(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 502 381 B9**

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

(15) Correction information:
Corrected version no 1 (W1 B1)
Corrections, see
Description Paragraph(s) 4, 9, 10, 11, 14, 16, 17
Claims DE 1, 2, 4, 6
Claims EN 1
Claims FR 1, 4

(48) Corrigendum issued on:
25.02.2015 Bulletin 2015/09

(45) Date of publication and mention of the grant of the patent:
30.04.2014 Bulletin 2014/18

(21) Application number: **10785020.8**

(22) Date of filing: **19.11.2010**

(51) Int Cl.:
H04L 9/30 *(2006.01)*

(86) International application number:
PCT/EP2010/067817

(87) International publication number:
WO 2011/061285 (26.05.2011 Gazette 2011/21)

(54) **METHOD FOR PUBLIC-KEY ATTRIBUTE-BASED ENCRYPTION WITH RESPECT TO A CONJUNCTIVE LOGICAL EXPRESSION.**

VERFAHREN FÜR EIGENSCHAFTSBASIERTE VERSCHLÜSSELUNG MIT ÖFFENTLICHEM SCHLÜSSEL IM ZUSAMMENHANG MIT EINER KONJUNKTIVEN LOGISCHEN EXPRESSION

PROCÉDÉ DE CHIFFREMENT À CLÉ PUBLIQUE AVEC ATTRIBUTS RELATIVEMENT À UNE EXPRESSION LOGIQUE CONJONCTIVE

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **19.11.2009 US 262602 P**

(43) Date of publication of application:
26.09.2012 Bulletin 2012/39

(73) Proprietor: **Nagravision S.A.**
1033 Cheseaux-sur-Lausanne (CH)

(72) Inventors:
- **KARLOV, Alexandre**
  CH-1217 Meyrin (CH)
- **JUNOD, Pascal**
  CH-1302 Vufflens-la-Ville (CH)

(74) Representative: **Leman Consulting S.A.**
Chemin de Précossy 31
1260 Nyon (CH)

(56) References cited:
EP-A1- 2 068 489

- **DAN BONEH ET AL: "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys", 1 January 2005 (2005-01-01), ADVANCES IN CRYPTOLOGY - CRYPTO 2005 LECTURE NOTES IN COMPUTER SCIENCE;; LNCS, SPRINGER, BERLIN, DE, PAGE(S) 258 - 275, XP019016555, ISBN: 978-3-540-28114-6 section 3.2**

Printed by Jouve, 75001 PARIS (FR)

(Cont. next page)

- **N. ATTRAPADUNGH. IMAI: "Conjunctive broadcast and attribute-based encryption", PAIRING-BASED CRYPTOGRAPHY - PAIRING 2009, THIRD INTERNATIONAL CONFERENCE, PALO ALTO, CA, USA, AUGUST 12-14, 2009, 14 August 2009 (2009-08-14), pages 248-265, XP019125129, cited in the application**

Description

Field of the invention

[0001] This invention refers to the field of broadcast encryption, in particular the way to manage authorization rights to access the content described by a logical expression in a broadcast system having a management center and a plurality of receiving devices which have certain characteristics.

Introduction

[0002] The area of broadcast encryption is well known in the art and was discussed for the first time by Fiat and Naor [1]. In this setting, the broadcasting center can send an encrypted message to a set of privileged (i.e., non-revoked) users which is a subset of the set of all possible receivers. Sometimes these terminals can be arranged according to some natural characteristics or attributes like their ZIP code based geographical location, their subscription to certain packages or their software version. Intuitively the broadcaster would like to broadcast to receivers which satisfy some of these properties in a more or less complex manner. For instance the broadcaster may want to enforce the access policy by sending the content only to receivers which are in (("New York") OR ("New Jersey")) AND (with a receiver's firmware not older than 2.1.1). It should be emphasized that in this scenario, the broadcaster does not know the receivers identities and broadcasts to a subsets of receivers according to a logical expression based on their characteristics contrary to the standard broadcast encryption model, where the center broadcasts to a specific subset of receivers by specifying explicitly their identities.

Prior Art

[0003] The notion of attribute-based encryption (ABE) where the center broadcasts to a subset of receivers in terms of descriptive attributes was introduced by Sahai and Waters in [2]. There are two types of ABE, namely: key-policy ABE where the access policy (also called the access structure) is specified in the private key and ciphertext-policy ABE where the access policy is specified in the ciphertext. Bethencourt, Sahai and Waters proposed the first construction of a ciphertext-policy ABE in [3]. Current invention concerns only ciphertext-policy ABE schemes, which will be further referenced simply as ABE schemes.

[0004] Those skilled in the art would agree that a logical access policy can be expressed using **AND**, **OR** and **NOT** logical gates. These expressions can be generalized under two forms, namely the *disjunctive normal form* (DNF) and the *conjunctive normal form* (CNF). The CNF is the conjunction (in other words a logical **AND**) of clauses, where a clause is a disjunction (in other words a logical **OR**) of attributes. The DNF is the disjunction (a logical **OR**) of conjunctions (a logical **AND**) of attributes. The **NOT** gate can be only part of a single attribute. For a set of attributes A_1,A_2,..., A_n an example of a CNF expression would be: $(A_1 \vee A_2, \vee A_3) \wedge (A_4 \vee A_5 \vee \neg A_6) \wedge ... \wedge (A_{n-2} \vee \neg A_{n-1} \vee \neg A_n)$ and an example of a DNF expression would be: $(A_1 \wedge \neg A_2 \neg \wedge A_3) \vee (\neg A_4 \wedge A_5 \wedge A_6) \vee ... \vee (A_{n-2} \wedge A_{n-1} \wedge \neg A_n)$. In the two examples above the symbol $\wedge$ represents a logical **AND**, and the symbol $\vee$ represents a logical **OR**.

[0005] An important notion is the one of a monotonic logical expression. The expression is called monotonic if it can be defined as a composition of logical **ANDs** and **ORs**, but without any **NOTs**.

[0006] It should be noted that the prior art describes ABE schemes, methods and systems which operate with DNF types of logical expressions, most of the them being monotonic and restricted to a certain fixed number of clauses or attributes per such expression. For instance, recently, such methods were disclosed in [4],[5] and [6].

[0007] Those skilled in the art would notice that the crucial property of an ABE scheme is the so-called attribute-collusion resistance property. This is represented by the fact that provided two decryption keys dk_{u_1} and dk_{u_2} for attributes A_1 and A_2 respectively, such that the key dk_{u_1} is not able to decrypt any ciphertext intended solely for A_2 and vice-versa, these keys can not be used in any way in order to decrypt a cryptogram described by an expression $A_1 \wedge A_2$.

Problem to be solved

[0008] The aim of the present invention is to address CNF types of logical expressions for ABE. The benefit of the present application is hence the possibility to efficiently perform ciphertext-policy ABE for CNF expressions with logical **AND**s and **OR**s, as well as logical **NOT**s.

Brief description of the invention

[0009] The aim is achieved thanks to a method for providing attribute-based encryption for conjunctive normal form (CNF) expressions, the said CNF expression consisting of at least one clause over a set of attributes, the said method

consisting of a key generation engine, an encryption engine and a decryption engine, and comprising the steps of:

Generating by the key generation engine a random $g \in G$, where G is a prime order group of order p, four random values $\alpha,\gamma,\beta,r \in_R Z/pZ$, and for $i = 1,2,...,n, n+2,...,2n$ computing by the key generation engine 2n values $g_i = g^{\alpha^i} \in G$ and $v = g^{\gamma} \in G$.

[0010] Generating by the encryption engine the encryption key $PK = (g^r, g_1^r, \ldots, g_n^r, g_{n+2}^r, \ldots, g_{2n}^r, v^r, g_n^{\beta}, g_n)$ consisting of 2n+3 group elements, n being the number expressing the size of the attribute set. For the abovementioned CNF expression over a set of attributes, CNF expression consisting of N clauses, generating by the encryption engine N random values $t_1,t_2,...,t_N \in_R Z/pZ$, computing by the encryption engine the value $t = \sum_{i=1}^{N} t_i \mod p$, generating by the encryption engine the cryptogram $hdr = (g_n^t, hdr_1, \ldots, hdr_N)$ consisting of 2N+1 group elements with $hdr_i = \left(g^{rt_i}, \left(v^r \prod_{j \in \beta_i} g_{n+1-j}^r \right)^{t_i} \right)$ for each clause β_i in the abovementioned CNF expression and generating the session key SK as $SK = e(g_1^r, g_n^{\beta})^t = e(g,g)^{\beta r \alpha^{(n+1)} t}$, wherein the said session key or parts thereof is used to derive a symmetric key to encrypt the message, or to encrypt the message with the said session key. Generating by the key generation engine a plurality of private decryption keys $dk_u = (g_1^{r(\beta+s_u)}, g_1^{s_u}, \ldots, g_n^{s_u}, g_{n+2}^{s_u}, \ldots, g_{2n}^{s_u}, d_{i_1}, \ldots, d_{i_N}, d_{j_1}, \ldots, d_{j_R})$ each of the said decryption keys explicitly associated with at least one positive attribute by the mean of the group element $d_{i_j} = g_{i_j}^{\gamma \cdot s_u}$ and explicitly associated with at least one negative attribute by the means of the group element $d_{j_k} = g_{j_k}^{\gamma \cdot s_u}$ wherein the value s_u, is a random group element and is unique for every decryption key.

Brief description of the figure

[0011] The method of the invention will be better understood thanks to the attached figures in which:

- the figure 1 illustrates a broadcaster and a plurality of receivers
- the figure 2 illustrates a management center in communication with a plurality of receivers.

Detailed description of the invention

[0012] The present invention relates to cryptographic systems and methods and provides an attribute collusion-resistant ciphertext-policy attribute-based encryption scheme for conjunctive normal form (CNF) expressions.

Bilinear Maps

[0013] The present invention relies on bilinear maps (also called pairings in the related art). Let G and G_T be two cyclic groups of prime order p and a generator $g \in G$. Let $e : G \times G \rightarrow G_T$ be a non-degenerate bilinear map such that for all $x, y \in G$ and $a, b \in Z/pZ$, we have $e(x^a, y^b) = e(x,y)^{ab}$ and $e(g,g) \neq 1$. The function e(.,.) should be also efficiently computable. For example, such maps can be, for instance, Weil or Tate pairings on supersingular elliptic curves. Their usage and implementation is well-known in the art. Weil and Tate pairings are provided here as examples and for the purpose of the preferred embodiment and it should be noted that any admissible pairing function e(.,.) with the above properties can be used. The preferred method involved in the computation of such a function will be the so-called Miller's algorithm for pairing calculation which is well known in the related art [7].

Choice of the parameters

[0014] In the preferred embodiment we are using a supersingular elliptic curve $E(F_p)$ with $p \equiv 3 \pmod 4$ a prime number of at least 512 bits and the order of $E(F_p) = p+1$. The group of point on the elliptic curve $E(F_p)$ should also have a subgroup of prime order q of at least 160 bits. The sizes of these parameters correspond to the (block cipher) security equivalent of 80 bits. The generation of such elliptic curves is well known in the related art. Hence the following map is defined based on the Tate pairing function: $E[q] \times E'(F_p) \rightarrow F_{p^2}^*$, where $E'(F_p)$ is defined to be the twisted curve and $E[q]$ is the group of q-torsion points on E. Such parameters selection allows us to use a lightweight version of the Miller's algorithm along with arithmetic operations performed mostly in F_p, which is much faster, contrary to traditional methods of using arithmetic in F_{pk}. In fact, these methods are also well-known in the art and are disclosed in details in [8]. It should be noted that in this case the group G is represented by the q-torsion subgroup of $E(F_p)$ and has the prime order q.

Preferred implementation of the scheme

[0015] According to the preferred embodiment of the current invention we consider a system where receivers can be arranged according to some characteristics or attributes, such as geographical position, firmware version, etc. Let n be the total number of such characteristics or attributes and λ be the total number of receivers. Hence for the sake of the preferred embodiment we can name these characteristics with n literals $A_1, A_2, ..., A_n$. The preferred implementation of the current invention includes three randomized algorithms, namely *KeyGen, Encrypt* and *Decrypt* implemented on a computer or in a dedicated apparatus. It should be also noted that in the below preferred implementation we will use an additive group law notation which is also frequently used in the art.

[0016] KeyGen algorithm starts by generating a random point $G \in E[g]$ by any well known mean of the art, as well as four random values $\alpha,\gamma,\beta,r \in_R Z/qZ$. Then for $i = 1,2,..., n, n+2,...,2n$ the algorithm computes 2n-1 values $G_i = \alpha^i G$ and $V = \gamma G$. The algorithm then generates a public encryption key $PK = (rG, rG_1,...,rG_n, rG_{n+2},...,rG_{2n}, rV, \beta G_n, G_n)$ consisting of 2n+3 points in the group E[q]. The algorithm will also generate a plurality of individual private decryption keys for each of ℓ receivers as follows. First the algorithm generates by any known mean of the art a random value $s_u \in Z/qZ$. Then, for $i = 1,2,...,n,n+2,...,2n$ it sets 2n-1 values $s_uG_1,...,s_uG_n, s_uG_{n+2},...,s_uG_{2n}$ and computes the value $r(\beta + s_u)G_n$. Finally, for every defined property among $A_1, A_2,..., A_n$ which characterizes the receiver, the algorithm computes N+R values $D_{i1},...,D_{iN}, D_{j1},...,D_{jR}$ where $D_{ij} = \gamma \cdot s_u G_{ij}$ and $D_{jk} = \gamma \cdot s_u G_{jk}$. Hence the decryption key for an individual receiver, characterized by N+R properties among n, consists of 2n+N+R group elements (or in the case of the preferred embodiment - points on the elliptic curve $E(F_p)$), that is $dk_u = (r(\beta + S_u)G_1, s_uG_1,...,s_uG_n, s_uG_{n+2},...,s_uG_{2n}, D_{i1},...D_{iN}, D_{j1},.... D_{jR})$. The said individual decryption key is loaded into the receiver, preferably by loading the said key into the secure and tamper-resistant non-volatile memory using methods known in the corresponding art.

[0017] Encryption algorithm is provided with an expression in CNF of the form $\beta_1 \wedge \beta_2 \wedge ... \wedge \beta_N$, wherein every clause β_i consists of a disjunction (logical **OR**s) of several attributes. First, the algorithm randomly generates N values $t_1,...,t_N \in Z/qZ$ by any well known mean of the art and computes the value $t = \sum_{i=1}^{N} t_i \bmod q$. The encryption algorithm also computes the value $hdr_0 = t \cdot G_n$. The algorithm then computes for every clause β_i a pair of values, namely $hdr_{i,0} = t_i rG$ and $hdr_{i,1} = t_i \left(rV + \sum_{j \in \beta_i} rG_{n+1-j} \right)$. It should be noted that the value j corresponds to an attribute in the clause β_i. The said pair of values constitutes the i-th part of the cryptogram. After computing N-th such pair (for the last clause β_N), the encryption algorithm computes the session key $SK = e(r \cdot G_1, \beta \cdot G_n)^t = e(G,G)^{\beta r \alpha^{(n+1)} t}$. The resulting session key hence has a size of 1024 bits with the parameters of the preferred embodiment. The said session key is then hashed, in the context of the preferred embodiment, using the SHA-256 hash function known in the art. The resulting 128 less significant bits are used as the key for the AES algorithm in encryption mode, the said algorithm also well-known in the art, to encrypt video, audio or other useful messages. Finally, the encryption algorithm outputs the generated cryptogram $hdr = (hdr_0, hdr_{i.0}, hdr_{i,1},...,hdr_{N.0}, hdr_{N,1})$. It should be noted, that the CNF expression is broadcasted along with the cryptogram and the useful message which is encrypted by mean of the session key above to the intended recipients.

Decryption algorithm, upon receiving the cryptogram

[0018] $hdr = (hdr_0, hdr_{i,0}, hdr_{i,1}, \ldots, hdr_{N,0}, hdr_{N,1})$, the corresponding expression in CNF and the useful encrypted message, examines the expression and determines whether or not the receiver fulfils the necessary conditions for decrypting the message. In the case where it does fulfil the necessary conditions, the decryption algorithm proceeds as follow. First, for every clause in the expression it computes the values $SK_i^{s_u} = \frac{e(s_u \cdot G_k, hdr_{i,1})}{e\left(D_k + \sum_{j \in \beta_i, j \neq k} s_u \cdot G_{n+1-j+k}, hdr_{i,0}\right)}$, where the values D_k are bonded to the characterizing attributes of the receiver, the said attributes being also listed in the clause β_i. Each of such N computations is performed using two pairing function described above. After computing N such values $SK_1^{s_u}, \ldots, SK_N^{s_u}$, the decryption algorithm computes the session key as $SK = \frac{e(hdr_0, r(\beta + s_u) \cdot G_1)}{\prod_{i=1}^{N} SK_i^{s_u}}$. The said session key is then hashed, in the context of this preferred embodiment, using the SHA-256 hash function and the resulting 128 less significant bits are used as the key for the AES algorithm in decryption mode to decrypt the useful message.

[0019] The person skilled in the art would appreciate the fact that the encryption key is public, any party can use it to encrypt any useful contents with respect to any CNF expression and that the said encryption key can not be used to derive the session key or decrypt the useful message without fulfilling a given CNF expression by explicitly possessing the decryption keys corresponding to the said expression. Those familiar with the art would also appreciate the fact that the proposed method fulfills the attribute collusion-resistance property described above. Contrary to the existing schemes of the art, the present invention can support expressions of any number of clauses and attributes without any constraints. Also, the size of the header is linear in the number of clauses and does not depend on the number of the attributes in any clause or in the whole expression.

[0020] It is important to note that the use of the particular supersingular elliptic curve over the finite field of a given size, its prime order subgroup, the specific bilinear map function as defined above, its parameters, key sizes, the use of the SHA-256 hash function and AES encryption algorithm is solely defined for the purpose of the preferred embodiment of the present invention and is not, in any case, limiting. Any elliptic curve, or any other group where the bilinear map can be efficiently and securely computed for a given security parameter can be used for the purpose of the present invention. The useful message, such as (but not limited to) video or audio content, can be encrypted or scrambled by any cryptographically secure means using key or keys derived from the session key defined in the scope of the present invention. The above broadcast encryption scheme can be used to transmit messages from a control center to a plurality of terminals. These messages contain initialization data pertaining to one terminal.

[0021] In the figure 2, the management center MC stores in its database DB a copy of the key materials sent in the receiving devices RD1, RD2, RD3. According to our example, two subscription packages B1, B2 have been defined, the first one being related to the positive key material K1 and the negative material K1', the second one being related to the positive key material K2 and the negative material K2'.

[0022] The receiving device RD1 being entitled to the subscription package B1 has received the key material K1. Due to the fact that this receiving device RD1 is not entitled to the subscription package B2, the key material K2' was also sent to it.

[0023] The receiving device RD2 being entitled to the subscription package B1 and B2, both key material K1 and K2 were sent to this device.

[0024] The receiving device RD2 being entitled to the Subscription package B2, the key material K2 was sent to it. Due to the fact that this receiving device RD3 is not entitled to the Subscription package B1, the key material K1' was also sent to it.

[0025] In case that the management center MC needs to transmit an access key K to only the receiving devices allowed to the second Subscription package B2 and not allowed to the first Subscription package B1, the cryptogram CY sent to the receiving devices RD will contain the access key combined with the negative key material K1' and the positive key material K2.

[0026] In the authorization message containing the cryptogram, another field into the message contains a descriptor of the keys to be used for the decryption. This can be in the form of two bitmap, each active bits defining a subscription package, and one bitmap for the positive keys and the other one for the negative keys. According to the implementation

of the invention, it could decided that the positive keys are used first to decrypt the cryptogram and then the negative keys.

[0027] The product key can release a single broadcast product, e.g. a film or can release a service for a day or a month.

[0028] The subscription package can refer to a plurality of services or a single service. The invention thus allows to define the access rule of this product by combining the access to the channel 3 (first subscription package) and not the channel 6 (second subscription package).

[0029] The invention has been described in detail with particular reference to the preferred embodiment thereof. It should be however understood that variations and modifications can be produced.

REFERENCES

[0030]

[1] A. Fiat and M. Naor, "Broadcast encryption", CRYPTO'93, Lecture Notes in Computer Science 773, pp. 480491, Springer-Verlag, 1994.

[2] A. Sahai and B. Waters. Fuzzy identity-based encryption. In Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, pages 457-473, 2005.

[3] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In 2007 IEEE Symposium on Security and Privacy (S&P 2007), 20-23 May 2007, Oakland, California, USA, pages 321-334, 2007.

[4] B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. http://eprint.iacr.org/2008/290.pdf, 2008. Unpublished manuscript.

[5] D. Lubicz and T. Sirvent. Attribute-based broadcast encryption scheme made efficient. In S. Vaudenay et al., editor, Proc. of Advances in Cryptology - Africacrypt'08, volume 5023 of LNCS, pages 325-342. Springer-Verlag, 2008.

[6] N. Attrapadung and H. Imai. Conjunctive broadcast and attribute-based encryption. In Pairing-Based Cryptography - Pairing 2009, Third International Conference, Palo Alto, CA, USA, August 12-14, 2009, pages 248-265, 2009.

[7] V. Miller. Short program for functions on curves. http://crypto.stanford.edu/miller/miller.pdf, 1986. Unpublished manuscript.

[8] P. Barreto, H. Kim, B. Lynn, M. Scott. Efficient Algorithms for Pairing-Based Cryptosystems. In Advances in Cryptology- CRYPTO 2002, 22nd Annual International Cryptology Conference, pages 354-368, London, UK, 2002. Springer-Verlag.

Claims

1. A method for providing attribute-based encryption of a message using conjunctive normal form (CNF) expressions, the said CNF expression comprising at least one clause over a set of *n* attributes, the said method using a key generation engine, an encryption engine and a decryption engine, and comprising the steps of:

   a. generating by the key generation engine: a random $g \in G$, where G is a group of order p where p is a prime number, four random values $\alpha,\gamma,\beta,r \in_R Z/pZ$, and for $i = 1,2,...,n,n+2,...,2n$ where n is the number of attributes, computing by the key generation engine at least 2n-1 values $g_i = g^{\alpha^i} \in G$ and at least one value $v = g^{\gamma} \in G$;

   b. generating by the encryption engine an encryption key $PK = (g^r, g_1^r, \ldots, g_n^r, g_{n+2}^r, \ldots, g_{2n}^r, v^r, g_n^{\beta}, g_n)$ comprising at least 2n+3 group elements;

   c. for an abovementioned CNF expression over a set of attributes, CNF expression comprising N clauses, generating by the encryption engine N random values $t_1,t_2,...,t_N \in_R Z/pZ$, computing by the encryption engine

the value $t = \sum_{i=1}^{N} t_i$ mod *p*, generating by the encryption engine a cryptogram $hdr = (g_n^t, hdr_1, \ldots, hdr_N)$

consisting of at least 2N+1 group elements with $hdr_i = \left(g^{rt_i}, \left(v^r \prod_{j \in \upsilon_i} g_{n+1-j}^r \right)^{t_i} \right)$ for each clause υ_i in the abovementioned CNF expression and generating a session key *SK*, wherein the said session key or parts thereof is used to derive a symmetric key which is used to encrypt the message, or to encrypt the message with the said session key;

d. generating by the key generation engine a plurality of private decryption keys $dk_u = (g_1^{r(\beta+s_u)}, g_1^{s_u}, \ldots, g_n^{s_u}, g_{n+2}^{s_u}, \ldots, g_{2n}^{s_u}, d_{i_1}, \ldots, d_{i_N}, d_{j_1}, \ldots, d_{j_R})$ each of the said decryption keys explicitly associated with at least one positive attribute by the mean of the group element $d_{i_j} = g_{i_j}^{\gamma \cdot s_u}$ and explicitly associated with at least one negative attribute by the means of the group element $d_{j_k} = g_{j_k}^{\gamma \cdot s_u}$ wherein the value s_u is a random group element and is unique for every decryption key dk_u.

2. The method defined in claim 1 wherein the session key *SK* is computed by the encryption engine using a bilinear map as $SK = e(g_1^r, g_n^\beta)^t = e(g,g)^{\beta r \alpha^{(n+1)} t}$.

3. The method defined in claim 1 further comprising providing the decryption engine with the decryption key dk_u associated with at least one positive and one negative attribute, providing the decryption engine with the cryptogram hdr consisting of at least 2N+1 group elements, and providing the decryption engine with the conjunctive normal form (CNF) expression over a set of attributes of N clauses corresponding to the said cryptogram.

4. The method defined in claims 1 and 3 further comprising computing for each of N clauses by the decryption engine the intermediate values $SK_i^{s_u} = \frac{e(g_k^{s_u}, hdr_{i,1})}{e\left(d_k \cdot \prod_{j \in \upsilon_i, j \neq k} g_{n+1-j+k}^{s_u}, hdr_{i,0} \right)}$, wherein d_k is explicitly associated with an attribute present in the said clause.

5. The method defined in claim 4 wherein the said intermediate values are computed using bilinear maps.

6. The method defined in claims 4 or 5 further comprising computing by the decryption engine the value of the session key $SK = \frac{e(hdr_0, g_1^{r(\beta+s_u)})}{\prod_{i=1}^{N} SK_i^{s_u}}$.

7. The method defined in claims 1, 3, 4 and 6 further comprising using the session key or parts thereof to derive a symmetric key to decrypt the message, or to decrypt the message with said session key.

8. The method defined in claims 1, 3, 4 and 6 wherein the said session key SK is computed using a bilinear map.

9. A device adapted to implement the method of any of claims 1 to 8.

Patentansprüche

1. Verfahren zur attributbezogenen Verschlüsselung einer Nachricht unter Verwendung von Ausdrücken in konjunktiver Normalform (KNF), wobei der besagte KNF-Ausdruck mindestens eine Klausel über eine Menge von *n* Attributen umfasst und das besagte Verfahren einen Schlüsselgenerator, eine Verschlüsselungsroutine und eine Entschlüsselungsroutine verwendet, mit folgenden Phasen:

   a. Erzeugung, mit Hilfe des Schlüsselgenerators: eines zufälligen $g \in G$, wobei G eine Gruppe p-ter Ordnung ist, wobei p eine Primzahl ist; vier zufälliger Werte $\alpha,\gamma,\beta,r \in_R Z/pZ$, und für $i = 1,2,...,n,n+2,...,2n$ wobei n die Zahl der Attribute ist; und Berechnung, mit Hilfe des Schlüsselgenerators, von mindestens 2n-1 Werten $g_i = g^{\alpha^i} \in G$ und mindestens eines Wertes $v = g^{\gamma} \in G$;
   b. Erzeugung, mit Hilfe der Verschlüsselungsroutine, eines Chiffrierschlüssels $PK = (g^r, g_1^r, \ldots, g_n^r, g_{n+2}^r, \ldots, g_{2n}^r, v^r, g_n^{\beta}, g_n)$, der mindestens 2n+3 Gruppenelemente umfasst;
   c. für einen oben erwähnten KNF-Ausdruck über eine Menge von Attributen, wobei der KNF-Ausdruck N Klauseln umfasst, Erzeugung, mit Hilfe der Verschlüsselungsroutine, von N zufälligen Werten $t_1,t_2,...,t_N \in_R Z/pZ$, Berechnung, mit Hilfe der Verschlüsselungsroutine, des Wertes $t = \sum_{i=1}^{N} t_i \bmod p$, Erzeugung, der mit Hilfe der Verschlüsselungsroutine, eines Kryptogramms $hdr = (g_n^t, hdr_1, \ldots, hdr_N)$, das aus mindestens 2N+1-Gruppenelementen besteht, mit $hdr_i = \left(g^{rt_i}, \left(v^r \prod_{j \in \upsilon_i} g_{n+1-j}^r \right)^{t_i} \right)$ für jede Klausel υ_i in dem oben erwähnten KNF-Ausdruck und durch Erzeugung eines Sitzungsschlüssels *SK*, wobei der besagte Sitzungsschlüssel, oder Teile davon, benutzt wird, um einen symmetrischen Schlüssel abzuleiten, der benutzt wird, um die Nachricht zu verschlüsseln, oder um die Nachricht mit dem besagten Sitzungsschlüssel zu verschlüsseln;
   d. Erzeugung, mit Hilfe des Schlüsselgenerators, einer Vielzahl von privaten Dechiffrierschlüsseln $dk_u = (g_1^{r(\beta+s_u)}, g_1^{s_u}, \ldots, g_n^{s_u}, g_{n+2}^{s_u}, \ldots, g_{2n}^{s_u}, d_{i_1}, \ldots, d_{i_N}, d_{j_1}, \ldots, d_{j_R})$, wobei jeder der besagten Dechiffrierschlüssel mittels des Gruppenelements $d_{i_j} = g_{i_j}^{\gamma \cdot s_u}$ mindestens einem positiven Merkmal eindeutig zugeordnet ist und mittels des Gruppenelements $d_{j_k} = g_{j_k}^{\gamma \cdot s_u}$ mindestens einem negativen Merkmal eindeutig zugeordnet ist, wobei der *Wert* s_u ein zufälliges Gruppenelement und für jeden Dechiffrierschlüssel dk_u einmalig ist.

2. Verfahren nach Anspruch 1, wobei der Sitzungsschlüssel *SK* von der Verschlüsselungsroutine unter Verwendung einer bilinearen Abbildung wie $SK = e(g_1^r, g_n^{\beta})^t = e(g,g)^{\beta r \alpha^{(n+1)} t}$ berechnet wird.

3. Verfahren nach Anspruch 1, wobei die Entschlüsselungsroutine des weiteren den Dechiffrierschlüssel dk_u umfasst, dem mindestens ein positives und ein negatives Merkmal zugeordnet ist, wobei die Entschlüsselungsroutine das Kryptogramm hdr umfasst, bestehend aus mindestens 2N+1- Gruppenelementen, und wobei die Entschlüsselungsroutine den Ausdruck in konjunktiver Normalform (KNF) über eine Menge von Attributen von N Klauseln entsprechend dem besagten Kryptogramm umfasst.

4. Verfahren nach den Ansprüchen 1 und 3 mit zusätzlicher Berechnung der Zwischenwerte $SK_i^{s_u} = \frac{e(g_k^{s_u}, hdr_{i,1})}{e\left(d_k \cdot \prod_{j \in \upsilon_i, j \neq k} g_{n+1-j+k}^{s_u}, hdr_{i,0} \right)}$ für jede von N Klauseln durch die Entschlüsselungsroutine, wobei d_k ein

Merkmal, das in der besagten Klausel vorhanden ist, eindeutig zugeordnet ist.

5. Verfahren nach Anspruch 4, wobei die Zwischenwerte unter Verwendung von bilinearen Abbildungen berechnet werden.

6. Verfahren nach den Ansprüchen 4 oder 5 mit zusätzlicher Berechnung des Wertes des Sitzungsschlüssels $SK = \frac{e(hdr_0, g_1^{r(\beta+s_u)})}{\prod_{i=1}^{N} SK_i^{s_u}}$ durch die der Entschlüsselungsroutine.

7. Verfahren nach den Ansprüchen 1, 3, 4 und 6 mit zusätzlicher Verwendung des Sitzungsschlüssels oder von Teilen davon, um einen symmetrischen Schlüssel abzuleiten, um die Nachricht zu entschlüsseln, oder um die Nachricht mit besagtem Sitzungsschlüssel zu entschlüsseln.

8. Verfahren nach den Ansprüchen 1, 3, 4 und 6, wobei der Sitzungsschlüssel SK unter Verwendung einer bilinearen Abbildung berechnet wird.

9. Vorrichtung zur Durchführung des Verfahrens nach einem beliebigen der Ansprüche 1 bis 8.

Revendications

1. Méthode pour assurer un cryptage à base d'attributs pour un message utilisant des expressions de forme normale conjonctive (FNC), ladite expression FNC comprenant au moins une clause sur un ensemble de n attributs, ladite méthode utilisant un générateur de clés, un moteur de chiffrement et un moteur de déchiffrement, et comprenant les étapes suivantes:

a. générer au moyen du générateur de clés: une valeur aléatoire $g \in G$, où G est un groupe d'ordre p où p est un nombre premier, quatre valeurs aléatoires $\alpha,\gamma,\beta,r \in_R Z/pZ$, et pour $i = 1,2,\ldots,n,n+2,\ldots,2n$ où n est le nombre d'attributs, calculer au moyen du générateur de clés au moins 2n-1 valeurs $g_i = g^{\alpha^i} \in G$ et au moins une valeur $v = g^{\gamma} \in G$;
b. générer par le moteur de chiffrement une clé de chiffrement $PK = (g^r, g_1^r, \ldots, g_n^r, g_{n+2}^r, \ldots, g_{2n}^r, v^r, g_n^{\beta}, g_n)$ comprenant au moins 2n+3 éléments de groupe;
c. pour une expression FNC précitée sur un ensemble d'attributs, l'expression FNC comprenant N clauses, générer par le moteur de chiffrement N valeurs aléatoires $t_1,t_2,\ldots,t_N \in_R Z/pZ$, calculer par le moteur de chiffrement la valeur $t = \sum_{i=1}^{N} t_i \mod p$, générer par le moteur de chiffrement un cryptogramme $hdr = (g_n^t, hdr_1, \ldots, hdr_N)$ constitué d'au moins 2N+1- éléments de groupe avec $hdr_i = \left(g^{rt_i}, \left(v^r \prod_{j \in \upsilon_i} g_{n+1-j}^r \right)^{t_i} \right)$ pour chaque clause υ_i dans l'expression FNC précitée et générer une clé de session *SK*, dans laquelle ladite clé de session, ou des parties de celle-ci, est utilisée pour dériver une clé symétrique qui est utilisée pour chiffrer le message, ou pour chiffrer le message avec ladite clé de session;

d. générer par le générateur de clés une pluralité de clés de déchiffrement privées $dk_u = (g_1^{r(\beta+s_u)}, g_1^{s_u}, \ldots, g_n^{s_u}, g_{n+2}^{s_u}, \ldots, g_{2n}^{s_u}, d_{i_1}, \ldots, d_{i_N}, d_{j_1}, \ldots, d_{j_R})$ chacune desdites clés de déchiffrement étant explicitement associée à au moins un attribut positif au moyen de l'élément de groupe $d_{i_j} = g_{i_j}^{\gamma \cdot s_u}$

et explicitement associée à au moins un attribut négatif au moyen de l'élément de groupe $d_{j_k} = g_{j_k}^{\gamma \cdot s_u}$ dans lequel la valeur s_u est un élément de groupe aléatoire et est unique pour chaque clé de déchiffrement dk_u.

2. Méthode selon la revendication 1, **caractérisée en ce que** la clé de session *SK* est calculée par le moteur de chiffrement en utilisant une application bilinéaire comme $SK = e(g_1^r, g_n^\beta)^t = e(g,g)^{\beta r \alpha^{(n+1)} t}$.

3. Méthode selon la revendication 1, comprenant en outre une étape visant à fournir au moteur de déchiffrement une clé de déchiffrement dk_u associée à au moins un attribut positif et un attribut négatif, fournir au moteur de déchiffrement un cryptogramme hdr constitué d'au moins 2N+1- éléments de groupe, et fournir au moteur de déchiffrement l'expression de forme normale conjonctive (FNC) sur un ensemble d'attributs de N clauses correspondant audit cryptogramme.

4. Méthode selon les revendications 1 et 3, comprenant en outre, pour chacune des N clauses, le calcul par le moteur de déchiffrement des valeurs intermédiaires $SK_i^{s_u} = \dfrac{e(g_k^{s_u}, hdr_{i,1})}{e\left(d_k \cdot \prod_{j \in \upsilon_i, j \neq k} g_{n+1-j+k}^{s_u}, hdr_{i,0}\right)}$, dans lesquelles d_k est explicitement associé à un attribut présent dans ladite clause.

5. Méthode selon la revendication 4, **caractérisée en ce que** lesdites valeurs intermédiaires sont calculées en utilisant des applications bilinéaires.

6. Méthode selon les revendications 4 ou 5, comprenant en outre le calcul par le moteur de déchiffrement de la valeur de la clé de session $SK = \dfrac{e(hdr_0, g_1^{r(\beta + s_u)})}{\prod_{i=1}^{N} SK_i^{s_u}}$.

7. Méthode selon les revendications 1, 3, 4 et 6 comprenant en outre l'utilisation de la clé de session, ou de parties de celle-ci, pour dériver une clé symétrique pour déchiffrer le message, ou pour déchiffrer le message avec ladite clé de session.

8. Méthode selon les revendications 1, 3, 4 et 6, **caractérisée en ce que** ladite clé de session SK est calculée en utilisant une application bilinéaire.

9. Dispositif pour la mise en oeuvre de la méthode selon l'une quelconque des revendications 1 à 8.

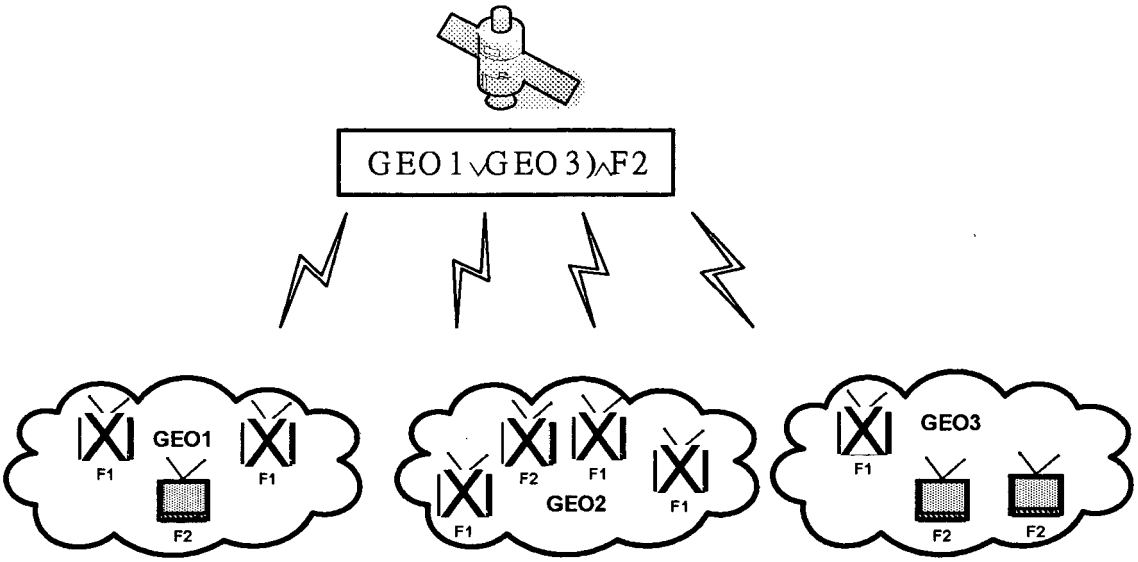
GEO 1 ∨ GEO 3) ∧ F2
GEO1
F1
F1
F2
F2
F1
GEO2
F1
F1
GEO3
F1
F2
F2

FIG. 1

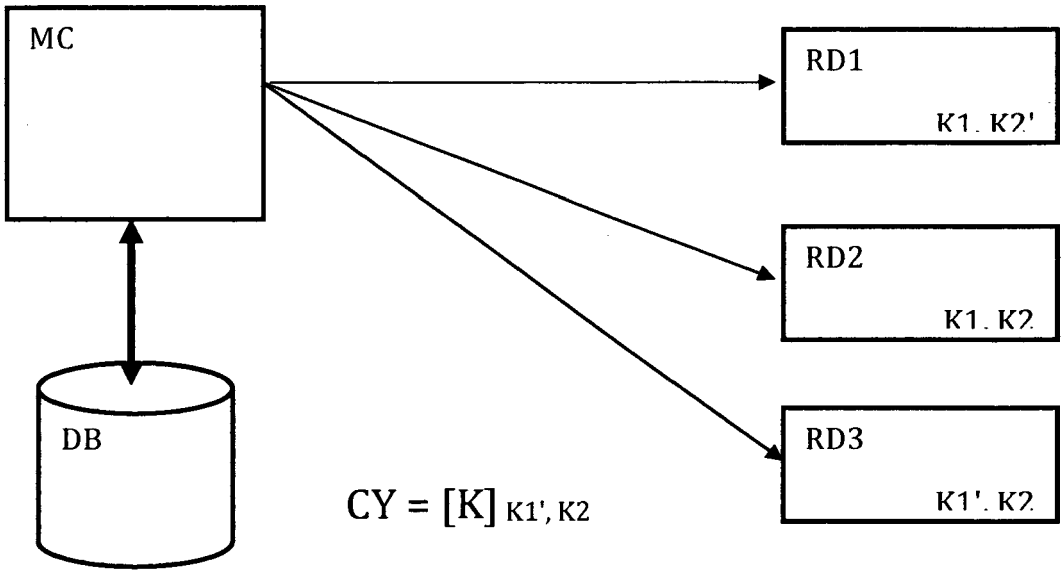
MC
DB
RD1
K1. K2'
RD2
K1. K2
RD3
K1'. K2
CY = [K] K1', K2

Fig. 2

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Non-patent literature cited in the description

- Broadcast encryption. **A. FIAT ; M. NAOR.** CRYPTO'93, Lecture Notes in Computer Science 773. Springer-Verlag, 1994, 480491 **[0030]**
- Fuzzy identity-based encryption. **A. SAHAI ; B. WATERS.** Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark. 2005, 457-473 **[0030]**
- **J. BETHENCOURT ; A. SAHAI ; B. WATERS.** Ciphertext-policy attribute-based encryption. *2007 IEEE Symposium on Security and Privacy,* 20 May 2007, 321-334 **[0030]**
- **B. WATERS.** *Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization, http://eprint.iacr.org/2008/290.pdf, 2008. Unpublished manuscript* **[0030]**
- Attribute-based broadcast encryption scheme made efficient. **D. LUBICZ ; T. SIRVENT et al.** Proc. of Advances in Cryptology - Africacrypt'08. LNCS, 2008, vol. 5023, 325-342 **[0030]**
- **N. ATTRAPADUNG ; H. IMAI.** Conjunctive broadcast and attribute-based encryption. *Pairing-Based Cryptography - Pairing 2009, Third International Conference, Palo Alto, CA, USA,* 12 August 2009, 248-265 **[0030]**
- **V. MILLER.** *Short program for functions on curves,* 1986, http://crypto.stanford.edu/miller/miller.pdf **[0030]**
- Efficient Algorithms for Pairing-Based Cryptosystems. **P. BARRETO ; H. KIM ; B. LYNN ; M. SCOTT.** Advances in Cryptology- CRYPTO 2002, 22nd Annual International Cryptology Conference. Springer-Verlag, 2002, 354-368 **[0030]**