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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 July 2009 (23.07.2009)

PCT

(10) International Publication Number
WO 2009/090519 A1

(51) International Patent Classification:
H04L 9/30 (2006.01) *H04L 9/08* (2006.01)
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/IB2008/055577

(22) International Filing Date:
30 December 2008 (30.12.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
08100505.0 15 January 2008 (15.01.2008) EP

(71) Applicant *(for all designated States except US)*: **NXP B.V.** [NL/NL]; High Tech Campus 60, NL-5656 AG Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **NIKOV, Ventzislav** [BG/BE]; c/o NXP Semiconductors, IP & L Department, HTC 60, NL-5656 AG Eindhoven (NL). **VAUCLAIR, Marc** [BE/BE]; c/o NXP Semiconductors, IP & L Department, HTC 60, NL-5656 AG Eindhoven (NL). **JANSSENS, Pieter, Johan** [BE/BE]; c/o NXP Semiconductors, IP Department, HTC 60, NL-5656 AG Eindhoven (NL).

(74) Agent: **VAN DER VEER, Johannis, L.**; c/o NXP Semiconductors, IP Department, HTC 60 1.31, NL-5656 AG Eindhoven, (NL).

(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, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Declaration under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— *with international search report*

(54) **Title:** EFFICIENT RECONSTRUCTION OF A PUBLIC KEY FROM AN IMPLICIT CERTIFICATE

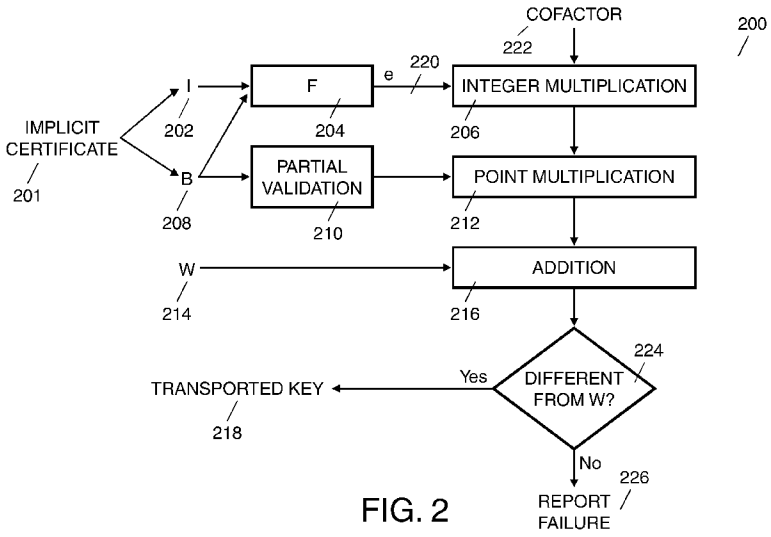

FIG. 2

(57) **Abstract:** A method for reconstructing a transported public key from an implicit certificate, wherein the implicit certificate comprises reconstruction data for reconstructing the transported public key, said method comprising the steps of: obtaining an authoritative public key; processing the implicit certificate in accordance with a mathematical function to derive an entity information; carrying out a partial validation of said reconstruction data; reconstructing the transported public key from the reconstruction data, the entity information, and the authoritative public key; wherein the method is executable at a data processing system.

WO 2009/090519 A1

Efficient reconstruction of a public key from an implicit certificate

FIELD OF THE INVENTION

The invention relates to cryptography. In particular, this invention relates to secure and efficient reconstruction of public keys from implicit certificates.

BACKGROUND OF THE INVENTION

In digital communication there is a need for digital signatures. Such a digital signature can be attached to an electronic document or other digital file, and indicates to a recipient that the sender of the electronic document or digital file authenticates the document or the digital file and/or that such file was unaltered during transit. Also digital signatures are used extensively in cryptographic protocols. In the remainder of this document the term "signature" will refer to a digital signature.

To create a signature one needs a private key. If a recipient of the signature needs to verify the signature, he/she needs a public key that corresponds to the private key that was used to create the signature. Public and private keys are related to the field of public key cryptography. Public and private keys can also be used for purposes other than signatures, for example, for encryption and decryption. Public and private keys are related to the field of asymmetric cryptography.

One way to create public and private key pairs is to use the mathematical concept of a group. A group is a set of elements together with an operation to join two elements. For convenience, in equations the joining operation is noted as "+" and referred to as "an addition". A person skilled in the art will know that the operation may need additional constraints.

Given an integer "d" and an element "Q" in a group, there can be an operation that combines these two entities, in a manner that has some of the properties of a multiplication. Such a combination can, for example, be accomplished by repeating the addition a number of times, the number given by the integer "d", this is sometimes called a

scalar multiplication. More generally a person skilled in the art will recognize that such a combination can, e.g., be produced using an action of a cyclic second group, on the group that contains Q, see, e.g., "Abstract Algebra" by David S. Dummit and Richard M. Foote.

For example, in the case of an elliptic group such a combination created using repeated additions is called a "point-multiplication". A person skilled in the art will recognize that many algorithms are available for doing this kind of combination, for example, the 'double and add' method. The point-multiplication is used to illustrate the invention, but only by way of example.

It is known that a group can have a subset that itself is also a group. Such a subset is called a "subgroup". A person skilled in the art will know that many groups and subgroups are suitable for creating cryptographic objects and operations, such as public keys, private keys, shared keys, signatures, creation of a signature and verification of a signature.

Suitable groups include, for example, elliptic groups using as joining the addition of points, or a multiplicative group modulo a number where the joining is multiplication modulo the number, or hyper-elliptic groups. Suitable subgroups include, for example, the subgroup generated by a single element.

One way to use a group to create public and private keys is to have the public key represent an element in the group and to have the private key represent an integer.

A group has an associated integer, referred to as the "order of the group". The order of a group is equal to the number of elements in the group. Likewise, a subgroup has an associated integer, referred to as the "order of the subgroup". The order of the subgroup is equal to the number of elements in the subgroup.

A group can have one or more elements that may need to be avoided for some applications. Such elements are referred to herein as "designated elements". For example, for an elliptic group the point at infinity can be a designated element.

A group and subgroup have associated with them an integer "h", called the "cofactor". A cofactor is equal to the order of the group divided by the order of the subgroup.

The field of cryptography that is based on elliptic groups is called Elliptic Curve Cryptography (ECC). ECC has lately grown in popularity for different (embedded) applications because of its security, speed and memory requirements. For example, it was adopted as a standard for the USA government by the National Institute of Standards and Technology.

An elliptic group comprises the points on an elliptic curve. An elliptic curve is a mathematical concept. Persons skilled in the art will appreciate that elliptic curves can be used over many types of ground fields, such as the Galois field with a number of elements that is a prime number or a field of characteristic two, such as the Galois field with a number of elements that is a power of 2, or a field of characteristic three, or a field of any other characteristic. Elliptic curve cryptosystems are characterized in that public keys correspond to points on an elliptic curve.

Descriptions of ECC, including elliptic groups and the related addition and point-multiplication can be found in many references, e.g., D.Hankerson, A.Menezes, S.vanstone, “Guide to Elliptic Curve Cryptography”, Springer Verlag 2004.

For security it is important that a user of a public key has assurance that the public key is valid and corresponds to the private key of the purported sender of a signature.

The usual way to transfer public keys securely and conveniently is in the form of a certificate. The most widely used certificates nowadays are those according to the X.509 standard. For background on the X.509 standard see, e.g., Housley, R., W. Ford, W. Polk and D. Solo, "Internet X.509 Public Key Infrastructure: Certificate and CRL Profile", RFC 3280, April 2002. Some applications, however, use certificates with a proprietary, non-standard format that is different from the X.509 format.

A conventional certificate, such as an X.509 certificate, typically comprises a transported public key and a certificate signature. In 2002 a new form of certificates, the so-called implicit certificates, were proposed. An implicit certificate comprises reconstruction data. The reconstruction data is not equal to the transported public key, but the transported public key can be reconstructed from the reconstruction data.

Implicit certificates have the advantage that they are shorter in bytes than conventional certificates, such as X.509 certificates. Also it can be faster to process implicit certificates than conventional certificates, such as X.509 certificates.

The first implicit certificates scheme was published as: D.Brown, R.Gallant, S.Vanstone, "Provably secure Implicit Certificate Schemes", Financial Cryptography 2001, LNCS 2339, pp.156-165, Springer, 2002. Also patents were granted that describe implicit certificates: EP 1 066 699 "Method of generating a public key in a secure digital communication system and implicit certificate", and US 6,792,530 "Implicit certificate scheme". An implementation adapted for use with elliptic curve cryptography was published as SEC 4: "Elliptic Curve Cryptography", Standards for Efficient Cryptography, version 1.1r1, Certicom Research, June 9, 2006. Said document will be referred to herein as [SEC4].

The algorithm, which a verifier uses to reconstruct a transported public key from an implicit certificate, typically takes inputs from two parties: a sender and a trusted party. It is not an interactive algorithm between two or more parties. Rather, once a verifier has all the required inputs he/she can execute the algorithm without further interaction. For a successful reconstruction of the transported public key it is not necessary for the verifier to send data to the sender or to the trusted party.

After the verifier has reconstructed the transported public key the verifier typically does not have a corresponding private key. The sender typically does have a private key corresponding to the transported public key. The private key can be used to create a signature, the corresponding public key can be used to verify said signature.

If the reconstruction is done by a second verifier the result will be the same transported public key. The identity of a verifier has no influence on the outcome of the reconstruction.

Implicit certificates are typically used in electronic communication systems, such as e-mail. In that context, certificates enable signatures. Also implicit certificates can be used to prove the authenticity of a web page to a browser, for example, using the https protocol, such as is used on the Internet. If a web browser receives a web page with a

certificate that cannot be verified, that browser may disable the rendering of the page. Also implicit certificates are used in smartcards, or in so-called smart badges. In that context, certificates can be used for authorization purposes, such as for log-on to a computer, or to a computer network, or for physical access to an area, such as access to a building.

When using certificates in a secure communication system a user, who needs to verify a signature attached to a document or other digital file, must be cautious that somebody may try to present him with a tampered implicit certificate. Therefore, it is advisable that the user verify the implicit certificate. One aspect of this verification includes a validation of an intermediate public key.

For a public key Q, a group and a subgroup, the validation of Q can comprise any of the following steps:

-Verifying that the public key Q is an element of the group, for example, by checking that Q has some predetermined form.

-Verifying that the public key Q is not equal to a designated element.

-Verifying that the public key Q is an element of the subgroup.

If the validation comprises the step of checking that the public key Q is an element of the subgroup, the validation is called *full validation*. If the validation does not comprise this step, the validation is called *partial validation*. It is known that partial validation is more efficient than full validation, with respect to computing time.

A typical way, in which it can be checked that the public key Q is an element of the subgroup, is to combine the order of the subgroup with the public key Q, and to check that the result is a designated element of the group.

It is known that full validation in the case of ECC typically takes the following form:

-Verifying that the public key corresponds to a point on the elliptic curve

-Checking that the public key is not equal to a designated element;

-Verifying that the result of the point-multiplication of the order of the subgroup and the public key is equal to the designated element on the elliptic curve.

The partial validation can make use of system information. System information comprises configuration parameters of the cryptographic algorithms used in the method. The system information comprises the parameters of the underlying cryptographic system, e.g., what group or subgroup is used. The system information may comprise a generator of a used subgroup. The system information may also comprise additional parameters that are needed for performing the combination or joining of values. The system information may also comprise a designated element.

It is known that there exist algorithms that need full validation.

Omitting validation can result in breaches of security, e.g., a failure to deliver secure communication. An example of a security breach is that the verifier might be led to believe that an implicit certificate is valid, whereas, in fact, it is not. Examples of security breaches caused by omitting to check the validity of the entities used include the so-called Pohlig-Hellman attack, such as described, for example, in S.C. Pohlig and M.E. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance", IEEE Transactions on Information Theory, 24, pages 106–110, 1978. As a further example, omitting to check that some entities lie in a correct subgroup may give rise to a small subgroup attack, for example, such as described in D. Johnson, "Diffie-Hellman Key Agreement Small Subgroup Attack", a Contribution to X9F1 by Certicom, July 16, 1996; or in D. Jungnickel, "Finite Fields: Structure and Arithmetics", B.I.Wissenschaftsverlag, Mannheim, 1993.

It is also known that most algorithms requiring validation are only secure if full validation is done. There exist an algorithm that can be modified to use partial validation instead of full validation while still remaining secure: the Diffie-Hellman key agreement algorithm. Descriptions of this algorithm and its variant can be found in: SEC 1: "Elliptic Curve Cryptography", Standards for Efficient Cryptography, version 1.0, Certicom Research, September 20, 2000, referred to herein as [SEC1]. The Diffie-Hellman key agreement algorithm, adapted in order to use the cofactor, is referred to as the "cofactor Diffie-Hellman key agreement algorithm".

A key agreement algorithm is an algorithm in which two parties interactively determine a negotiated key. Typically both parties need to send data to each other. Both

parties need to execute an algorithm in order for both parties to be in possession of the same negotiated key.

A party that executes a key agreement algorithm typically only needs input from one other party. After both parties have executed the key agreement algorithm, both parties are in possession of the same negotiated key.

The negotiated key cannot be used as a public or private key. For the negotiated key either no corresponding private key exists or normal use of the algorithm would result in neither party knowing the corresponding private key.

In a key agreement algorithm neither party can determine the outcome of the negotiation. Instead, both parties can influence the outcome. If one of the parties subsequently executes a key agreement algorithm with a different second party, the resulting negotiated key will be different. A key agreement algorithm cannot be used to transport a key. The negotiated key thus created is called a "shared secret key". A shared secret key can, e.g., be used to encrypt a data communication between the two parties. The shared secret key can be used in the field of symmetric cryptography.

In the unmodified Diffie-Hellman key agreement algorithm as described in [SEC1], full validation is done for an entity Q, which is a point on an elliptic curve. Elsewhere in the algorithm the entity Q is combined with an integer d using a point-multiplication d·Q. It is possible to replace the full validation of the entity Q by partial validation. However, replacing the full validation by partial validation would make the algorithm insecure. To compensate for this, a so-called cofactor h needs to be introduced in the equations. In particular, said point-multiplication d·Q, being a product of two entities, needs to be replaced by h·d·Q, being a product of three entities. The formula h·d·Q can be obtained by two point-multiplications, e.g., first d·Q, the result of which thereafter point-multiplied with h. alternatively, first the integer product h·d can be calculated, the result of which is thereafter point-multiplied with Q.

In [SEC1] the MQV key agreement algorithm is described. It is another key agreement algorithm that uses a cofactor. Instead of the Diffie-Hellman algorithms the MQV key agreement algorithm was designed from the outset to use a cofactor. The situation with

the MQV key agreement algorithm is otherwise similar to that with co-factor Diffie-Hellman described above.

In [SEC4] an implicit certificate system is presented. In all pertinent algorithms the full validation method is used. In the algorithm to reconstruct the transported public key from an implicit certificate, a full validation is done for an entity Q, which is a point on an elliptic curve. Later the entity Q is combined with an integer e and a public key W in a formula $e \cdot Q + W$, an addition of the result of a point-multiplication to entity W.

SUMMARY OF THE INVENTION

The inventors have recognized that a problem with the current state of the art lies in the necessary full validation of an intermediate key during a secure reconstruction of a transported public key from an implicit certificate.

Partial validation schemes enjoy a computational advantage over full validation schemes which require 'fully' valid public keys. The computational advantage stems from the fact that public key partial validation is more efficient than public key full validation. Especially when using implicit certificates on constrained hardware, such as mobile phones, palmtop computers, personal digital assistants (PDAs) or smart cards, full validation is a problem, as the extra step is rather time-consuming in such a context.

The prior art does not suggest to replace the full validation by partial validation, rather the prior art teaches away, since it is known that partial validation can lead to security problems.

The invention is defined by the independent claims. Dependent claims describe advantageous implementations.

Accordingly, a first aspect of the invention is that the transported public key can be reconstructed in a manner that is faster than disclosed in [SEC4] by replacing full validation by partial validation.

Therefore the inventors propose a method according to claim 1.

In claim 1 the reconstruction uses a cryptographic algorithm that reconstructs the transported public key from the entity information, the reconstruction data, and the authoritative public key. For example, the algorithm of Section 5 in [SEC4] can be used.

Note that the steps in a method of the invention need not be executed in the order given. The only requirement imposed on the order is that the entity information, and the authoritative public key are available before they are needed in the reconstruction.

Note that the system can make use of system information.

There are various ways to obtain the authoritative public key. Ways to obtain include, for example, retrieving the authoritative public key from another digital system, for example, using the Internet. Or the obtaining can be done by having another party send the authoritative public key, for example, using the Internet, or using electronic mail, or using a storage device that can be physically transported, etc. Obtaining the authoritative public key can be done by looking up in a database, locally or at a remote site. Obtaining the authoritative public key can be done by reconstructing the authoritative public key from other data. Obtaining the authoritative public key also includes retrieving the authoritative public key already available by being built-in into a device.

Furthermore, it is not clear from the prior art how the algorithm for reconstructing the transported public key could be modified to replace the full validation by partial validation, while keeping an adequate security level. Other algorithms, such as the Diffie-Hellman key agreement algorithm, for which it is known how to replace the full validation by partial validation do not teach how to introduce the cofactor into the more complicated equations needed for implicit certificates. A priori it is unclear from the prior art if a cofactor can be introduced in the equations in a meaningful way at all. The inventors have found that a meaningful use of the cofactor in an implicit certificate scenario is indeed possible, and propose a way to accomplish this.

Accordingly, a second aspect of the invention is that the transported public key can be reconstructed in a manner that is still faster than disclosed in [SEC4], while introducing the cofactor into the computations. Adopting the cofactor in the reconstruction

allows the reconstruction to be done securely, for example, using the embodiments of claim 3, 4, or 5.

Therefore the inventors propose a method as in claim 2.

The aggregating can be done by, e.g., combining the cofactor with the reconstruction data. The aggregating can also be done by, e.g., by first multiplying the cofactor with the entity information and then combining with the reconstruction data.

An advantageous embodiment, keeping an adequate security level, is proposed in claim 3. Note that the joining could be performed by addition in a group. The combining could be done by point-multiplication, which could be performed by repeated additions. Other constructions of combining or joining elements, such as using polynomials or functions, may be possible depending on the nature of the underlying group used.

It should be verified in the case of claim 3 that the reconstructed public key is not equal to the authoritative key. There exists many ways in which this can be done. For example, one could compare a binary representation of the reconstructed transported public key to a binary representation of the authoritative key. Alternatively, one could check that the combination of the cofactor with the reconstruction data is not equal to a designated element. Alternatively, one could check that the combination of the reconstruction data with the product of the entity information and the cofactor is not equal to a designated element. The last option could be integrated in the reconstruction itself.

Another advantageous embodiment, also keeping an adequate security level, is proposed in claim 4. A method for reconstructing a transported public key from an implicit certificate that uses partial validation can also be made secure by introducing an extra check. This extended method has the additional advantage that it would be compatible with existing [SEC4] implementations, but can still benefit from the computation advantages offered by partial evaluation.

The combination of claim 4 could also be produced during reconstruction. Therefore the inventors propose a method as in claim 5.

Partial validation can be particularly advantageous in combination with ECC. ECC is often applied in devices with constrained resources, such as mobile communication devices. Since ECC is faster and than most other cryptographic algorithms and works on smaller cryptographic objects, such as keys. By combining the computational advantages of ECC with those of the invention an additional saving is achieved making the method well suited for devices with constrained resources.

Therefore the inventors propose a method as in claim 6.

When using ECC, joining operations are conveniently done using additions, and combining operations are conveniently done as point-multiplications. A person skilled in the art knows how to add two elements or how to point-multiply an integer and an element if those elements correspond to points on an elliptic curve.

Therefore the inventors propose methods as in claim 7 and claim 8.

The methods of the invention can be used advantageously in systems, wherein the implicit certificate is linked to the identity of the sender. Therefore, according to the present invention, the processing of the reconstruction data could operate on further information.

Therefore the inventors propose a method as in claim 9.

Note that the further information can be obtained in similar ways as the authoritative public key, described above. Information identifying a sender could also be wholly or partly contained in the content of the implicit certificate.

The inventors have recognized that the partial validation technique used can be applied for any choice of the mathematical function. However, it is advantageous if the mathematical function has cryptographic properties. Therefore, according to the present invention, the mathematical function used in an embodiment of the method, comprises a secure hash function.

Therefore the inventors propose a method as in claim 10.

The method can be executed using a data processing system, e.g., a mobile phone or other network enabled device, or a desktop computer. The data processing system can be configured to use the method using software, or the data processing system may comprise hardware, such as electronic circuits that are configured to perform the method, or the data processing system can be controlled using software, or the data processing system may comprise a combination of possibly dedicated hardware and software to implement the method of the invention. A single device could comprise such a data processing system. On the other hand such a data processing system could also comprise a plurality of separate devices, i.e. the data processing system is a distributed data processing system. Therefore the inventors propose a system as in claim 11 and 12.

Similarly the method can be implemented using software.

Therefore the inventors propose software as in claim 13.

It is convenient to have a provider system provide the software. For example, a server provides the software by making it available for download, or for streaming, e.g., streaming of control code, via a data network, such as the Internet. Or, as a further example, the provider system comprises a storage unit storing the software from which later the software can be provided by reading from the storage unit. Or the provider system comprises a processing device for enabling such providing, including downloading, streaming or storing.

Therefore the inventors propose a provider system as in claim 14.

It is convenient to use a providing method for providing the software.

Therefore the inventors propose a providing method as in claim 15.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is explained in further detail, by way of example and with reference to the accompanying drawing, wherein:

Fig.1 is a block diagram showing how the invention could be used in a larger communication system.

Fig.2 is a block diagram illustrating a preferred embodiment of the invention.

Fig.3 is a block diagram illustrating a preferred embodiment of partial validation for an elliptic curve based system.

Fig.4. is a block diagram illustrating an alternate embodiment.

Throughout the Figures, similar or corresponding features are indicated by same reference numerals.

DETAILED DESCRIPTION OF THE EMBODIMENTS

Legend

Reference numeral (102) denotes a trusted party;

Reference numeral (104) denotes a sender;

Reference numeral (106) denotes the trusted party (102) sending an implicit certificate (I,B) and private key reconstruction data *s* ;

Reference numeral (108) denotes the sender (104) sending the implicit certificate (I,B) to a verifier (110);

Reference numeral (110) denotes the verifier;

Reference numeral (112) denotes the trusted party sending an authoritative key to the verifier (110). Note that alternatively the verifier (110) could also obtain the authoritative key from some other source. Alternatively it could be looked up in a database.

Reference numeral (200) denotes the claimed method.

Reference numeral (201) denotes an implicit certificate;

Reference numeral (202) denotes a content of the implicit certificate (201), wherein said content includes identifying information;

Reference numeral (204) denotes a mathematical function;

Reference numeral (206) an integer multiplication;

Reference numeral (208) denotes a content of the implicit certificate (201). The content is reconstruction data;

Reference numeral (210) denotes a partial validation done on reconstruction data (208);

Reference numeral (212) denotes a point-multiplication done on reconstruction data (208) and an integer;

Reference numeral (214) denotes an authoritative public key;

Reference numeral (216) denotes an addition. Note that in a preferred embodiment this addition operates on two points on an elliptic curve;
Reference numeral (218) denotes a transported public key, the intended result of the method;
Reference numeral (220) denotes an entity information, the result of the mathematical function (204);
Reference numeral (222) is a cofactor that is associated with the particular group and subgroup used.
Reference numeral (224) denotes a check whether the transported public key differs from the authoritative public key.
Reference numeral (226) denotes a reporting of a failure.
Reference numeral (302) denotes a check whether the reconstruction data (208) differs from a designated element associated with the group;
Reference numeral (304) denotes a check whether reconstruction data (208) is a point on the elliptic curve
Reference numeral (400) denotes the additional check for increased security;
Reference numeral (402) denotes a point-multiplication;
Reference numeral (404) denotes a check whether the result from (402) is a designated element.

While this invention is susceptible of embodiment in many different forms, there is shown in the drawings and will herein be described in detail one or more specific embodiments, with the understanding that the present disclosure is to be considered as exemplary of the principles of the invention and not intended to limit the invention to the specific embodiments shown and described.

For convenience, the method of reconstructing the transported public key (218) is described using elliptic curve arithmetic, where the joining operation associated with the group is indicated as addition. However, these schemes are equally implementable in cryptosystems based on other groups. Note that sometimes the joining operation associated with the group is indicated as multiplicatively. Let “E” be the elliptic curve used. The public keys used below correspond to points on this elliptic curve. For convenience, it is assumed that a specific public key directly represents a specific point on the curve. However, a person skilled in the art will appreciate that more elaborate constructions are possible. For example,

instead of working on a direct representation of the coordinates of the point, a more efficient representation of points on the curve is also possible, such representations could include using compressed representation or using projective coordinates or normalized coordinates, etc.

It is first described how the method (200) could be used in a larger system, such as a secure communication system, by three entities, a verifier (110), a sender (104) and a trusted party (102).

Trusted party (102) creates an implicit certificate (201) and a corresponding private key reconstruction data "s". Trusted party (102) sends (106) both to the sender (104). If the sender (104) needs a private key, for example, to create a signature for a document, he/she uses the implicit certificate (201) and the corresponding private key reconstruction data "s" to reconstruct a private key. Using the private key the sender (104) can create a signature for the document. The sender (104) sends (108) the document (not shown), the signature (not shown) and his implicit certificate (201) to the verifier (110).

If the verifier (110) needs a public key, for example, to verify the signature, he/she needs to reconstruct the transported public key (218) from the implicit certificate (201).

Trusted party (102) has an authoritative public key (214) "W", which is sent (112) to the verifier (110). The implicit certificate (201) comprises of information "I" (202) identifying the sender (104) and of a reconstruction data "B" (208). The reconstruction data "B" (208) is not the transported public key (218). Note that in the case of the preferred embodiments below, reconstruction data "B" (208) also corresponds to a point on an elliptic curve.

In order to reconstruct the transported public key (218) the verifier (110) performs the following steps:

1. According to a mathematical function "F = F (I, B)" (204), the verifier (110) calculates an entity information "e" (220). For example, the function (204) could concatenate "I" and "B" and use that concatenation as an input to a secure hash function, for example, the

Secure Hash Algorithm (SHA-1). It is noted that if the output of function "F" is not suitable for use in the remainder of the algorithm it could be modified. For example, if the entity information (220) is larger than a certain number the entity information (220) could be truncated.

2. Partially Validate (210) reconstruction data "B" (208) by performing the following steps:

a. Verify that reconstruction data "B" (208) is not a designated element. In particular, check that reconstruction data "B" (208) is not the point at infinity (302).

b. Verify that reconstruction data "B" (208) is a point on "E" (304).

3. The transported public key (218) can now be reconstructed from the entity information "e" (220), a cofactor "h" (222), the reconstruction data "B" and an authoritative public key "W" (214) by performing the computation: $e \cdot h \cdot B + W$ as shown in (200). This computation comprises the following steps:

a. First a cofactor (222) is multiplied with the entity information (220). This multiplication could use regular arithmetic on integers. However, this step could also be performed using modular arithmetic.

b. The result of the multiplication of the cofactor (222) and the entity information (220) is point-multiplied (212) with the reconstruction data (208).

c. The authoritative public key (214) is added (216) to the result of the point-multiplication done in step b). Here the addition is done for points on an elliptic curve.

4. Check that the result of step 3c is different from W (244), if not report a failure (226)

5. The result of step 3c is the reconstructed transported public key

The failure could, for example, be reported to a user of a system that comprises the method. Or the failure could, for example, be reported to an application that comprises the method. As a result of the reporting an action may be blocked or prohibited.

In an alternative to the first embodiment the final step 4) is skipped. Instead a new step 4 is introduced:

4) Check that the result of step 3b) (212) is not a designated element. If the result of step 3b) (212) is a designated element then report a failure.

In step 3b the entity e·h·B is used. Instead the check can also be done on the part h·B, that is, check that h·B is not a designated point.

In another embodiment the reconstruction can be done, e.g., as in Section 5 of [SEC4], except that an additional step is needed:

Checking (400) that the cofactor "h" (222) point-multiplied (402) with the reconstruction data "B" (208) is not a point at infinity (404).

The present invention, as described in embodiments herein, may be implemented using a programmed processor executing programming instructions that are broadly described above in flow chart form that can be stored on any suitable electronic storage medium. However, those skilled in the art will appreciate that the processes described above can be implemented in any number of variations and in many suitable programming languages without departing from the present invention. For example, the order of certain operations carried out can often be varied, additional operations can be added or operations can be deleted without departing from the invention. Error trapping, enhancements and variations can be added without departing from the present invention. Such variations are contemplated and considered equivalent.

The present invention could be implemented using special purpose hardware and/or dedicated processors. Similarly, general purpose computers, microprocessor based computers, digital signal processors, microcontrollers, dedicated processors, custom circuits, ASICS and/or dedicated hard wired logic may be used to construct alternative equivalent embodiments of the present invention.

Those skilled in the art will appreciate that the program steps and associated data used to implement the embodiments described above can be implemented using disc storage as well as other forms of storage, such as, for example, Read Only Memory (ROM) devices, Random Access Memory (RAM) devices, optical storage elements, magnetic storage elements, magneto-optical storage elements, flash memory and/or other equivalent storage technologies without departing from the present invention. Such alternative storage devices should be considered equivalents.

While the invention has been described in conjunction with specific embodiments, it is evident that many alternatives, modifications, permutations and variations will become apparent to those of ordinary skill in the art in light of the foregoing description. Accordingly, it is intended that the present invention embrace all such alternatives, modifications and variations as fall within the scope of the appended claims.

CLAIMS:

1. A method (200) for reconstructing a transported public key (218) from an implicit certificate (201), wherein the implicit certificate (201) comprises reconstruction data (208) for reconstructing the transported public key, said method comprising the steps of:

- obtaining an authoritative public key;
- processing the implicit certificate (201) in accordance with a mathematical function (204) to derive an entity information (220);
- carrying out a partial validation (210) of said reconstruction data (208);
- reconstructing the transported public key from the reconstruction data (208), the entity information (220), and the authoritative public key (214);

wherein the method is executable at a data processing system.

2. The method of claim 1, wherein the reconstructing uses a group-based algorithm and wherein the method further comprises:

- a first representation of a group with an associated procedure for joining two elements from the group,
- a second representation of a subgroup of the group,
- a cofactor (222) with respect to the group and the subgroup,
- a procedure for combining an integer with an element from the group, wherein
- the reconstruction data is a specific element of the group, and wherein the reconstructing comprises aggregating the cofactor (222) with the reconstruction data (208).

3. The method of claim 2, wherein the aggregating comprises:

- producing a product by multiplying (206) said cofactor (222) with said entity information (220);
- producing a combination by combining (216) said product with the reconstruction data (208);

and wherein the reconstruction comprises:

- joining the combination with the authoritative public key (214);

and wherein it is verified that the reconstructed public key is not equal to the authoritative key (224).

4. The method of claim 1, wherein the method further comprises:

- a first representation of a group with an associated procedure for joining two elements from the group,
- a second representation of a subgroup of the group,
- a cofactor (222) with respect to the group and the subgroup,
- a procedure for combining an integer with an element from the group,
- a designated element of the group,

and wherein the method further comprises additional steps

- producing a combination by combining the cofactor (222) with the reconstruction data (208)
- checking (404) that the combination differs from the designated element.

5. The method of claim 2, wherein the method further comprises:

- a designated element of the group,

and wherein the aggregating comprises:

- producing a combination by combining the cofactor (222) with the reconstruction data (208)

and wherein the method further comprises:

- checking (404) that the combination differs from the designated element.

6. The method of claim 1, 2, 3, 4 or 5, wherein the reconstruction data (208) corresponds to a first point on an elliptic curve, and wherein the authoritative public key (214) corresponds to a second point on the elliptic curve, and wherein the transported public key (218) corresponds to a third point on the elliptic curve.

7. The method of claim 6, in so far as it refers to claim 3, wherein combining is done by point-multiplication and joining is done by addition.

8. The method of claim 6, in so far as it refers to claim 4 or 5, wherein combining is done by point-multiplication.

9. The method specified by any of claims 1 to 8, wherein the processing comprises:

- obtaining further information (202) representative of an identity of a sender (104) of the implicit certificate; and wherein said further information and the implicit certificate (201) are processed in accordance with the mathematical function (204) to derive the entity information (220).

10. The method specified by any of claims 1 to 9, wherein the mathematical function (204) comprises a secure hash function.

11. A data processing system operable to reconstruct the transported public key (218) from an implicit certificate (201); wherein the data processing system is configured to use the method of any of claims 1 to 10.

12. The data processing system of claim 11 accommodated in a mobile network-enabled device.

13. Software for configuring a data processing system to be operable to reconstruct the transported public key (218) from an implicit certificate (201) using the method of any of claims 1 to 10.

14. A providing system configured to provide the software of claim 13.

15. A providing method arranged to provide the software of claim 13; wherein the method is executable at a providing system as in claim 14.

1/3

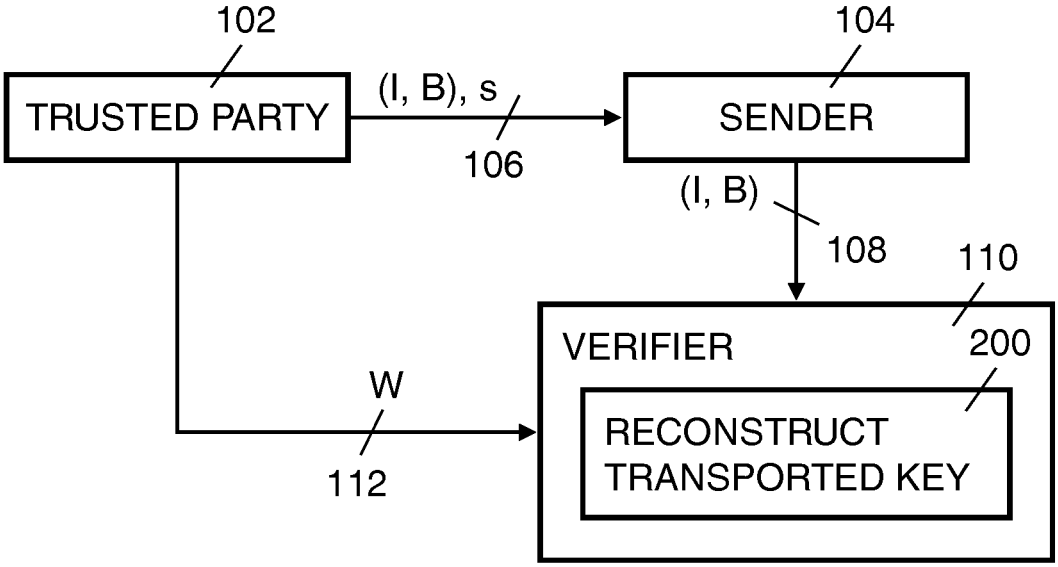
102
TRUSTED PARTY
(I, B), s
106
104
SENDER
(I, B)
108
110
VERIFIER
200
RECONSTRUCT TRANSPORTED KEY
W
112

FIG. 1

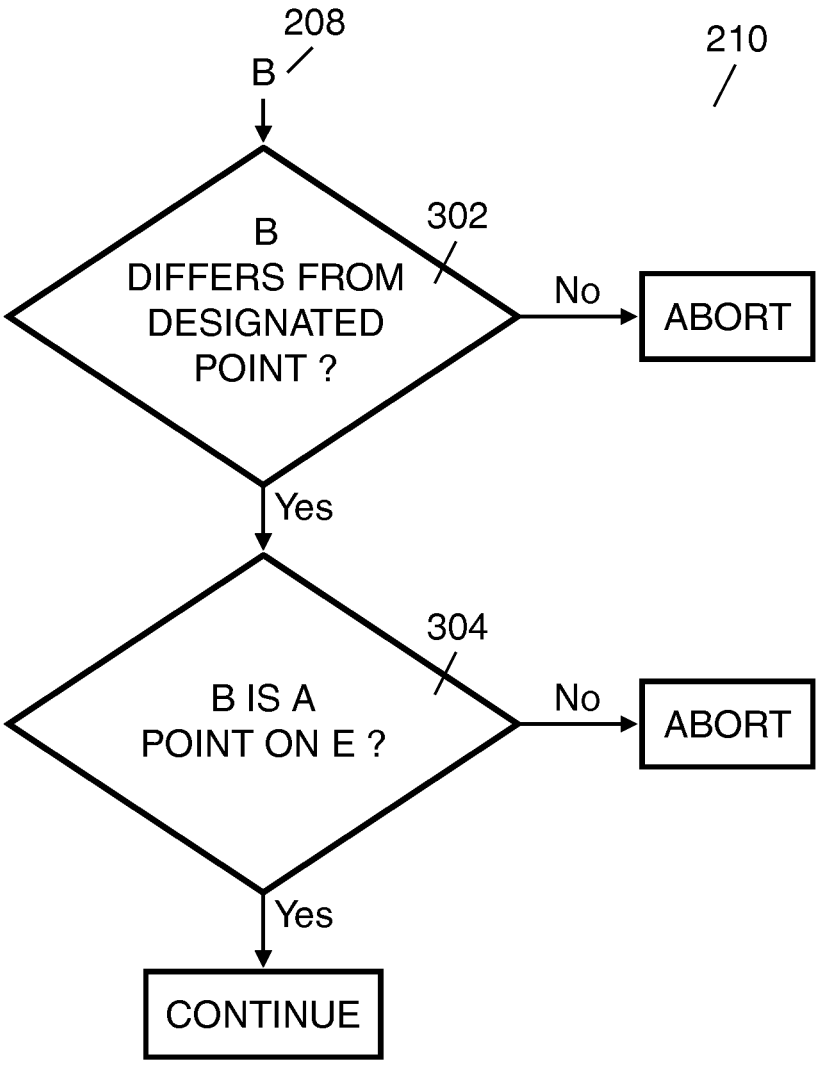
208
B
210
B DIFFERS FROM DESIGNATED POINT ?
302
No
ABORT
Yes
B IS A POINT ON E ?
304
No
ABORT
Yes
CONTINUE

FIG. 3

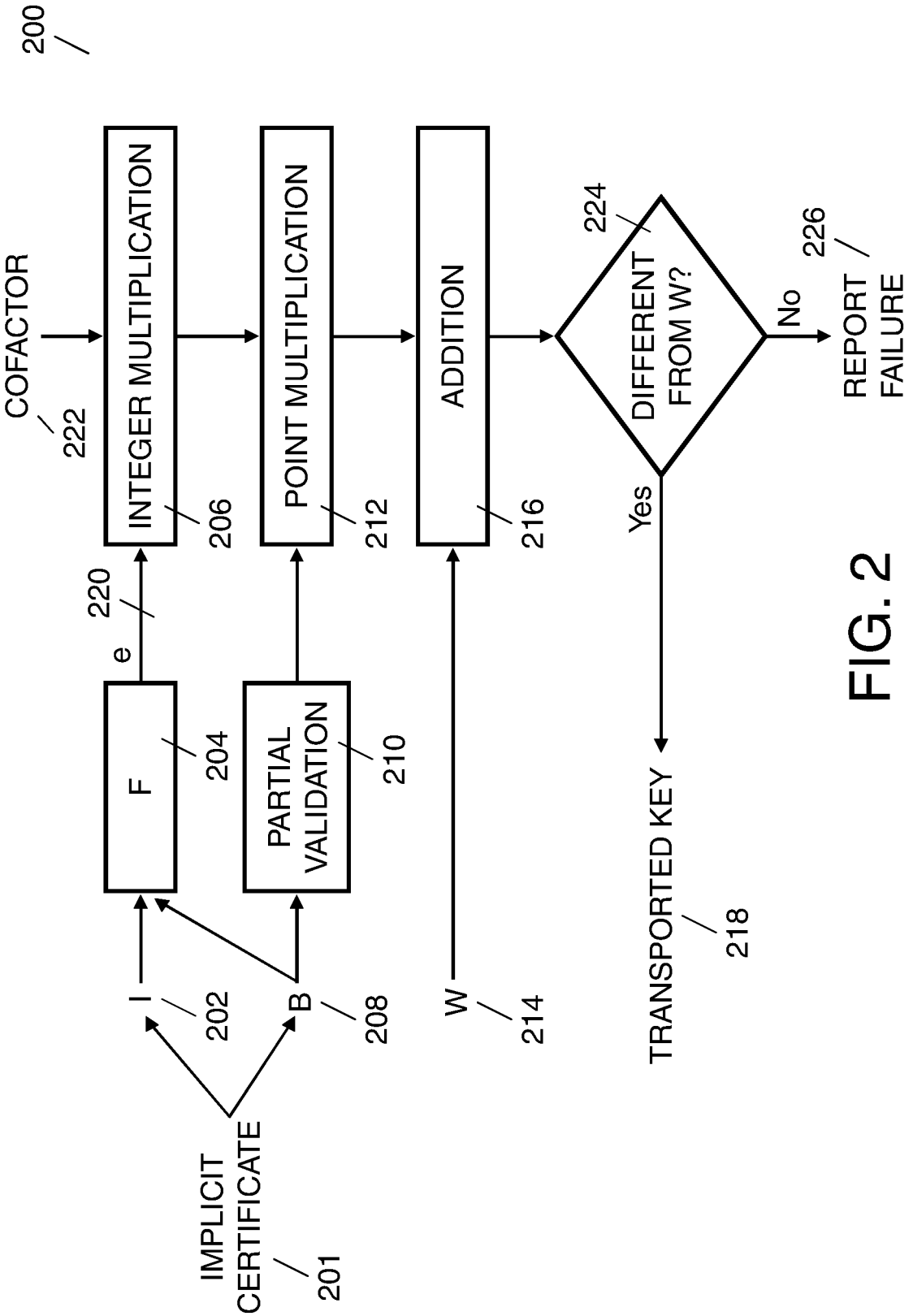
200
COFACTOR
222
INTEGER MULTIPLICATION
206
POINT MULTIPLICATION
212
ADDITION
216
DIFFERENT FROM W?
224
No
226
REPORT FAILURE
Yes
TRANSPORTED KEY
218
220
e
F
204
PARTIAL VALIDATION
210
I
202
B
208
W
214
IMPLICIT CERTIFICATE
201

FIG. 2

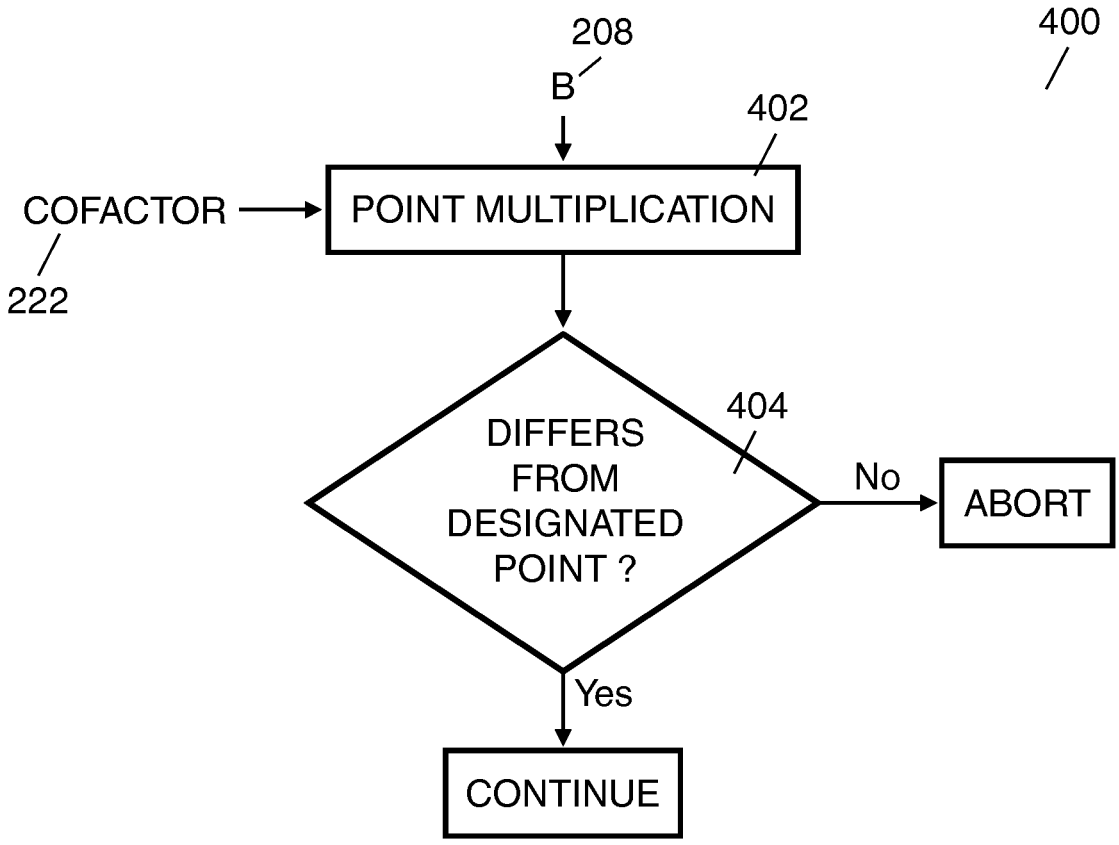
208
B
400
402
COFACTOR
POINT MULTIPLICATION
222
DIFFERS FROM DESIGNATED POINT ?
404
No
ABORT
Yes
CONTINUE

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2008/055577

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/30 H04L9/32 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC, WPI Data, PAJ, 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	BROWN D R L ET AL: "Provably secure implicit certificate schemes" FINANCIAL CRYPTOGRAPHY. 5TH INTERNATIONAL CONFERENCE, FC 2001. PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOL.2339) SPRINGER-VERLAG BERLIN, GERMANY, [Online] 2002, pages 156-165, XP002524293 ISBN: 3-540-44079-8 Retrieved from the Internet: URL:http://www.springerlink.com/content/74451264h287wp17/fulltext.pdf> the whole document ----- -/--	1-15

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

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 April 2009	08/05/2009

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/IB2008/055577

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BILLY BOB BRUMLEY ET AL: "Differential Properties of Elliptic Curves and Blind Signatures" INFORMATION SECURITY; [LECTURE NOTES IN COMPUTER SCIENCE], SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, vol. 4779, 9 October 2007 (2007-10-09), pages 376-389, XP019101588 ISBN: 978-3-540-75495-4 paragraphs [0004], [0005], [000A]	1-15
E	WO 2009/009869 A (CERTICOM CORP [CA]; VANSTONE SCOTT A [CA]) 22 January 2009 (2009-01-22) abstract paragraph [0022] - paragraph [0035]	1-15
A,P	WO 2008/058388 A (CERTICOM CORP [CA]; STRUIK MARINUS [CA]) 22 May 2008 (2008-05-22) paragraph [0020] - paragraph [0049]	1-15
A	WO 99/49612 A (CERTICOM CORP [CA]; QU MINGHUA [CA]; VANSTONE SCOTT A [CA]) 30 September 1999 (1999-09-30) page 2, line 29 - page 13, line 19	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2008/055577

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2009009869 A	22-01-2009	US 2009046852 A1	19-02-2009
WO 2008058388 A	22-05-2008	NONE	
WO 9949612 A	30-09-1999	AU 758044 B2	13-03-2003
		AU 2823599 A	18-10-1999
		CA 2235359 A1	23-09-1999
		DE 69918818 D1	26-08-2004
		DE 69918818 T2	25-08-2005
		EP 1066699 A1	10-01-2001
		JP 2002508529 T	19-03-2002
		US 2009041238 A1	12-02-2009
		US 6792530 B1	14-09-2004