identify modifiable parts of the message and the modifying party is held back from changing for example order and content of the non-modifiable and modifiable parts of the message.

According to the invention it has been further recognized that providing authenticability or authenticity and/or en- and decryptability of the message to the modifying party in such a way that the modifying party can only modify the modifiable parts of the message, the modifying party is provided with a so-called trapdoor to delete and/or modify predetermined portions or parts of the encrypted and/or authenticated message. Therefore it has further been recognized that the present invention is inherently non-homomorphic.

Further features, advantages and preferred embodiments are described in the following subclaims.

According to a preferred embodiment a key tuple for encrypting/decrypting the message according to the secure communication protocol and a sanitizing key tuple for modifying the modifiable parts are generated. This enables an easy way to provide en- and decryptability of the message to the modifying party since for example the modifying party can use the sanitizing key tuple for changing parts of the message for further processing.

According to a further preferred embodiment the clear message is divided into a message header and a message payload and the modifiable part information is encoded into the message header. This enables an easy implementation of modifiable part information into a message and enables separating message content and message related information.

According to a further preferred embodiment the clear message is encrypted with the encryption key according to the secure communication protocol in a first message part and the message identification information is authenticated with the sanitizing key tuple in a second message part in step c). A modifying party is for example then given a session key of the secure communication protocol for decrypting the encrypted message with the message identification information.

According to a further preferred embodiment for modifying, both message parts are decrypted wherein the modifiable parts are identified based on the decrypted modifiable part information. The modifying party can then extract the message parts which are subjected to modification in an easy and efficient way.

According to a further preferred embodiment a hash value is generated for indicating security integrity of a message prior to modification and for step f) a hash function is used providing a value identical to the generated hash value for the modified message. This enables in a very efficient way so that the receiving party may easily check the security integrity of the message according to the message authentication code.

According to a further preferred embodiment the hash function is a chameleon hash function. By using a chameleon hash function hash collisions may be computed with the function, i.e. the modifying party may compute identical hash values for messages of his choice. For example, given a secret key the chameleon hash function may generate randomness for a different message so that the hash value is identical.

According to a further preferred embodiment a message tag is generated based at least on a sanitizing key tuple, the key tuple and the modifiable part information. This allows a message to be tagged with the necessary information for encrypting, decrypting and verifying message security.

According to a further preferred embodiment steps a) – c) include the substeps of

g1) choosing a random number for each modifiable part,

g2) generating a message header including the random numbers and modifiable part information,

g3) generating a message tag,

g4) encrypting and authenticating the message with the encryption key into a first part,

g5) encrypting a secure communication protocol session key and a message ID represented by the hash value for the message header with the sanitizable key tuple into a second part, and

g6) combining, preferably by concatenating, the first and second part.

This enables an easy implementation of the steps a), b) as well as c) and an efficient processing of these steps.

According to a further preferred embodiment steps d) and e) include the substeps of

h1) decrypting the second part,

h2) decrypting the first part based on the decrypted second part,

h3) identifying the modifiable parts,

h4) modifying one or more modifiable parts,

h5) encrypting the modified message with key tuple.

This enables in an easy and efficient way a modifying party to modify the message according to privileges given to the modifying party and preserving security integrity of the message for a receiving party.

According to a further preferred embodiment security integrity of the modifying message is checked by recomputing the hash values of the modifiable and non-modifiable parts of the modified message, by generating a new message tag from the recomputed hash values and by comparing the new message tag with the message tag of the original message. This provides a fast and efficient checking of the security integrity of the message.

There are several ways how to design and further develop the teaching of the present invention in an advantageous way. To this end it is to be referred to the patent claims subordinate to patent claim 1 on the one hand and to the following explanation of preferred embodiments of the invention by way of example, illustrated by the figure on the other hand. In connection with the explanation of the preferred embodiments of the invention by the aid of the figure, generally preferred embodiments and further developments of the teaching will be explained. In the drawings

Fig. 1 shows schematically a method according to a first embodiment of the present invention;

Fig. 2 shows a flow diagram of a method according to a second embodiment of the present invention;

Fig. 3 shows a flow diagram of a part of a method according to a third embodiment of the present invention;

Fig. 4 shows a flow diagram of a part of a method according to a fourth embodiment of the present invention;

Fig. 5 shows a flow diagram of a part of a method according to a fifth embodiment of the present invention;

Fig. 6a shows a flow diagram of a part of a method according to a sixth embodiment of the present invention;

Fig. 6b shows a flow diagram of a part of a method according to a seventh embodiment of the present invention; and

Fig. 7 shows a flow diagram of a part of a method according to an eighth embodiment of the present invention.

Fig. 1 shows schematically a method according to a first embodiment of the present invention.

In Fig. 1 an interceptable secure communication allowing a delegated party C to have control access to a confidential and authenticated message is shown. Two parties A and B establish a secure communication and a third party C wishes to alter a message $m = m_1 | \ldots | m_n$. The sending party A knows the public encryption key PK_S of the modifying party C for which the modifying party C holds the corresponding secret key SK_S. The modifying party C modifies part of the message denoted with m_i to m'_i with $1 \leqq i \leqq n$ according to the privileges given to the modifying party C. The party A sends the message m to party B and delegates party C to modify blocks of the message according to a predetermined set ID comprising indexes i of message parts m_i to be modified.

Before describing encryption modifying and decryption in detail with regard to Fig. 3 – Fig. 5 based on Fig. 1, the principle message authentication scheme is described in Fig. 2.

In a first step 21 a sanitizable key generation generation algorithm sKeyGen on input a security parameter n outputs a secret key SK and a sanitization key tuple (PK_{san}, SK_{san}).

In a second step 22 a tagging algorithm sMAC on input a secret key SK, a sanitizing public key PK_{san}, a message m, randomness r, and an index set ID, outputs a tag t.

In a third step 23 a verification algorithm sVrfy on input a secret key SK, a sanitizing public key PK_{san}, a message m, tag t, the set of modified blocks ID with its corresponding randomness r, outputs true if the tag t is a valid tag of message m for secret key SK; otherwise it outputs false.

And in a fourth step 24 a sanitizing algorithm Sanit on input a message m authenticated by tag t, and randomness r, secret key SKsan, and a message m', outputs randomness r' such that the verification algorithm sVrfy(SK, PK_{san}, m', ID, r', t)=true.

Summarizing the steps 21-24 the message is splitted into blocks or parts and all message blocks are hashed prone to interference through a chameleon hash function and all message blocks are authenticated afterwards via a standard message authentication scheme MAC. Using a chameleon hash function allows with the use of modifiable part information to compute collusions, i.e. compute a hash for a modified message. Due to the identical hash value the message authentication scheme, MAC check of the message blocks even when modified is positive, i.e. the message has security integrity according to the MAC.

Fig. 3 shows a flow diagram of a part of a method according to a third embodiment of the present invention.

In a first step 31 party A or party B generates a sanitizing key tuple PK_{san}, SK_{san} and bootstraps modifying party C with SK_{san}, for example by using out-of-band communication.

In a second step 32 party A and party B run a key exchange protocol and as a result both parties A and B derive an encryption and authentication key K_{enc} and K_{mac} respectively.

In the following is assumed a uni-directional communication and further that the message m encodes a sequence number.

When party A sends now a message m to party B and wishes that modifying party C interferes the message blocks in ID, then party A secures the message m in a second step 32 by choosing a random number r_i for blocks $i \in ID$. Then in a third step 33 a message tag t over $m = m_1|...|m_n$ using randomness $r = r_1|...|r_n$ where $t = sMAC(SK, PK_{san}, m, r, ID)$ is generated.

In a fourth step 34 a message header $h=<r_i,i>$ with $i \in ID$ containing randomness r and pointers i of modifiable message blocks m_i is computed.

In a fifth step 35 and in a sixth step 36 header h and payload $m_1|m_2|...|m_n$ is encrypted and authenticated, i.e. $C_1 = Enc(K_{enc}, h|m|t)$.

In a seventh step 37 the session key K_{enc} and the message id $m_{id}=hash(h)$ being the hash over the header, i.e. $C_2 = Enc(PK_S, m_{id}|K_{enc})$ is encrypted with a sanitizer's public key PK_S. m_{id} aids the modifying party C to verify that K_{enc} is the right key to properly decrypt the message header h and message payload C_1.

In an eighth step 38 $C =(C_1|C_2)$ is outputted. If C is not the initial ciphertext, then C_2 may be left out.

Fig. 4 shows a flow diagram of a part of a method according to a fourth embodiment of the present invention.

In Fig. 4 a flow diagram is shown when the modifying party C receives a message for modification. In a first step 41 upon receiving a message $C=(C_1|C_2)$, the modifying party C decrypts message id and session key $(m_{id}|K_{enc}) = Dec(SK_s, C_2)$.

In a second step 42 the modifying party C decrypts C_1 with the session key K_{enc} and obtains $(h|m|t)=Dec(K_{enc}, C_1)$.

In a third step 43 the modifying party C checks that the message m_{id}=hash(h). If not, it aborts.

In a fourth step 44 the modifying party C parses h=<r_i,i> with i ∈ ID and identifies all i's as the block messages subjected to modification. This way, the modifying party C learns ID.

In a fifth step 45 the modifying party C recomputes randomness r_i' in order to replace message m_i with m_i' by invoking

$$r_i' = CAdapt(PK_{san}, SK_{san}, m_i, r_i, m_i').$$

In a sixth step 46 the modifying party C replaces the original header h with the new header with new randomness h'=<r_i',i> .

In a seventh step 47 the modifying party C encrypts the modified header h' and payload $C_1' = Enc(K_{enc}, h'|m|t)$ and sends C_1' to the party B for further processing.

Fig. 5 shows a flow diagram of a part of a method according to a fifth embodiment of the present invention.

In Fig. 5 is shown a flow diagram when the receiving party B receives an encrypted modified message.

In a first step 51 upon receiving the message C_1', the receiving party B decrypts with its sessions key K_{enc} the ciphertext.

In a second step 52 $(h'|m'|t') = Dec(K_{enc}, C_1')$ is obtained.

In a third step 53 the necessary parameters, namely randomness r and blocks i ∈ ID are extracted from the header h' = < r'$_i$, i > to check the validity of the message tag t.

In a fourth step 54 the receiving party B runs the verification alogrithm sVrfy(SK, m', t', PK_{san}, ID, r') and accepts m', if t' is a valid tag. Otherwise, in a fifth step 55 the message m' is rejected by the receiving party B.

Fig. 6a shows a flow diagram of a part of a method according to a sixth embodiment of the present invention.

In Fig. 6a steps for providing a chameleon hash function are schematically shown.

In a first step 61a a key generation algorithm CHKeyGen on input a security parameter n outputs a key pair (PK_{san}, SK_{san}).

In a second step 62a the hashing algorithm CHash takes as input the public key PK_{san}, a message m, and randomness r and outputs a hash value h=CHash(PK_{san}, m, r).

In a third step 63a a collision-finding algorithm CHAdapt on input a public key $PK_{san,}$, a secret key SK_{san}, messages m, m' and randomness r, outputs randomness r' such that

$$CHash(PK_{san}, m, r) = CHash(PK_{san}, m', r').$$

To summarize provided the secret key SK_{san} and the input parameters to the chameleon hash function, a randomness for a different message m' is generated such that the hash values of the different message m' and the original message m are identical.

Fig. 6b shows a flow diagram of a part of a method according to a seventh embodiment of the present invention.

In Fig. 6b a collision resistant hash function and a standard message authentication code consisting of three steps 61b – 63b is shown.

In a first step 61b a key generation algorithm KeyGen on input a security parameter n outputs a secret key SK.

In a second step 62b the tagging algorithm Mac on input the secret key SK, a message m, outputs a tag t and in a third step 63b the verification algorithm Vrfy on input the secret key SK, the message m and tag t, checks that t is a valid tag of message m for secret key SK. If so, it outputs 1 else 0 is outputted.

Fig. 7 shows a flow diagram of a part of a method according to an eighth embodiment of the present invention.

In Fig. 7 a sanitizable message authentication code method is shown. It is assumed that the message m consists of n data chunks $m = m_1|m_2|\ldots|m_n$. The following steps enable a modifying party holding the trapdoor key SK_{san} to replace a batch m_i with m'_i for any $i \in ID$:

In a first step 71 the key generation algorithm sKeyGen on security parameter n invokes CHKeyGen(n) to obtain a sanitizing key tuple (PK_{san}, SK_{san}).

In a second step 72 KeyGen(n) computes a secret key SK for the standard MAC scheme.

In a third step 73 for every message m_i for $i \in ID$ a chameleon hash is computed $h_i = CHash(PK_{san}, m_i, r_i)$ and for any non-modifying message block $i \notin ID$ a standard hash $h_i = Hash(m_i)$ is computed in a fourth step 74.

In a fifth step 75 a tag t is computed according to a tagging algorithm MAC: $t=Mac(SK, h_1|\ldots|h_n)$ for all $1 \leq i \leq n$ and in a sixth step 76 the tag t is outputted.

In a seventh step 77 a verification method takes as input the secret key SK, the message m, the tag t, the sanitizing public key PK_{san}, the set of modified blocks ID and the randomness r of the modified blocks.

In an eighth step 78 the validity of the message tag t is verified by recomputing the hash values h_i of the message blocks: In case of a modification the verification method uses the chameleon hash function on messages in ID with randomness r_i otherwise the standard hash algorithm is used.

In a ninth step 79 the tag t is accepted if it equals the original tag generated by the tagging algorithm MAC(SK, h_1|…|h_n). In a tenth step 80 the message is rejected otherwise.

In a further step 81 following step 79 the sanitizing algorithm Sanit on input a sanitizing public key PK_{san}, a message m, and randomness r, secret key SK_{san} and a new message m', invokes an adapting/modifying algorithm CAdapt(PK_{san}, SK_{san}, m, m', r) to obtain r', i.e. the randomness for modified message (block) m'.

In summary the present invention allows to alter messages in transit between two parties communicating via a secure communication protocol by designating privileges to a modifying party for modifying the message. Further the present invention provides a concrete header/payload format for efficient usage of chameleon hashes in data communications and enables efficient interceptable communication and deployment of the header/payload format in practice.

With the present invention control to modify authenticated messages is delegated without the capability of impersonation: A sender may define online what message chunks intermediates may alter. Further the present invention provides invisibility to a receiver: a receiver is not able to distinguish an unmodified message from an admissibly modified message ensuring that the receiver may properly decode encrypted messages. A further advantage of the present invention is that arbitrary implementation of chameleon hashes and message authentication schemes are used in order to overcome performance penalties or interoperability problems. Even further the present invention may be easily integrated in existing flagship protocols such as TLS via the addition of a new cipher specification. The present invention is inherently non-honomorphic providing an efficient secure channel protocol for secure communication. Even further the present invention enhances

flexibility, since a sender may delegate privileges to modify messages when sending the messaging and by incorporation of this information into the message.

Many modifications and other embodiments of the invention set forth herein will come to mind the one skilled in the art to which the invention pertains having the benefit of the teachings presented in the foregoing description and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

Claims

1. A method for modifying an authenticated and/or encrypted message (m) by a modifying party (C) exchanged between a sending party (A) and a receiving party (B) based on a secure communication protocol, characterized by
   a) Dividing a clear message (m) into non-modifiable parts (m_1, m_2, ...) and modifiable parts (m'_1, m'_2, ...) by the sending party (A),
   b) Including modifiable part information (i) into the message (m) by the sending party,
   c) Authenticating and/or encrypting the message (m) by the sending party (A),
   d) Providing en- and decrypticability and/or authenticability of the message (m) to the modifying party (C) in such a way that the modifying party (C) can only modify the modifiable parts (i) of the message (m),
   e) Modifying one or more modifiable parts (m'_i) by the modifying party (C), and
   f) Providing an authenticated and/or encrypted modified message (m') according to the secure communication protocol to the receiving party (B).

2. The method of claim 1, characterized in that a key tuple (K_{enc}, K_{mac}) for encrypting/decrypting the message (m) according to the secure communication protocol and a sanitizing key tuple (PK_{san}, SK_{san}) for modifying the modifiable parts (i) are generated.

3. The method according to one of the claims 1-2, characterized in that the clear message (m) is divided into a message header (h) and a message payload (m_1, m_2, ...) and that the modifiable part information (i) is encoded into the message header (h).

4. The method according to one of the claims 1-3, characterized in that the clear message is encrypted with the encryption key according to the secure communication protocol in a first message part (C), that the message identification information is authenticated with the sanitizing key tuple (PK_{san}, SK_{san}) in a second message part (C_2) in step c).

5. The method according to one of the claims 1-4, characterized in that for modifying, both messages parts (C_1, C_2) are decrypted, wherein the modifiable parts are identified based on the decrypted modifiable part information (i).

6. The method according to one of the claims 1-5, characterized in that a hash value (h_i) is generated for indicating security integrity of a message prior to modification and for step f) a hash function (CHash) is used providing a value identical to the generated hash value (Hash) for the modified message.

7. The method according to claim 6, characterized in that the hash function is a chameleon hash function.

8. The method according to one of the claims 1-7, characterized in that a message tag (t) is generated based at least on the sanitizing key tuple (PK_{san}, SK_{san}), the key tuple (K_{enc}, K_{mac}), and the modifiable part information (i).

9. The method according to one of the claims 1-8, characterized in that steps a) – c) include the substeps of

g1) choosing a random number (r_i) for each modifiable part (mi),

g2) generating a message header (h) including the random numbers (r_i) and modifiable part information (i),

g3) generating a message tag (t),

g4) encrypting and authenticating the message (m) with the encryption key into a first part (C_1),

g5) encrypting a secure communication protocol session key (K_{enc}) and a message id (m_{ID}) represented by the hash value (hash (h)) for the message header (h) with the sanitizable key tuple into a second part (C_2), and

g6) combining, preferably by concatenating (C_1, C_2), the first (C_1) and second (C_2) part into a single message.

10. The method according to one of the claims 1-9, characterized in that steps d) and e) include the substeps of

h1) decrypting the second part (C_2),

h2) decrypting the first part (C_1) based on the decrypted second part (C_2),

h3) identifying the modifiable parts (m_i),

h4) modifying one or more modifiable parts (m_i),

h5) encrypting the modified message (m'_i) with key tuple (K_{enc}).

11. The method according to one of the claims 1-10, characterized in that security integrity of the modified message (m') is checked by recomputing the hash values (hash (h)) of the modifiable and non-modifiable parts (m_i) of the modified message (m_i), by generating a new message tag (t') from the recomputed hash-values and by comparing the new message tag (t') with the message tag (t) of the original message (m).

12. A system for modifying an authenticated and/or encrypted message (m) by a modifying party (C) exchanged between a sending party (A) and a receiving party (B) based on a secure communication protocol, preferably for performing with a method according to one of the claims 1-11, characterized in that

the sending party (A) is operable to divide a clear message (m) into non-modifiable parts (m_1, m_2, ...) and modifiable parts (m_1, m_2, ...), to include modifiable part information (i) into the message (m), and to authenticate and/or to encrypt the message (m) by the sending party (A), that

the modifying party (C) is operable to be provided with en- and decrypticability and/or authenticability of the message (m) in such a way that the modifying party (C) can only modify the modifiable parts (i) of the message (m), and to modify one or more modifiable parts (m_i) by the modifying party (C), and that

the receiving party (B) is operable to receive the authenticated and/or encrypted modified message (m') according to the secure communication protocol and preferably is operable to check security integrity according to the secure communication protocol of a received message (m).

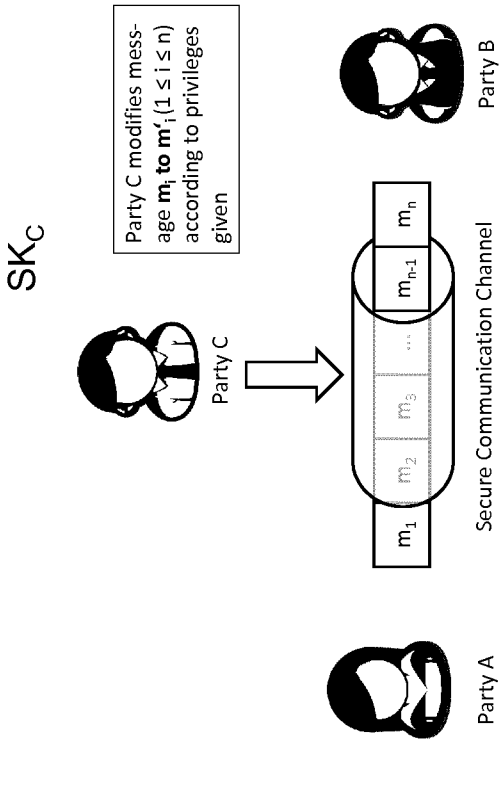

SK_C
Party C modifies message m_i to m'_i (1 ≤ i ≤ n) according to privileges given
Party C
Party A
Party B
m_1
m_2
m_3
m_{n-1}
m_n
Secure Communication Channel
PK_C

Fig. 1

Fig. 2

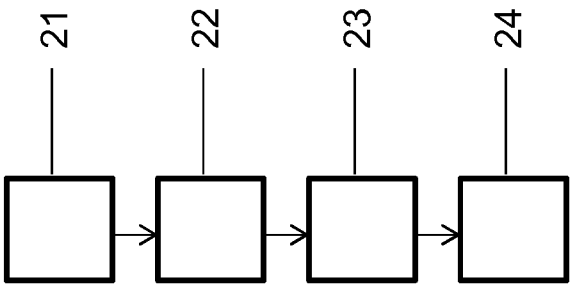


Fig. 3

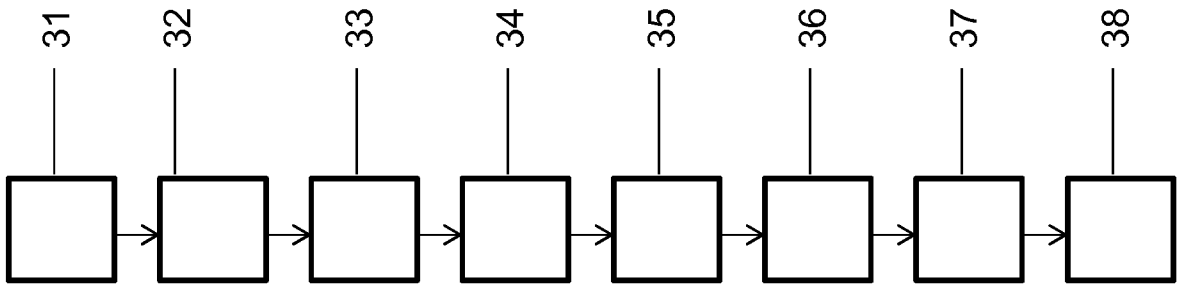


Fig. 4

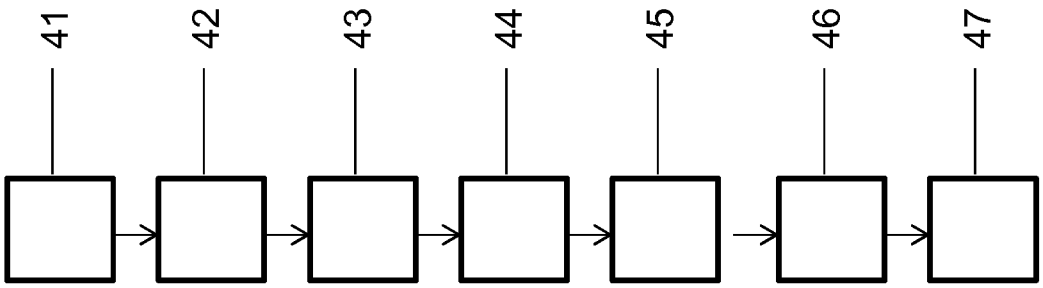


Fig. 5

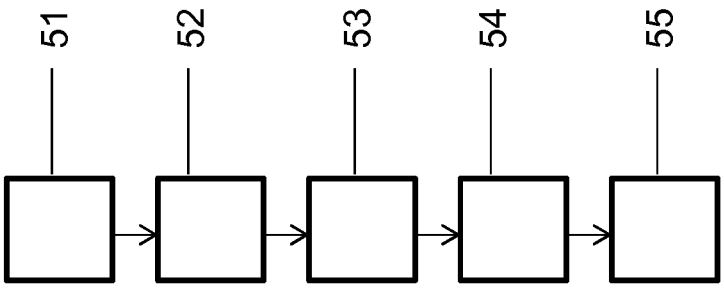


Fig. 6a

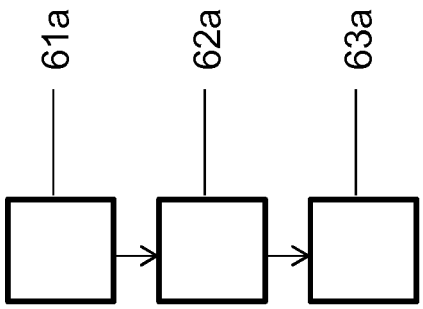


Fig. 6b

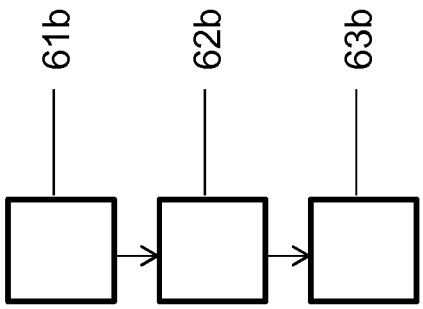
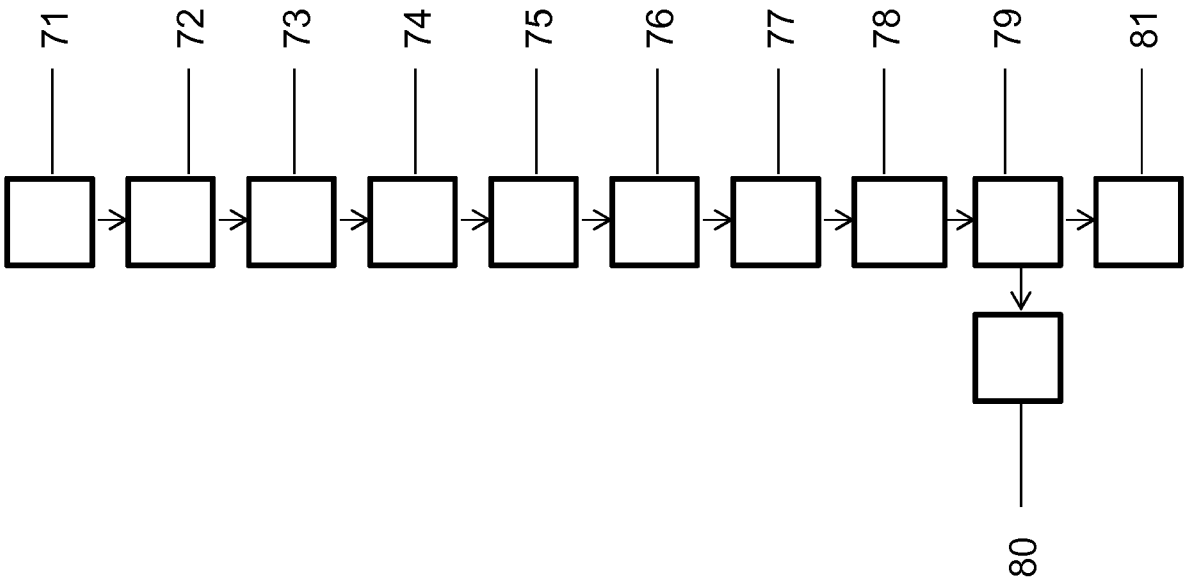


Fig. 7



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/057260

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2007/033391 A1 (HIRAMATSU TAKAHIRO [JP] ET AL) 8 February 2007 (2007-02-08) paragraph [0014] paragraph [0024] - paragraph [0025] paragraph [0035] -----	1-12
A	US 2003/196081 A1 (SAVARDA RAYMOND [US] ET AL) 16 October 2003 (2003-10-16) paragraph [0044] -----	1-12
A	WO 2007/103338 A2 (CIPHEROPTICS INC [US]; MCALISTER DONALD [US]) 13 September 2007 (2007-09-13) page 5, line 8 - line 16 page 11, line 8 - page 12, line 10 -----	1-12

☐ 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 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
26 July 2013	05/08/2013

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	Lázaro, Marisa

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/057260

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007033391 A1	08-02-2007	CN 1909443 A	07-02-2007
		JP 2007041223 A	15-02-2007
		US 2007033391 A1	08-02-2007
US 2003196081 A1	16-10-2003	AT 491184 T	15-12-2010
		AU 2003226286 A1	27-10-2003
		CA 2481651 A1	23-10-2003
		EP 1497745 A1	19-01-2005
		JP 2005522924 A	28-07-2005
		US 2003196081 A1	16-10-2003
		WO 03088072 A1	23-10-2003
WO 2007103338 A2	13-09-2007	US 2007214502 A1	13-09-2007
		WO 2007103338 A2	13-09-2007