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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 April 2012 (19.04.2012)

PCT

(10) International Publication Number
WO 2012/049630 A1

(51) International Patent Classification:
H04L 9/32 (2006.01) *H04L 9/00* (2006.01)
H04L 12/58 (2006.01)

(21) International Application Number:
PCT/IB2011/054490

(22) International Filing Date:
11 October 2011 (11.10.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/393,730 15 October 2010 (15.10.2010) US

(71) Applicants *(for all designated States except US)*: **CERTICOM CORP.** [CA/CA]; 4701 Tahoe Blvd., Building A, Mississauga, Ontario L4W 0B5 (CA). **CERTICOM (U.S.) LIMITED** [US/US]; The Corporation Trust Center, 1209 Orange Street, Wilmington, Delaware 19801 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CAMPAGNA, Matthew John** [US/US]; 264 Old Sib Road, Ridgefield, Connecticut 06877 (US). **BROWN, Daniel Richard L.** [CA/CA]; 4701 Tahoe Blvd., Ext. 14157, Mississauga, Ontario L4W 0B5 (CA). **ZAVERUCHA, Gregory Marc** [CA/CA]; 4701 Tahoe Blvd, Ext. 15460, Mississauga, Ontario L4W 0B5 (CA).

(74) Agents: **INTEGRAL IP** et al.; Suite 300, 1370 Don Mills Road, Toronto, Ontario M3B 3N7 (CA).

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

[Continued on next page]

(54) Title: AUTHENTICATED ENCRYPTION FOR DIGITAL SIGNATURES WITH MESSAGE RECOVERY

(57) Abstract: A framework is proposed for authenticated encryption for digital signatures with message recovery whereby authentication is achieved without a redundancy requirement. The finite cyclic group signature scheme is modified through the use of authenticated encryption, thereby enabling authentication using a message authentication code (1028). The authenticated encryption may be performed within a single function or as two separate functions. The authenticated encryption may also be applied to associated data in the message (104) to be signed.

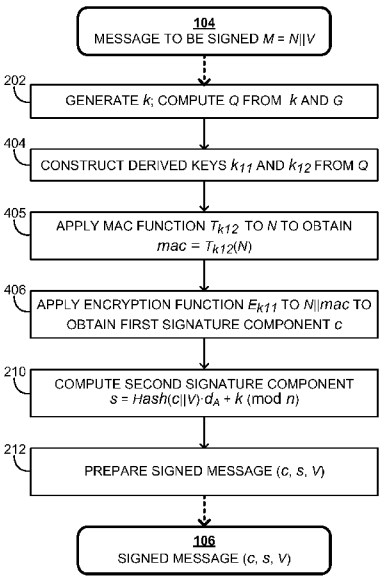

FIG. 4

WO 2012/049630 A1

(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, MD, 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))*

AUTHENTICATED ENCRYPTION FOR DIGITAL SIGNATURES WITH MESSAGE RECOVERY

TECHNICAL FIELD

[0001] The technology described herein relates generally to cryptographic signatures, and particularly to the generation and use of cryptographic signatures with message recovery.

BACKGROUND

[0002] Traditional cryptographic signature schemes can be used to provide (1) assurance of the identity of the signer, and (2) assurance that a received message has not been altered during transmission. Typically, a signer generates an unforgeable signature on a message, such that a recipient may subsequently verify the signature for authentication of the signer's identity and the origin of the message.

[0003] In general, smaller-sized cryptographic values are desirable because they may reduce storage and transmission requirements. Signature schemes which are based on the intractability of the elliptic curve discrete logarithm problem, such as the Elliptic Curve Digital Signature Algorithm (ECDSA), for example as described in "American National Standard for Financial Services ANS X9.62-2005: Public Key Cryptography for the Financial Services Industry - The Elliptic Curve Digital Signature Algorithm (ECDSA)", Accredited Standards Committee X9, Inc., 2005, may enable the use of smaller signatures than those of other cryptography schemes, such as the Rivest Shamir Adleman (RSA) algorithm, for example as described in "PKCS #1 v2.1: RSA Cryptography Standards", RSA Laboratories, 2002, while still offering the same level of security. Digital signatures with partial message recovery, for example as described by Nyberg et al. in "Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem", Advances in Cryptology – Eurocrypt '94, Springer Verlag, New York, 1994, may also reduce transmission requirements of the [message, signature] pair by embedding a portion of the message (the hidden portion) within the signature value, while not increasing the size of the signature. For example, the portion of the message that is embedded might include the address of the sender, or a confirmation of the recipient's address. The Elliptic Curve Pintsov-Vanstone Signature (ECPVS) scheme is an example of a digital signature scheme with partial message recovery. The ECPVS scheme is described in more detail, for

example in "American National Standard for Financial Services Draft X9.92-2007-02-21: Public Key Cryptography for the Financial Services Industry, Digital Signature Algorithms Giving Partial Message Recovery Part 1: Elliptic Curve Pintsov-Vanstone Signatures (ECPVS)", Accredited Standards Committee X9, Inc., 2007, as well as by Vanstone et al. in U.S. Patent No. 7,249,259. In ECPVS, all or part of the message to be signed can be embedded or "hidden" in and recovered from the signature. This scheme can also be used to provide a level of confidentiality by adding the restriction that the public key of the signer be kept secret, such that only parties who possess the public key may verify the signature, and hence only they may compute the hidden portion of the message.

[0004] In order for an ECPVS signature to be verified, the hidden portion of the message to be signed has a predefined characteristic that is chosen by the signer and agreed on by the verifier. For example, the hidden portion may contain a certain level of redundancy, which is checked by the verifier in order to verify the signature. The redundancy allows the hidden portion of the message to be identified as belonging to a set of valid plaintexts. Given sufficient redundancy, it should be infeasible for a forger to produce a signature which satisfies all criteria. The more redundancy there is in the hidden portion of the message, the higher the level of security, and the longer the signed message to be transmitted.

SUMMARY

[0005] A framework for using authenticated encryption in digital signatures with message recovery is herein proposed whereby the ECPVS scheme is modified to remove the redundancy criteria on the hidden portion of a message to be signed. The framework proposed herein augments the security of regular symmetric key encryption with authenticity by replacing the encryption traditionally used in ECPVS with authenticated encryption. The proposed framework can be applied to signature generation and signature verification.

[0006] In one example, an Authenticated Encryption – Pintsov Vanstone (AE-PV) scheme uses an authenticated encryption (AE) function to encrypt a hidden portion of a message to be signed while creating a message authentication code (MAC) on the hidden portion that shall be used by a verifier to verify the signed message.

[0007] In another example, a MAC-then-Encrypt – Pintsov Vanstone (ME-PV) scheme uses a MAC function to obtain a MAC on the hidden portion of the message to be signed, followed by an encryption function to encrypt a combination of the hidden portion and the MAC, such that the MAC may be used by the verifier to verify the signed message. In a variation, an Encrypt-then-MAC – Pintsov Vanstone (EM-PV) scheme uses the encryption function to encrypt the hidden portion of the signed message first, followed by the MAC function to obtain a MAC on the encryption result.

[0008] In yet another example, an Authenticated Encryption with Associated Data – Pintsov Vanstone (AEAD-PV) scheme uses an authenticated encryption with associated data (AEAD) function to encrypt the hidden portion of the message and to create a MAC on both the hidden portion and on non-encrypted associated data in the message, thereby allowing for authentication of both the hidden portion and the associated data.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The figures of the accompanying drawings are intended to illustrate by way of example and not limitation. Like reference numbers in the figures indicate corresponding, analogous or similar elements.

[0010] Figure 1 is a simplified block diagram of an example authenticated encryption signature scheme for a signer and a verifier;

[0011] Figure 2 is a simplified flowchart of a first example method for applying a signature to a message to generate a signed message;

[0012] Figure 3 is a simplified flowchart of a first example method for verifying a signed message signed by a signer;

[0013] Figure 4 is a simplified flowchart of a second example method for applying a signature to a message to generate a signed message;

[0014] Figure 5 is a simplified flowchart of a second example method for verifying a signed message signed by a signer;

[0015] Figure 6 is a simplified flowchart of a third example method for applying a signature to a message to generate a signed message;

[0016] Figure 7 is a simplified flowchart of a third example method for verifying a signed message signed by a signer;

[0017] Figure 8 is a simplified flowchart of a fourth example method for applying a signature to a message to generate a signed message;

[0018] Figure 9 is a simplified flowchart of a fourth example method for verifying a signed message signed by a signer; and

[0019] Figure 10 is a simplified block diagram of an example signer device and an example verifier device.

DETAILED DESCRIPTION

[0020] While the signature schemes described herein are instantiated using a group of points on an elliptic curve, they could alternatively be instantiated using any finite cyclic group, for example, a subgroup of $\mathbb{Z}p$, the group of integers modulo a prime number p. In this case, the group order may be $p - 1$ and a generator G generates a subgroup of order n, where n divides $p - 1$. Traditionally, arithmetic in subgroups of $\mathbb{Z}p$ is written multiplicatively, where the product of two elements P and Q is PQ, and the analogue of scalar multiplication in elliptic curve groups by an integer k is exponentiation, that is, P^k.

[0021] Protocols based on elliptic curve cryptography (ECC) rely on the intractability of the elliptic curve discrete logarithm problem. Given publicly-known points G and Q on an elliptic curve E, where point Q is equal to a product of a scalar multiplying factor d and point G, that is $Q = dG$, it is conjecturally very difficult to determine scalar multiplying factor d. With known algorithms, the computational difficulty of solving this problem increases exponentially with the size of the subgroup generated by G.

[0022] To implement an ECC-based protocol, all participants agree on the domain parameters of the elliptic curve. An elliptic curve E defined over a prime finite field $\mathbb{F}_p$, that is $E(\mathbb{F}_p)$, is defined by elliptic curve domain parameters $D = (p, a, b, G, n, h)$, where p is an odd prime number that represents the number of elements in the field, integers a and b are elements of prime finite field $\mathbb{F}_p$ that satisfy for example $4a^3 + 27b^2 \neq 0 \pmod{p}$, (however curves specified by another equation may be suitable), G is a base point or generator on elliptic curve $E(\mathbb{F}_p)$ that has order n, and cofactor h is a relatively small integer that is defined as a ratio of the number of points $\#E(\mathbb{F}_p)$ on elliptic curve $E(\mathbb{F}_p)$ over n. Arithmetic in subgroups of $E(\mathbb{F}_p)$ may be written additively, where the sum of two points P and Q is $P + Q$, and scalar multiplication by an integer k is kP. Further details of existing ECC-based protocols are described in "Standards for Efficient Cryptography SEC1: Elliptic Curve Cryptography", Certicom Research, Certicom Corp., 2000, and

"Standards for Efficient Cryptography SEC2: Recommended Elliptic Curve Domain Parameters version 2.0", Certicom Research, Certicom Corp., 2000. Elliptic curves can also be defined over the finite field F_2m, which is a binary representation with 2^m elements, rather than over a prime finite field $\mathbb{F}_p$, and the techniques described in this document can be modified to suit elliptic curves defined over the finite field F_2m.

[0023] The Elliptic Curve Pintsov-Vanstone Signature (ECPVS) scheme provides a digital signature scheme with partial message recovery. The ECPVS scheme has been used to provide a level of confidentiality by enabling a portion of the message being signed to be embedded or "hidden" within one of the resultant signature components. ECPVS can be used by a signer to generate a digital signature on data and by a verifier to verify the authenticity of the signature and to recover the portion of the message hidden within the signature. A private key of the signer is used in the signature generation process, and the corresponding public key is used in the signature verification process. In order for the hidden portion of the message to remain confidential, the public key of the signer needs to be kept secret.

[0024] The term "signer" as used herein refers to any computerized device able to generate a digital signature on data. The term "verifier" as used herein refers to any computerized device able to verify the authenticity of a digital signature.

[0025] One aspect of the ECPVS scheme is the selection by the signer of message redundancy criteria for a hidden portion of a message to be signed, where the redundancy criteria are known by the verifier in order to verify the signed message. Examples of redundancy criteria include that the message is an ASCII file, that the message is in a specific format, that the message contains certain key words, or that each paragraph ends with a period. The amount of total redundancy is a scalable security parameter which is chosen to achieve security objectives. Given sufficient redundancy, it should be infeasible for a forger to produce a valid signature on a message which satisfies the redundancy criteria. The more redundancy there is in the hidden portion of the message to be signed, the higher the level of security, and the longer the signed message to be transmitted.

Consequently, selection of an appropriate cryptographic signature may involve a tradeoff between security requirements and storage/transmission requirements.

[0026] A framework for using authenticated encryption in digital signatures with message recovery is herein proposed whereby the ECPVS scheme is modified to remove the redundancy criteria on the hidden portion of a message to be signed. proposed framework can be applied to signature generation and signature verification.

[0027] In one example, an Authenticated Encryption – Pintsov Vanstone (AE-PV) scheme uses an authenticated encryption (AE) function to encrypt a hidden portion of a message to be signed while creating a message authentication code (MAC) on the hidden portion that shall be used by a verifier to verify the signed message.

[0028] In another example, a MAC-then-Encrypt – Pintsov Vanstone (ME-PV) scheme uses a MAC function to obtain a MAC on the hidden portion of the message to be signed, followed by an encryption function to encrypt a combination of the hidden portion and the MAC, such that the MAC may be used by the verifier to verify the signed message. In a variation, an Encrypt-then-MAC – Pintsov Vanstone (EM-PV) scheme uses the encryption function to encrypt the hidden portion of the signed message first, followed by the MAC function to obtain a MAC on the encryption result.

[0029] In yet another example, an Authenticated Encryption with Associated Data – Pintsov Vanstone (AEAD-PV) scheme uses an authenticated encryption with associated data (AEAD) function to encrypt the hidden portion of the message and to create a MAC on both the hidden portion and on non-encrypted associated data in the message, thereby allowing for authentication of both the hidden portion and the associated data.

[0030] The framework proposed herein may also be applied to keyed ECPVS and other signcryption techniques.

[0031] In the following examples, it may be assumed, unless otherwise stated, that a signer and a verifier in a signature scheme have agreed on suitable domain parameters. For example, for a signature scheme instantiated using a group of points on an elliptic curve, the signer and the verifier agree on the corresponding elliptic curve domain parameters, including a base point G.

[0032] As previously described, while the Pintsov-Vanstone (PV) signature schemes described herein are instantiated using a group of points on an elliptic curve, the schemes may be instantiated using any finite cyclic group. In this case, the signer and the verifier would have to agree on domain parameters associated with that group, including a generator G.

[0033] The signer and the verifier using a particular signature scheme agree on the functions and parameters associated with that scheme. For example, with an Authenticated Encryption – Pintsov Vanstone (AE-PV) scheme, the signer and the verifier agree on an authenticated encryption (AE) function keyed by an integer k_1 that is able to take a message M as input and output an encrypted value c_1 and a message authentication code (MAC) *mac*, that is $AE_{k1}(M) = (c_1, mac)$. The signer and the verifier also agree on an authenticated decryption (AD) function which is a reverse transformation of AE that is keyed by an integer k_1 and that takes an encrypted value c_1' and a MAC *mac'* as inputs and outputs either the message M and an indication of validity, or null and an indication of invalidity, that is $AD_{k1}(c_1', mac') = (M, \text{VALID})$ or $AD_{k1}(c_1', mac') = (\text{NULL}, \text{INVALID})$. The signer and the verifier also agree on the bit lengths of key k_1 and on the bit length of MAC *mac*.

[0034] The signer and the verifier agree on a suitable key derivation function (KDF). For example, with the (AE-PV) scheme, the KDF is able to be used to construct a key suitable for use with authenticated encryption function AE_{k1} and authenticated decryption function AD_{k1}. Any ANSI-X9-approved key derivation function may be used, for example, the KDFs described in "NIST SP 800-108 Recommendation for Key Derivation Using Pseudorandom Functions", National Institute of Standards and Technology, 2009.

[0035] In examples where a hash function is to be used as part of a signature scheme, the signer and the verifier agree on a cryptographic hash function which maps arbitrary length inputs to fixed-length outputs. Example hash functions include the SHA-2 family as

described in "FIPS PUB 180-3 Federal Information Processing Standards Publication: Secure Hash Standard (SHS)", National Institute of Standards and Technology, 2008.

[0036] The signer and the verifier agree on encoding methods to communicate values, including integers and group elements. An example encoding method is ASN.1 described by Dubuisson in "ASN.1 Communication Between Heterogeneous Systems", Morgan Kaufmann, 2000. The signer and the verifier also agree on a common encoding of lists of values as bitstrings prior to hashing them. For example, they may agree (1) to convert all values to octet strings, and then (2) to hash a concatenation of the octet strings. As with hashing, an encoding may be performed before deriving keys. With both the KDF and hash function, encoding may incorporate additional information, for example, date, time, name of signer, name of verifier, or contact information related to the message being signed.

[0037] For security of a signature scheme, the domain parameters should be chosen carefully. Further details of parameter choices for Pintsov Vanstone signature schemes may be found in "IEEE P1363a/D2, Standard Specifications for Public Key Cryptography: Pinstov Vanstone Signatures with Message Recovery", Institute of Electrical and Electronics Engineers, 2000. It should also be noted that, for security, a signer may comprise a secure random or pseudo-random number generator for generating keys and signed messages.

[0038] As described previously, a public key of the signer that corresponds to a private key that was used in the signature generation process is known to the verifier for verification of a signed message. Furthermore, for those implementations where the hidden portion of the message is to remain confidential, the public key of the signer should not be disclosed to other entities.

[0039] Figure 1 is a simplified block diagram of an example scheme for authenticated encryption for digital signatures with message recovery for a signer 100 and a verifier 102. Signer 100 is to sign a message *M* 104 which comprises a hidden portion *N* and a visible portion *V*. Hidden portion *N* is the portion of message *M* 104 that is to be embedded or "hidden" in a part of the signature. Signer 100 is to apply a signature to message *M* 104 to obtain a signed message 106 which is to be transmitted to verifier 102. Signed message 106 comprises at least a first signature component *c*, a second signature component *s*, and visible portion *V* of message *M* 104. In order for verifier 102 to verify signed message 106,

verifier 102 is in possession of a public key G_A 110 of signer 100. Public key G_A 110 may be received directly from signer 100 as shown by the dotted line in Figure 1 or may be received from a trusted entity (not shown) such as a certificate authority. For those implementations where hidden portion N of message M 104 is to remain confidential, this may be achieved by ensuring the confidentiality of public key G_A 110. The result of the authenticated decryption of signed message 106 performed by verifier 102 is shown at 108. If signed message 106 is verified, hidden portion N of message M 104 is recovered and accompanied by an indication of validity. If signed message 106 is not verified, hidden portion N is not recovered and there is an indication of invalidity.

[0040] Figure 2 is a simplified flowchart of an example authenticated encryption method to be performed by a signer, for example, signer 100, for applying a signature to message M 104 to generate a signed message 106. At 202, the signer generates a first value k that is a private value of the signer which should not be disclosed to other entities. From this first value k and a base point G on an elliptic curve, the signer calculates a second value Q that is equal to a scalar product of first value k and base point G, according to equation 1:

[0041] $$Q = k \cdot G. \qquad (1)$$

[0042] In some implementations, the pair (k,Q) is ephemeral. That is, a new pair (k,Q) is generated for each message M to which a signature is to be applied.

[0043] At 204, the signer constructs a derived key k_1 from second value Q. For example, derived key k_1 may be constructed by applying a key derivation function KDF to second value Q, according to equation 2:

[0044] $$k_1 = KDF(Q). \qquad (2)$$

[0045] At 206, the signer applies an AE function keyed by derived key k_1, that is AE_{k1}, to hidden portion N of message M 104 to obtain an encrypted value c_1 and a Message Authentication Code (MAC) mac of a prerequisite length L, where length L is a parameter of authenticated encryption function AE. This is shown in equation 3:

[0046] $(c_1, mac) = AE_{k1}(N)$. (3)

[0047] The AE function is used to encrypt hidden portion N of message M 104 and to create a MAC *mac* that can be used by a verifier for subsequent verification of signed message 106. An adversary who does not know derived key k_1, but observes a number of [encrypted value, MAC] pairs output by authenticated encryption function AE_{k1} should not be able to output a new [encrypted value, MAC] pair that could be used by the verifier to successfully verify signed message 106 and recover hidden portion N of message M 104. Authenticated decryption is described in more detail with respect to Figure 3.

[0048] One possible AE function that may be used is the Advanced Encryption Standard (AES) with Counter Mode Encryption (CME) and Cipher Block Chaining (CBC), also known as AES-CCM, which is described in "NIST SP 800-38C Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality", National Institute of Standards and Technology, 2007. Another possible AE function that may be used is AES with Galois Counter Mode (AES-GCM), which is described in "NIST SP 800-38D Recommendation for Block Cipher Modes of Operation: The Galois/Counter Mode (GCM) and GMAC", National Institute of Standards and Technology, 2007. Details of the AES are described in "FIPS PUB 197 Advanced Encryption Standard (AES)", Federal Information Processing Standards, 2001, and Section 7.2.2 of "Handbook of Applied Cryptography", CRC Press, ISBN 0-8493-8523-7. Yet another possible AE function that may be used is AES Key Wrap, which is described in "AES Key Wrap Specification", National Institute of Standards and Technology, November 2001, and variants thereof. The Accredited Standards Committee, X9, Inc. (ASC X9) has defined four algorithms in its draft standard published November 2004. Any of those four algorithms is a suitable AE function that may be used: AESKW (a variant of the AES Key Wrap Specification), TDKW (similar to AESKW, but using Triple DES as the underlying block cipher instead of AES), AKW1 (essentially the algorithm proposed in the Internet Engineering Task Force Request For Comment 3217), and AKW2 (the algorithm that is implicitly defined in a "key block" specification that has been developed for use in constrained legacy systems in the financial services industry). It is also contemplated to use an AE function that does not explicitly output a MAC value upon

encryption but still provides authentication. For example, such an AE function, when applied to an input I, outputs an encrypted value $AE_{k1}(I)$ but does not output any MAC, and its associated authenticated decryption function AD, when applied to an input I', outputs either that I' is not valid, or I and an indication that I is valid.

[0049] Returning to Figure 2, at 208, the signer forms a first signature component c from encrypted value c_1 and MAC mac. First signature component c may be, for example, a concatenation of encrypted value c_1 and MAC mac, as shown in equation 4:

[0050] $$c = c_1 || mac \quad (4)$$

[0051] Alternatively, first signature component c may be a concatenation of MAC mac and encrypted value c_1, that is, $c = mac||c_1$. More generally, first signature component c may be a result of applying any reversible function f to encrypted value c_1 and MAC mac, that is, $c = f(c_1, mac)$, where f is agreed on by the signer and the verifier. It will also be understood by a person of ordinary skill in the art that certain non-reversible functions may be used. For example, a function f that takes three elements x, y, and z as input, and outputs a concatenation of x and y, that is $f(x,y,z) = x||y$, is not reversible because the output contains no information about element z. However, this function could still be used.

[0052] At 210, the signer computes a second signature component s, according to equation 5:

[0053] $$s = Hash(c||V) \cdot d_A + k \pmod{n}, \quad (5)$$

[0054] where $Hash$ is a cryptographic hash function as described previously, and d_A is a private key of the signer, with a corresponding public key G_A having been computed as a product of private key d_A and base point G, that is $G_A = d_A \cdot G$.

[0055] While not explicitly shown in the figures, other methods of calculating second signature component s are contemplated. For example, second signature component s

could be calculated by switching the positions of private key d_A and first value k in equation 5, that is $s = Hash(c||V)\cdot k + d_A \pmod{n}$. Alternatively, either of the terms in either one of these equations could be negated. If second signature component s is calculated using such a modification of equation 5, the verification procedure is changed accordingly.

[0056] Although not explicitly shown, $Hash(c||V)$ is converted to an integer for use in equation 5 or any of the alternatives to equation 5.

[0057] The expression $c||V$ denotes a concatenation of first signature component c and visible portion V of message M 104. Alternatively, visible portion V may be concatenated with first signature component c, that is $V||c$. More generally, first signature component c may be combined with visible portion V using any reversible function g, that is, $g(c, V)$, where g is agreed on by the signer and the verifier. As described previously with respect to equation 4, certain non-reversible functions may also be used.

[0058] At 212, the signer prepares signed message 106, the signed message 106 comprising first signature component c, second signature component s, and visible portion V of message M 104. While first signature component c and visible portion V are shown as separate elements of signed message 106, it is contemplated that they may also be combined using reversible function g as was done during the computation of second signature component s at 210. For example, if first signature component c and visible portion V were concatenated as shown in equation 5, signed message 106 may comprise the same concatenation that is $c||V$.

[0059] Figure 3 is a simplified flowchart of an example authenticated decryption method to be performed by a verifier, for example, verifier 102, for verifying a signed message, for example, signed message 106, which is purported to be signed by a signer, for example, signer 100.

[0060] At 301, the verifier extracts first signature component c', second signature component s', and visible portion V' of message M 104 from signed message 106. **The apostrophe is used to indicate a value that has not yet been verified.** As described previously, if first signature component c and visible portion V have been combined using

reversible function g, the inverse of function g, that is g^{-1}, will be necessary to extract first signature component c' and visible portion V' from signed message 106.

[0061] At 302, the verifier extracts encrypted value c_1' and MAC mac' from first signature component c' using prerequisite length L associated with authenticated encryption function AE, which has been agreed on by the signer and the verifier. For example, if first signature component c was defined as the concatenation of encrypted value c_1 and MAC mac as shown in equation 4, the verifier can determine encrypted value c_1' by defining the last L bits of first signature component c' as MAC mac', such that the remaining bits at the beginning of first signature component c' correspond to encrypted value c_1'.

[0062] If encrypted value c_1 and MAC mac have been combined using some other reversible function f as described previously, the inverse of function f, that is f^{-1}, will be necessary to extract encrypted value c_1' and MAC mac' from first signature component c'.

[0063] It should be noted that the extraction described at 302 could be performed at any time prior to applying the authenticated decryption function at 308, as described in more detail below.

[0064] At 304, the verifier computes a value Q', according to equation 6:

[0065] $$Q' = s' \cdot G - Hash(c' \| V') \cdot G_A, \qquad (6)$$

[0066] where $Hash$ is the same cryptographic hash function used by the signer to compute second signature component s at 210 as shown in equation 5. As previously described, if second signature component s has been calculated using a modification of equation 5, equation 6 will need to be modified accordingly. As in equation 5, $Hash(c \| V)$ is converted to an integer for use in equation 6. Public key G_A 110 may be received directly from signer or may be received from a trusted entity, such as a certificate authority. As previously described, other combinations of first signature component c' and visible

portion V' are contemplated in place of the concatenation $c'||V'$ shown in equation 6, provided the combination used in equation 6 corresponds to that used in computing second signature component s in equation 5.

[0067] At 306, the verifier constructs a derived key k_1' from value Q' using the same method used by the signer to construct derived key k_1 at 204. For example, if the signer has used key derivation function KDF to construct derived key k_1 as shown in equation 2, the verifier is to construct derived key k_1' according to equation 7:

[0068] $$k_1' = KDF(Q'). \quad (7)$$

[0069] At 308, the verifier applies an AD function that is a reverse transformation of the AE function that was used by the signer at 206. The AD function, which is keyed by derived key k_1' and denoted AD_{k1}', may be used to verify signed message 106 and recover hidden portion N of message 104. Result 108 of the AD function depends on whether the verifier is able to verify signed message 106. If the verifier determines that signed message 106 is valid, result 108 comprises recovered hidden portion N of message M 104 and an indication of validity. If the verifier determines that signed message 106 is invalid, result 108 comprises only an indication of invalidity, without hidden portion N.

[0070] Instead of jointly creating encrypted value c_1 and MAC mac using an AE function as described in equation 3 and shown at 206, the encryption and creation of a MAC can be performed as two separate steps. There are at least two variants of this which will be referred to as: (1) MAC-then-Encrypt (ME), and (2) Encrypt-then-MAC (EM). (There is also an Encrypt-and-MAC variant. However, given that the Encrypt-and-MAC variant is only secure for specific choices of encryption function and MAC function, the Encrypt-and-MAC variant is not explicitly described.)

[0071] Both the encryption function and the MAC function may be secure functions. Examples of secure encryption functions include AES with Cipher Block Chaining (AES-CBC) and AES Counter Mode (AES-CTR) as described in "NIST SP 800-38A Recommendation for Block Cipher Modes of Operation", National Institute of Standards

and Technology, 2001. Examples of secure MAC functions include AES Cipher Block Chaining Message Authentication Code (AES-CBC-MAC) as described in "ISO/IEC 9797 Data Cryptographic Techniques – Data integrity mechanism using a cryptographic check function employing a block cipher algorithm", International Organization for Standardization,1989, and AES Cipher-based MAC (AES-CMAC) as described in "NIST SP 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication", National Institute of Standards and Technology, 2005. The encryption function and MAC function are agreed on by the signer and the verifier.

[0072] Figure 4 is a simplified flowchart of an example MAC-then-Encrypt variant of the AE method illustrated in Figure 2 for message M 104. As described with respect to Figure 2, the example method illustrated in Figure 4 includes generation of first value k and computation of second value Q at 202. As described with respect to Figure 2, in some implementations the pair (k, Q) is ephemeral. That is, a new pair (k,Q) is generated for each message M to which a signature is to be applied. However, in this method, the signer constructs a first derived key k_{11} and a second derived k_{12} from value Q at 404. For example, derived keys k_1 and k_2 may be constructed by applying a key derivation function KDF to second value Q, according to equation 8:

[0073] $$(k_1, k_2) = KDF(Q), \qquad (8)$$

[0074] where the output of KDF is longer than the output of the KDF used in equation 2, such that the output may be divided into first derived key k_{11} and second derived k_{12}. Alternatively, first derived key k_{11} and second derived k_{12} could be constructed by applying a KDF to second value Q twice, using different auxiliary information for each application. While it is possible to apply a KDF to second value Q twice without using different auxiliary information for each application, this may not be advisable for security reasons.

[0075] At 405, the signer applies a MAC function T keyed by second derived key k_{12}, that is T_{k12}, to hidden portion N of message M 104 to obtain a MAC *mac*, according to equation 9:

[0076] $$mac = T_{k12}(N), \quad (9)$$

[0077] where MAC *mac* has a prerequisite length L which is a parameter of MAC function T.

[0078] At 406, the signer applies an encryption function E keyed by first derived key k_{11}, that is E_{k11}, to a combination of hidden portion N and MAC *mac* to obtain a first signature component c, according to equation 10:

[0079] $$c = E_{k11}(N||mac). \quad (10)$$

[0080] The expression $N||mac$ denotes a concatenation of hidden portion N and MAC *mac*. Alternatively, MAC *mac* may be concatenated with hidden portion N, that is $mac||N$. More generally, hidden portion N may be combined with MAC *mac* using any reversible function j, that is $j(N, mac)$, where j is agreed on by the signer and the verifier. As described previously with respect to equation 4, certain non-reversible functions may also be used.

[0081] Upon obtaining first signature component c at 406, the method proceeds as described with respect to Figure 2, with the signer computing second signature component s at 210, and preparing signed message 106 at 212.

[0082] Figure 5 is a simplified flowchart of an example Decrypt-then-Verify variant of the AD method illustrated in Figure 3. As described with respect to Figure 3, the example method illustrated in Figure 5 includes extraction of first signature component c', second signature component s', and visible portion V' from signed message 106 at 301. **The apostrophe is used to indicate a value that has not yet been verified.** At 304, the verifier computes value Q' using public key G_A110. At 506 the verifier constructs a first

derived key k_{11}' and a second derived key k_{12}' from value Q' using the same method used by the signer to construct first derived key k_{11} and second derived key k_{12} at 404.

[0083] To decrypt first signature component c', the verifier applies a decryption function D to first signature component c' at 508, where decryption function D is a reverse transformation of encryption function E that was used by the signer at 406. The decryption function is keyed by first derived key k_{11}' and is denoted $D_{k11'}$. This is shown in equation 11:

[0084] $$N'||mac' = D_{k11'}(c), \qquad (11)$$

[0085] where $N'||mac'$ denotes a concatenation of a hidden portion N' of signed message 106 and a MAC mac'. The verifier is able to extract hidden portion N' and MAC mac' from the concatenation $N'||mac'$ using prerequisite length L associated with MAC function T agreed on by the signer and the verifier. If hidden portion N and MAC mac were combined at 406 using some other reversible function j as described previously, the inverse of function j, that is j^{-1}, will be necessary to obtain hidden portion N' and MAC mac'.

[0086] At 510, the verifier uses second derived key k_{12}' to verify that MAC mac' is a valid MAC of hidden portion N' of signed message 106, and accordingly determines whether signed message 106 is valid. As described previously with respect to Figure 3, if the verifier determines that signed message 106 is valid, result 108 comprises recovered hidden portion N of message M 104 and an indication of validity. If the verifier determines that signed message 106 is invalid, result 108 comprises only an indication of invalidity, without hidden portion N.

[0087] It is also contemplated that an Encrypt-then-MAC/Verify-then-Decrypt variant could be used as an alternative to the MAC-then-Encrypt/Decrypt-then-Verify variant. Figure 6 is a simplified flowchart of an example Encrypt-then-MAC variant of the AE method illustrated in Figure 2 for message M 104. As described with respect to Figure 2, the example method illustrated in Figure 6 includes generation of first value k and computation of second value Q at 202, such that $Q = k \cdot G$. As described with respect to

Figure 2, in some implementations the pair *(k, Q)* is ephemeral. That is, a new pair *(k,Q)* is generated for each message M to which a signature is to be applied. Then, as described with respect to Figure 4, the signer constructs first derived key k_{11} and second derived k_{12} from value Q at 404.

[0088] At 606, the signer applies an encryption function E keyed by first derived key k_{11}, that is E_{k11}, to hidden portion N to obtain an encrypted value c_1, according to equation 12:

[0089] $$c_1 = E_{k11}(N) \qquad (12)$$

[0090] At 607, the signer applies a MAC function T keyed by second derived key k_{12}, that is T_{k12}, to encrypted value c_1 to obtain a MAC *mac*, according to equation 13:

[0091] $$mac = T_{k12}(c_1), \qquad (13)$$

[0092] where MAC *mac* has a prerequisite length L which is a parameter of MAC function T.

[0093] Upon obtaining MAC *mac* at 607, the method proceeds as described with respect to Figure 2, with the signer forming first signature component c from encrypted value c_1 and MAC *mac* at 208, computing second signature component s at 210, and preparing signed message 106 at 212.

[0094] Figure 7 is a simplified flowchart of an example Verify-then-Decrypt variant of the AD method illustrated in Figure 3. As described with respect to Figure 3, the example method illustrated in Figure 7 includes extraction of first signature component c', second signature component s', and visible portion V' from signed message 106 at 301, extraction of encrypted value c_1' and MAC *mac'* from first signature component c' at 302, and computation of value Q' at 304 using public key G_A 110. **The apostrophe is used to indicate a value that has not yet been verified.** As described with respect to Figure 5, at 506 the verifier constructs a first derived key k_{11}' and a second derived key k_{12}' from

value Q' using the same method used by the signer to construct first derived key k_{11} and second derived key k_{12} at 404.

[0095] At 708, the verifier uses second derived key k_{12}' to verify that MAC *mac'* is a valid MAC of encrypted value c_1', and accordingly determines whether signed message 106 is valid.

[0096] If the verifier determines that MAC *mac'* is a valid MAC of encrypted value c_1', the verifier proceeds to apply a decryption function D to encrypted value c_1' at 710, where the decryption function is a reverse transformation of encryption function E that was used by the signer at 606. The decryption function is keyed by first derived key k_{11}' and is denoted D_{k11}'. This is shown in equation 14:

[0097] $$N = D_{k11}'(c_1'). \qquad (14)$$

[0098] Because the verifier has already determined at 708 that MAC *mac'* is a valid MAC of encrypted value c_1', and consequently that signed message 106 is valid, result 108 comprises recovered hidden portion N of message M 104 and an indication of validity.

[0099] If the verifier determines at 708 that MAC *mac'* is not a valid MAC of encrypted value c_1', the verifier does not apply decryption function D at 710, and result 108 comprises only an indication of invalidity, without hidden portion N.

[00100] In another example, Authenticated Encryption with Associated Data (AEAD) can be used as part of a Pintsov-Vanstone signature scheme with message recovery. For example, the AE function could be replaced by an AEAD function. AEAD is described in more detail by Rogaway in "Authenticated encryption with associated data", Proceedings of ACM CCS'02: 98-107, ACM, New York, 2002.

[00101] Similarly to the AE-PV, ME-PV, and EM-PV schemes, an AEAD – Pintsov Vanstone (AEAD-PV) scheme can be used to encrypt a hidden portion N of a message M that is to be embedded or hidden in the signature and to provide authenticity and

confidentiality to that portion of the message. The AEAD-PV scheme uses the AEAD function to guarantee the authenticity of a visible portion V of the message (and thus may avoid use of a hash function). In many settings there are data associated with an encrypted value that is public to allow processing or routing of a message by intermediate parties who are not in possession of the encryption key. Using an AEAD function in place of an AE function in the previously described signature scheme has an advantage that a hash function is not involved.

[00102] The AEAD-PV scheme includes that the signer and the verifier agree on an AEAD function keyed by an integer k_1 that is able to take a hidden portion N and a visible portion V as inputs and to output an encrypted value c_1 and a MAC mac, that is $AEAD_k(N, V) = (c_1, mac)$. The signer and the verifier also agree on an Authenticated Decryption with Associated Data (ADAD) function which is a reverse transformation of $AEAD$ that is keyed by an integer k_1' and that takes an encrypted value c_1' and a MAC mac' as inputs and outputs either the hidden portion N and an indication of validity, or null and an indication of invalidity, that is $ADAD_{k1'}(c_1', mac', V) = (N, \text{VALID})$ or $ADAD_{k1'}(c_1', mac', V) = (\text{NULL}, \text{INVALID})$. The signer and the verifier also agree on the bit length of key k_1 and on the bit length of MAC mac . An example AEAD scheme suitable for use in the proposed framework is described by Kohno et al. in "CWC: A High-Performance Conventional Authenticated Encryption Mode", Proceedings of Fast Software Encryption 2004 (FSE'04), LNCS 3017: 408-426, 2004.

[00103] Figure 8 is a simplified flowchart of an example Authenticated Encryption with Associated Data (AEAD) method to be performed by a signer, for example, signer 100, for applying a signature to message 104 to generate a signed message 106. As described with respect to Figure 2, at 202, the signer generates a first value k and calculates a second value Q, such that $Q = k \cdot G$. As described with respect to Figure 2, in some implementations the pair (k, Q) is ephemeral. That is, a new pair (k,Q) is generated for each message M to which a signature is to be applied. At 204, the signer constructs a derived key k_1 from second value Q.

[00104] At 806, the signer applies an AEAD function keyed by derived key k_1, that is $AEAD_{k1}$, to hidden portion N of message M 104 and visible portion V of message M 104 to obtain an encrypted value c_1 and a MAC mac of a prerequisite length L, where length L is a parameter associated with $AEAD$ which has been agreed on by the signer and the verifier. This is shown in equation 15:

[00105] $$(c_1, mac) = AEAD_{k1}(N, V). \quad (15)$$

[00106] The AEAD function is used to encrypt hidden portion N of message M 104 and to create a MAC that can be used by a verifier for subsequent verification of signed message 106. In particular, application of the AEAD function may be used to guarantee the authenticity of visible portion V, without involving a hash function, as described in more detail below.

[00107] After obtaining encrypted value c_1 and MAC mac at 806, the signer proceeds as described with respect to Figure 2 to form a first signature component c from encrypted value c_1 and MAC mac at 208.

[00108] At 810, the signer computes a second signature component s, according to equation 16:

[00109] $$s = mac \cdot d_A + k \pmod{n}, \quad (16)$$

[00110] where MAC mac has been converted to an integer for use in equation 16. A comparison of equation 16 to equation 5 reveals that the hash function of the AE-PV, ME-PV, and EM-PV authenticated encryption methods is not involved in AEAD-PV encryption.

[00111] While not explicitly shown in Figure 8, other methods of calculating second signature component s are contemplated. For example, second signature component s could be calculated by switching the positions of private key d_A and first value k in equation 16, that is $s = mac \cdot d_A + k \pmod{n}$. Alternatively, either of the terms in either one

of these equations could be negated. If second signature component s is calculated using such a modification of equation 16, the verification procedure is changed accordingly.

[00112] Following computation of second signature component s at 208, the signer proceeds as described with respect to Figure 2, preparing signed message 106 at 212.

[00113] Figure 9 is a simplified flowchart of an example Authenticated Decryption with Associated Data (ADAD) method to be performed by a verifier, for example, verifier 102, for verifying a signed message, for example, signed message 106, which is purported to be signed by a signer, for example, signer 100. As described with respect to Figure 3, the example method illustrated in Figure 9 includes extraction of first signature component c', second signature component s', and visible portion V' from signed message 106 at 301, extraction of encrypted value c_1' and MAC mac' from first signature component c' at 302. **The apostrophe is used to indicate a value that has not yet been verified.** In this case, MAC mac' has prerequisite length L which is a parameter of the AEAD function agreed on by the signer and the verifier.

[00114] At 904, the verifier computes a value Q' using public key G_A 110, according to equation 17:

[00115] $$Q' = s' \cdot G - mac' \cdot G_A, \qquad (17)$$

[00116] where MAC mac' has been converted to an integer prior to use in equation 17. A comparison of equation 17 to equation 6 reveals that the hash function of the AE-PV, ME-PV, and EM-PV authenticated decryption methods is not involved in AEAD-PV decryption.

[00117] As previously described, if second signature component s has been calculated using a modification of equation 16, equation 17 will need to be modified accordingly.

[00118] At 306, the verifier constructs a derived key k_1' from value Q' using the same method used by the signer to construct derived key k_1 at 204.

[00119] At 908, the verifier applies an ADAD function to encrypted value c_1', MAC *mac'* and visible portion *V'*, where the ADAD function is a reverse transformation of the AEAD function that was used by the signer at 806. The ADAD function, which is keyed by derived key k_1' and denoted $ADAD_{k1}'$, may be used to verify signed message 106 and recover hidden portion *N* of message *M* 104. Result 108 of the ADAD function depends on whether the verifier is able to verify signed message 106. If the verifier determines that signed message 106 is valid, result 108 comprises recovered hidden portion *N* of message *M* 104 and an indication of validity. If the verifier determines that signed message 106 is invalid, result 108 comprises only an indication of invalidity, without hidden portion *N*.

[00120] As discussed previously, the proposed framework may also be applied to keyed ECPVS and other signcryption techniques. Signcryption provides the functionality of both a public key signature and encryption. The signer uses the verifier's public key when creating the signcryption message. Only the verifier can decrypt the message and verify that it was signed by the signer using the verifier's secret key and the signer's public key. This differs from keeping the signer's public key secret as in ECPVS, since the confidentiality is provided by the secrecy of the verifier's secret key, and the signer's public key may be public.

[00121] It will be appreciated that for very short messages $M=N||V$, visible portion *V* may be null. The AE-PV scheme can handle the case when visible portion *V* is null without modification. If hidden portion *N* is null, then hidden portion *N* should be replaced in the AE-PV scheme by the zero byte or any other public constant. The AEAD-PV scheme may be able to handle null messages. If not, a null message or null portion of a message can be replaced by a public constant.

[00122] Figure 10 is a simplified block diagram of a signer device 1000 and a verifier device 1040.

[00123] Signer device 1000 is able to perform one or more of the example methods illustrated in Figures 2, 4, 6, and 8. Signer device 1000 comprises a processor 1002 which is coupled to a memory 1004 and to a communication interface 1006. Signer device 1000 may comprise a random or pseudo-random number generator (RNG) 1005. Signer device 1000 may contain other elements which, for clarity, are not shown in Figure 10.

[00124] Verifier device 1040 is able to perform one or more of the example methods illustrated in Figures 3, 5, 7, and 9. Verifier device 1040 comprises a processor 1042 which is coupled to a memory 1044 and to a communication interface 1046. Verifier device 1040 may contain other elements which, for clarity, are not shown in Figure 10.

[00125] Processors 1002 and 1042 may comprise any combination of processing units, digital signal processors, hardware accelerators, and the like. All or part of memory 1004 may be embedded in processor 1002. All or part of memory 1044 may be embedded in processor 1042.

[00126] Communication interfaces 1006 and 1046 may be wired communication interfaces or wireless communication interfaces or optical communication interfaces. For example, communication interfaces 1006 and 1046 may be Universal Serial Bus (USB) interfaces, Ethernet interfaces, Integrated Services Digital Network (ISDN) interfaces, Digital Subscriber Line (DSL) interfaces, Local Area Network (LAN) interfaces, High-Definition Multimedia (HDMI) interfaces, Digital Visual Interfaces (DVIs), or Institute of Electrical and Electronics Engineers (IEEE) 1394 interfaces such as i.LINK™, Lynx^{SM} or Firewire®. In another example, communication interfaces 1006 and 1046 may be Wireless Local Area Network (WLAN) interfaces, short-range wireless communication interfaces such as Wireless Personal Area Network (WPAN) interfaces, near field communication interfaces, wireless metropolitan area network (WMAN) interfaces, or Wireless Wide Area Network (WWAN) interfaces.

[00127] The functionality of one or more of the example methods illustrated in Figures 2, 4, 6 and 8 may be implemented by any combination of processor 1002 and code 1008 stored in memory 1004 of signer device 1000. Memory 1004 may also store applications (not shown) installed in signer device 1000 to be executed by processor 1002.

[00128] Each of memories 1004 and 1044 is able to store parameters 1010 that have been agreed on by signer device 1000 and verifier device 1040. Examples of agreed on parameters 1010 are elliptic curve domain parameters D, one or more key derivation functions, one or more hash functions, one or more functions associated with a signature scheme to be implemented (for example, one or more of an AE function, a MAC function, an encryption function, and an AEAD function), as well as parameters associated with the signature scheme, such as a prerequisite length L of a message authentication code.

[00129] Memory 1004 is able to store a private key d_A 1012 of signer device 1000 that corresponds to public key G_A 1014 of signer device 1000. Memory 1004 is also able to store a first value k 1016 and a second value Q 1018 as computed at 202, except for those implementations where the pair (k, Q) is ephemeral and thus not stored in memory. Memory 1004 is able to store a hidden portion N 1020 and a visible portion V 1022 of a message to be signed. In addition, memory 1004 is able to store one or more derived keys 1024 as constructed at 204 or 404, encrypted value c_1 1026 as computed at 206, 606, or 806 and message authentication code *mac* 1028 as determined at 206, 405, 607, or 806. Memory 1004 is able to store a first signature component c 1030 as determined at 208 or 406, and a second signature component s 1032 as determined 210 or 810. Memory 1004 may store additional elements which are not explicitly shown in Figure 10.

[00130] As denoted by an arrow 1034, a signed message 1036 comprising visible portion V 1022, first signature component c 1030, and second signature component s 1032 is able to be sent, directly or via one or more intermediaries, from signer device 1000 to verifier device 1040, where it may be stored in memory 1044 of verifier device 1040. While not explicitly shown, signed message 1036 may be sent from signer device 1000 via communication interface 1006 and may be received by verifier device 1040 via communication interface 1046.

[00131] The functionality of one or more of the example methods illustrated in Figures 3, 5, 7 and 9 may be implemented by any combination of processor 1042 and code 1048 stored in memory 1044 of verifier device 1040. Memory 1044 may also store applications (not shown) installed in verifier device 1040 to be executed by processor 1042.

[00132] Memory 1044 is able to store public key G_A 1014 of signer device 1000, which it may have received directly from signer device 1000 or from a trusted device (not shown), possibly via communication interface 1046 and possibly by other means. For example, public key G_A 1014 of signer device 1000 may be included in software installed on verifier device 1040. Memory 1044 is also able to store a value Q' 1050 as determined at 304 or 904, one or more derived keys 1052 as constructed at 306 or 506, encrypted value

c_1' 1054 as extracted at 302 and message authentication code *mac'* 1056 as determined at 302 or 508, and recovered hidden portion *N* 1020. Memory 1044 may store additional elements which are not explicitly shown in Figure 10.

[00133] Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the specific features or acts described above. Rather, the specific features and acts described above are disclosed as example forms of implementing the claims.

What is claimed is:

1. A method of applying a signature to an original message [M] (104) to generate a signed message (106, 1036) signed by a signer (100, 1000), the original message [M] (104) consisting of a first portion [N] (1020) and a second portion [V] (1022), the method comprising:

selecting a first integer value [k] (1016) and computing a second value [Q] (1018) from the first integer value [k] (1016) and from a generator [G] of a finite cyclic group such that the second value [Q] (1018) is included in the finite cyclic group;

constructing a derived key [k_1] (1024) by applying a key derivation function [KDF] to input that comprises the second value [Q] (1018);

applying an authenticated encryption function, keyed by the derived key [k_1] (1024), to the first portion [N] (1020) of the message [M] (104) to obtain an encrypted value [c_1] (1026) and a message authentication code [mac] (1028);

reversibly combining the encrypted value [c_1] (1026) and the message authentication code [mac] (1028) to form a first signature component [c] (1030),

computing a second signature component [s] (1032) using

(i) the first integer value [k] (1016);

(ii) a private key [d_A] (1012) of the signer (100, 1000); and

(iii) a second integer value dependent on the first signature component [c] (1030) and the second portion [V] (1022) of the message [M] (104); and

reversibly combining the first signature component [c] (1030), the second signature component [s] (1032) and the second portion [V] (1022) of the message [M] (104) to form the signed message (106, 1036),

wherein verification of the signed message (106, 1036) and recovery of the first portion [N] (1020) of the message [M] (104) from the signed message (106, 1036) involves a public key [G_A] (110, 1014) of the signer (100, 1000), and

wherein the finite cyclic group is a subgroup of the group of integers modulo a prime number.

2. A method of applying a signature to an original message [M] (104) to generate a signed message (106, 1036) signed by a signer (100, 1000), the original message [M] (104) consisting of a first portion [N] (1020) and a second portion [V] (1022), the method comprising:

selecting a first integer value [k] (1016) and computing a second value [Q] (1018) from the first integer value [k] (1016) and from a generator [G] of a finite cyclic group such that the second value [Q] (1018) is included in the finite cyclic group;

constructing a first derived key [k_{11}] (1024) and a second derived key [k_{12}] (1024) by applying a key derivation function [KDF] to input that comprises the second value [Q] (1018);

applying a message authentication code 'MAC' function, keyed by the second derived key [k_{12}] (1024), to the first portion [N] (1020) of the message [M] (104) to obtain a message authentication code [mac] (1028);

applying an encryption function, keyed by the first derived key [k_{11}] (1024), to a reversible combination of the first portion [N] (1020) of the message [M] (104) and the message authentication code [mac] (1028) to obtain a first signature component [c] (1030);

computing a second signature component [s] (1032) using

(i) the first integer value [k] (1016);

(ii) a private key [d_A] (1012) of the signer (100, 1000); and

(iii) a second integer value dependent on the first signature component [c] (1030) and the second portion [V] (1022) of the message [M] (104); and

reversibly combining the first signature component [c] (1030), the second signature component [s] (1032) and the second portion [V] (1022) of the message [M] (104) to form the signed message (106, 1036),

wherein verification of the signed message (106, 1036) and recovery of the first portion [N] (1020) of the message [M] (104) from the signed message (106, 1036) involves a public key [G_A] (110, 1014) of the signer (100, 1000).

3. A method of applying a signature to an original message [M] (104) to generate a signed message (106, 1036) signed by a signer (100, 1000), the original message [M] (104) consisting of a first portion [N] (1020) and a second portion [V] (1022), the method comprising:

selecting a first integer value [k] (1016) and computing a second value [Q] (1018) from the first integer value [k] (1016) and from a generator [G] of a finite cyclic group such that the second value [Q] (1018) is included in the finite cyclic group;

constructing a first derived key [k_{11}] (1024) and a second derived key [k_{12}] (1024) by applying a key derivation function [KDF] to input that comprises the second value [Q] (1018);

applying an encryption function, keyed by the first derived key [k_{11}] (1024), to the first portion [N] (1020) of the message [M] (104) to obtain an encrypted value [c_1] (1026);

applying a message authentication code 'MAC' function, keyed by the second derived key [k_{12}] (1024), to the encrypted value [c_1] (1026) to obtain a message authentication code [mac] (1028);

reversibly combining the encrypted value [c_1] (1026) and the message authentication code [mac] (1028) to form a first signature component [c] (1030);

computing a second signature component [s] (1032) using

(i) the first integer value [k] (1016);

(ii) a private key [d_A] (1012) of the signer (100, 1000); and

(iii) a second integer value dependent on the first signature component [c] (1030) and the second portion [V] (1022) of the message [M] (104); and

reversibly combining the first signature component [c] (1030), the second signature component [s] (1032) and the second portion [V] (1022) of the message [M] (104) to form the signed message (106, 1036),

wherein verification of the signed message (106, 1036) and recovery of the first portion [N] (1020) of the message [M] (104) from the signed message (106, 1036) involves a public key [G_A] (110, 1014) of the signer (100, 1000).

4. The method as recited in claim 1 or claim 2 or claim 3, the method further comprising:

applying a hash function to a reversible combination of the first signature component [c] (1030) and the second portion [V] (1022) of the message [M] (104) to obtain a hash result; and

calculating the second integer value equivalent to the hash result.

5. The method as recited in claim 4, wherein the reversible combination further comprises an identity of the signer (100, 1000).

6. The method as recited in claim 2 or claim 3, the method further comprising:

constructing the first derived key [k_{11}] (1024) by applying the key derivation function [KDF] to input that comprises the second value [Q] (1018) and first auxiliary information; and

constructing the second derived key [k_{12}] (1024) by applying the key derivation function [KDF] to input that comprises the second value [Q] (1018) and second auxiliary information.

7. The method as recited in claim 6, wherein the second auxiliary information is different than the first auxiliary information.

8. The method as recited in claim 2 or claim 3, the method further comprising:

applying the key derivation function [*KDF*] to input that comprises the second value [*Q*] (1018) to obtain a key;

dividing the key into a first part and a second part; and

constructing the first derived key [k_{11}] (1024) from the first part and constructing the second derived key [k_{12}] (1024) from the second part.

9. A method of applying a signature to an original message [*M*] (104) to generate a signed message (106, 1036) signed by a signer (100, 1000), the original message [*M*] (104) consisting of a first portion [*N*] (1020) and a second portion [*V*] (1022), the method comprising:

selecting a first integer value [*k*] (1016) and computing a second value [*Q*] (1018) from the first integer value [*k*] (1016) and from a generator [*G*] of a finite cyclic group such that the second value [*Q*] (1018) is included in the finite cyclic group;

constructing a derived key [k_1] (1024) by applying a key derivation function [*KDF*] to input that comprises the second value [*Q*] (1018);

applying an authenticated-encryption-with-associated-data function, keyed by the derived key [k_1] (1024), to the first portion [*N*] (1020) of the message [*M*] (104) and to the second portion [*V*] (1022) of the message [*M*] (104) to obtain an encrypted value [c_1] (1026) and to obtain a message authentication code [*mac*] (1028);

reversibly combining the encrypted value [c_1] (1026) and the message authentication code [*mac*] (1028) to form a first signature component [*c*] (1030); and

computing a second signature component [*s*] (1032) using

(i) the first integer value [*k*] (1016);

(ii) a private key [d_A] (1012) of the signer (100, 1000); and

(iii) a second integer value dependent on the first signature component [c] (1030) and the second portion [V] (1022) of the message [M] (104); and

reversibly combining the first signature component [c] (1030), the second signature component [s] (1032) and the second portion [V] (1022) of the message [M] (104) to form the signed message (106, 1036),

wherein verification of the signed message (106, 1036) and recovery of the first portion [N] (1020) of the message [M] (104) from the signed message (106, 1036) involves a public key [G_A] (110, 1014) of the signer (100, 1000).

10. The method as recited in claim 2 or claim 3 or claim 9, wherein the finite cyclic group is a subgroup of the group of integers modulo a prime number.

11. The method as recited in claim 2 or claim 3 or claim 9, wherein the finite cyclic group is a set of points on an elliptic curve and the generator [G] is a base point of the elliptic curve.

12. A method of verifying a signed message (106, 1036), the signed message (106, 1036) having been generated by applying a signature to an original message [M] (104) that consists of a first portion [N] (1020) and a second portion [V] (1022), the method comprising:

receiving the signed message (106, 1036) purported to be signed by a signer (100, 1000), the signed message (106, 1036) having been prepared in a reversible manner from a first signature component [c] (1030), a second signature component [s] (1032), and the second portion [V] (1022) of an original message [M] (104);

extracting the first signature component [c] (1030), the second signature component [s] (1032), and the second portion [V] (1022) from the signed message (106, 1036);

receiving a public key [G_A] (110, 1014) of the signer (100, 1000);

extracting a message authentication code [*mac'*] (1056) and an encrypted value [c_1'] (1054) from the first signature component [*c*] (1030);

computing a first value [*Q'*] (1050) using the second signature component [*s*] (1032), a generator [*G*] of a finite cyclic group, the public key [G_A] (110, 1014), and an intermediate value dependent on the first signature component [*c*] (1030) and the second portion [*V*] (1022) of the message [*M*] (104);

constructing a derived key [k_1'] (1052) by applying a key derivation function [*KDF*] to input that comprises the first value [*Q'*] (1050); and

applying an authenticated decryption function, keyed by the derived key [k_1'] (1052), to the encrypted value [c_1'] (1054) and to the message authentication code [*mac'*] (1056) to determine whether the signed message (106, 1036) is valid and, where the signed message (106, 1036) is valid, to recover the first portion [*N*] (1020) of the original message [*M*] (104),

wherein the finite cyclic group is a subgroup of the group of integers modulo a prime number.

13. A method of verifying a signed message (106, 1036), the signed message (106, 1036) having been generated by applying a signature to an original message [*M*] (104) that consists of a first portion [*N*] (1020) and a second portion [*V*] (1022), the method comprising:

receiving the signed message (106, 1036) purported to be signed by a signer (100, 1000), the signed message (106, 1036) having been prepared in a reversible manner from a first signature component [*c*] (1030), a second signature component [*s*] (1032), and the second portion [*V*] (1022) of an original message [*M*] (104);

extracting the first signature component [*c*] (1030), the second signature component [*s*] (1032), and the second portion [*V*] (1022) from the signed message (106, 1036);

receiving a public key [G_A] (110, 1014) of the signer (100, 1000);

computing a first value [Q'] (1050) using the second signature component [s] (1032), the generator [G], the public key [G_A] (110, 1014), and an intermediate value dependent on the first signature component [c] (1030) and the second portion [V] (1022) of the message [M] (104);

constructing a first derived key [k_{11}'] (1052) and a second derived key [k_{12}'] (1052) by applying a key derivation function [KDF] to input that comprises the first value [Q'] (1050);

applying a decryption function, keyed by the first derived key [k_{11}'] (1052), to the first signature component [c] (1030) to obtain a result;

extracting a recovered value [N'] and the message authentication code [mac'] (1056) from the result; and

using the second derived key [k_{12}'] (1052) to determine whether the message authentication code [mac'] (1056) is valid for the first portion [N] (1020), and, where the message authentication code [mac'] (1056) is valid, recovering the first portion [N] (1020) of the original message [M], wherein the recovered value [N'] is equal to the first portion [N] (1020).

14. A method of verifying a signed message (106, 1036), the signed message (106, 1036) having been generated by applying a signature to an original message [M] (104) that consists of a first portion [N] (1020) and a second portion [V] (1022), the method comprising:

receiving the signed message (106, 1036) purported to be signed by a signer (100, 1000), the signed message (106, 1036) having been prepared in a reversible manner from a first signature component [c] (1030), a second signature component [s] (1032), and the second portion [V] (1022) of an original message [M] (104);

extracting the first signature component [c] (1030), the second signature component [s] (1032), and the second portion [V] (1022) from the signed message (106, 1036);

receiving a public key [G_A] (110, 1014) of the signer (100, 1000);

extracting a message authentication code [mac'] (1056) and an encrypted value [c_1'] (1054) from the first signature component [c] (1030);

computing a first value [Q'] (1050) using the second signature component [s] (1032), the generator [G], the public key [G_A] (110, 1014), and an intermediate value dependent on the first signature component [c] (1030) and the second portion [V] (1022) of the message [M] (104);

constructing a first derived key [k_{11}'] (1052) and a second derived key [k_{12}'] (1052) by applying a key derivation function [KDF] to input that comprises the first value [Q'] (1050); and

using the second derived key [k_{12}'] (1052) to determine whether the message authentication code [mac'] (1056) is valid for the encrypted value [c_1'] (1054), and where the message authentication code [mac'] (1056) is valid, applying a decryption function, keyed by the first derived key [k_{11}'] (1052), to the encrypted value [c_1'] (1054) to recover the first portion [N] (1020).

15. The method as recited in claim 13 or claim 14, the method further comprising:

constructing the first derived key [k_{11}'] (1052) by applying the key derivation function [KDF] to input that comprises the first value [Q'] (1050) and first auxiliary information; and

constructing the second derived key [k_{12}'] (1052) by applying the key derivation function [KDF] to input that comprises the first value [Q'] (1050) and second auxiliary information.

16. The method as recited in claim 15, wherein the second auxiliary information is different than the first auxiliary information.

17. The method as recited in claim 13 or claim 14, the method further comprising:

applying the key derivation function [*KDF*] to input that comprises the first value [*Q'*] (1050) to obtain a key;

dividing the key into a first part and a second part; and

constructing the first derived key [k_{11}'] (1052) from the first part and constructing the second derived key [k_{12}'] (1052) from the second part.

18. A method of verifying a signed message (106, 1036), the signed message (106, 1036) having been generated by applying a signature to an original message [*M*] (104) that consists of a first portion [*N*] (1020) and a second portion [*V*] (1022), the method comprising:

receiving the signed message (106, 1036) purported to be signed by a signer (100, 1000), the signed message (106, 1036) having been prepared in a reversible manner from a first signature component [*c*] (1030), a second signature component [*s*] (1032), and the second portion [*V*] (1022) of an original message [*M*] (104);

extracting the first signature component [*c*] (1030), the second signature component [*s*] (1032), and the second portion [*V*] (1022) from the signed message (106, 1036);

receiving a public key [G_A] (110, 1014) of the signer (100, 1000);

extracting a message authentication code [*mac'*] (1056) and an encrypted value [c_1'] (1054) from the first signature component [*c*] (1030);

computing a first value [*Q'*] (1050) using the second signature component [*s*] (1032), the generator [*G*], the public key [G_A] (110, 1014), and the message authentication code [*mac'*] (1056);

constructing a derived key [k_1'] (1052) by applying a key derivation function [*KDF*] to input that comprises the first value [*Q'*] (1050); and

applying an authenticated-decryption-with-associated-data function, keyed by the derived key [k_1'] (1052), to the encrypted value [c_1'] (1054), to the message authentication code [*mac'*] (1056) and to the second portion [*V*] (1022) to determine whether the signed message (106, 1036) is valid and, where the signed message (106, 1036) is valid, to recover the first portion [*N*] (1020) of the original message [*M*] (104).

19. The method as recited in claim 13 or claim 14 or claim 18, wherein the finite cyclic group is a subgroup of the group of integers modulo a prime number.

20. The method as recited in claim 13 or claim 14 or claim 18, wherein the finite cyclic group is a set of points on an elliptic curve and the generator [*G*] is a base point of the elliptic curve.

21. A signer device (100, 1000) comprising:

a processor (1002);

a communication interface (1006) coupled to the processor (1002); and

a memory (1004) coupled to the processor (1002), the memory (1004) storing code (1008) which, when executed by the processor (1002), is arranged to perform any one of the methods as recited in claims 1 to 11.

22. A verifier device (102, 1040) comprising:

a processor (1042);

a communication interface (1046) coupled to the processor (1042); and

a memory (1044) coupled to the processor (1042), the memory (1044) storing code (1048) which, when executed by the processor (1002), is arranged to perform any one of the methods as recited in claims 12 to 20.

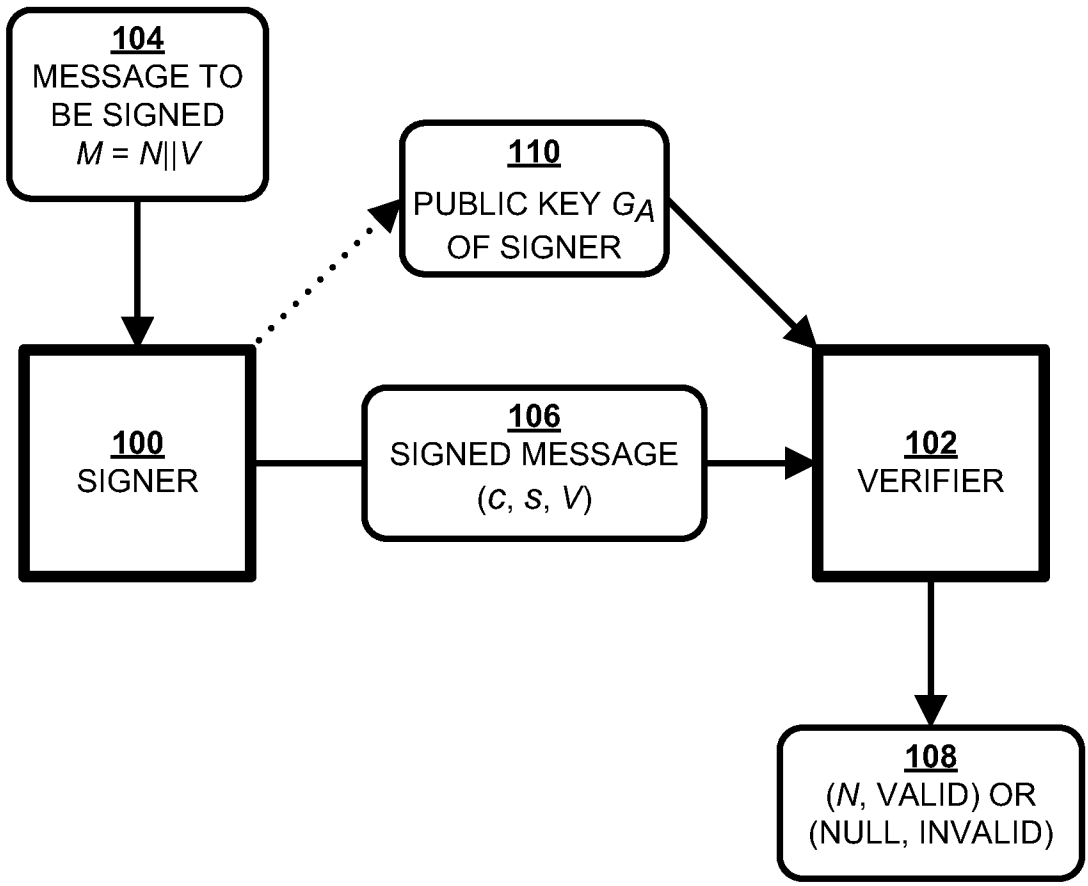
104
MESSAGE TO BE SIGNED
M = N||V
110
PUBLIC KEY G_A OF SIGNER
100
SIGNER
106
SIGNED MESSAGE
(c, s, V)
102
VERIFIER
108
(N, VALID) OR
(NULL, INVALID)

FIG. 1

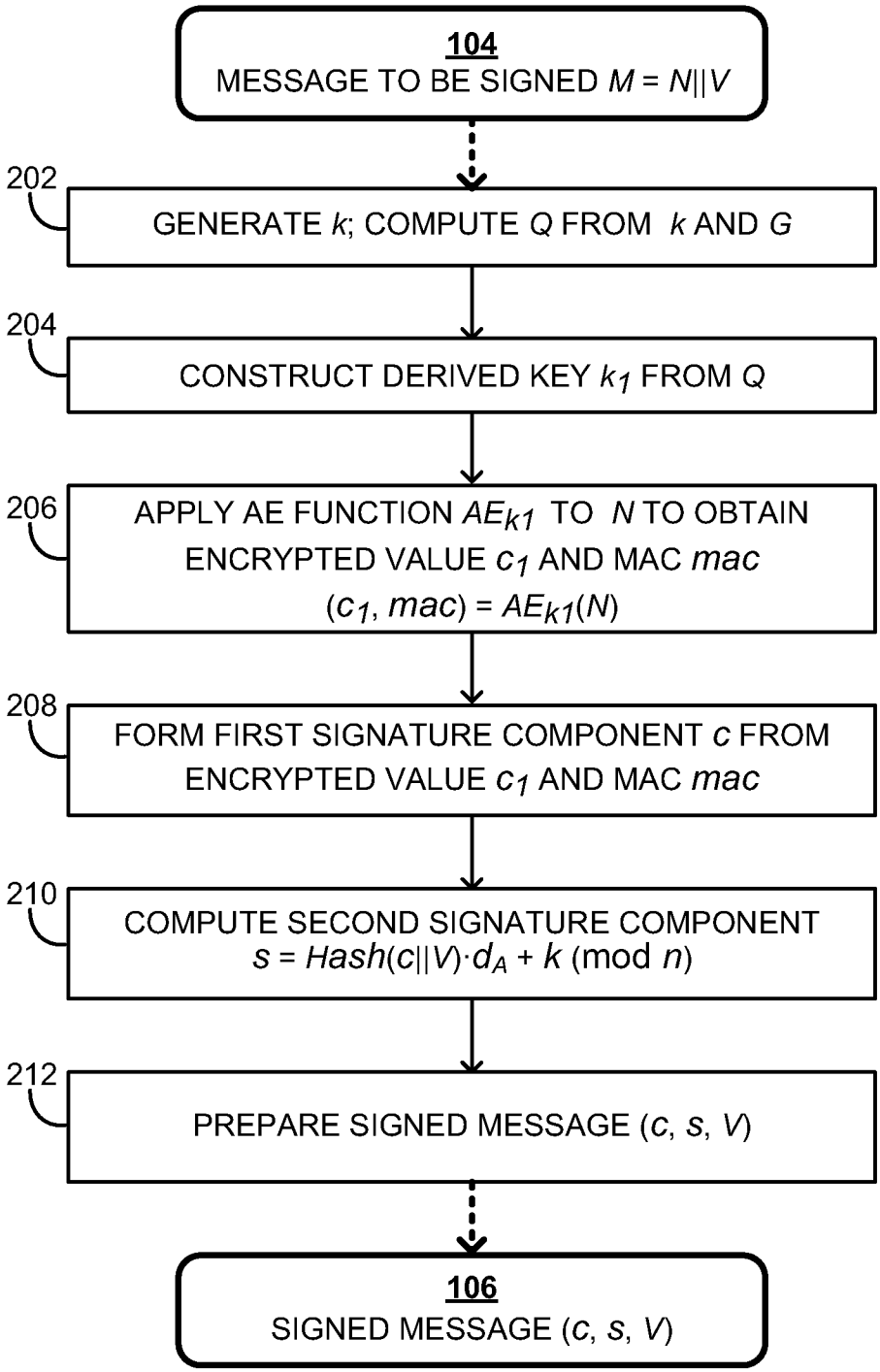
104
MESSAGE TO BE SIGNED $M = N||V$
202
GENERATE k; COMPUTE Q FROM k AND G
204
CONSTRUCT DERIVED KEY k_1 FROM Q
206
APPLY AE FUNCTION AE_{k1} TO N TO OBTAIN ENCRYPTED VALUE c_1 AND MAC mac
$(c_1, mac) = AE_{k1}(N)$
208
FORM FIRST SIGNATURE COMPONENT c FROM ENCRYPTED VALUE c_1 AND MAC mac
210
COMPUTE SECOND SIGNATURE COMPONENT
$s = Hash(c||V) \cdot d_A + k \pmod n$
212
PREPARE SIGNED MESSAGE (c, s, V)
106
SIGNED MESSAGE (c, s, V)

FIG. 2

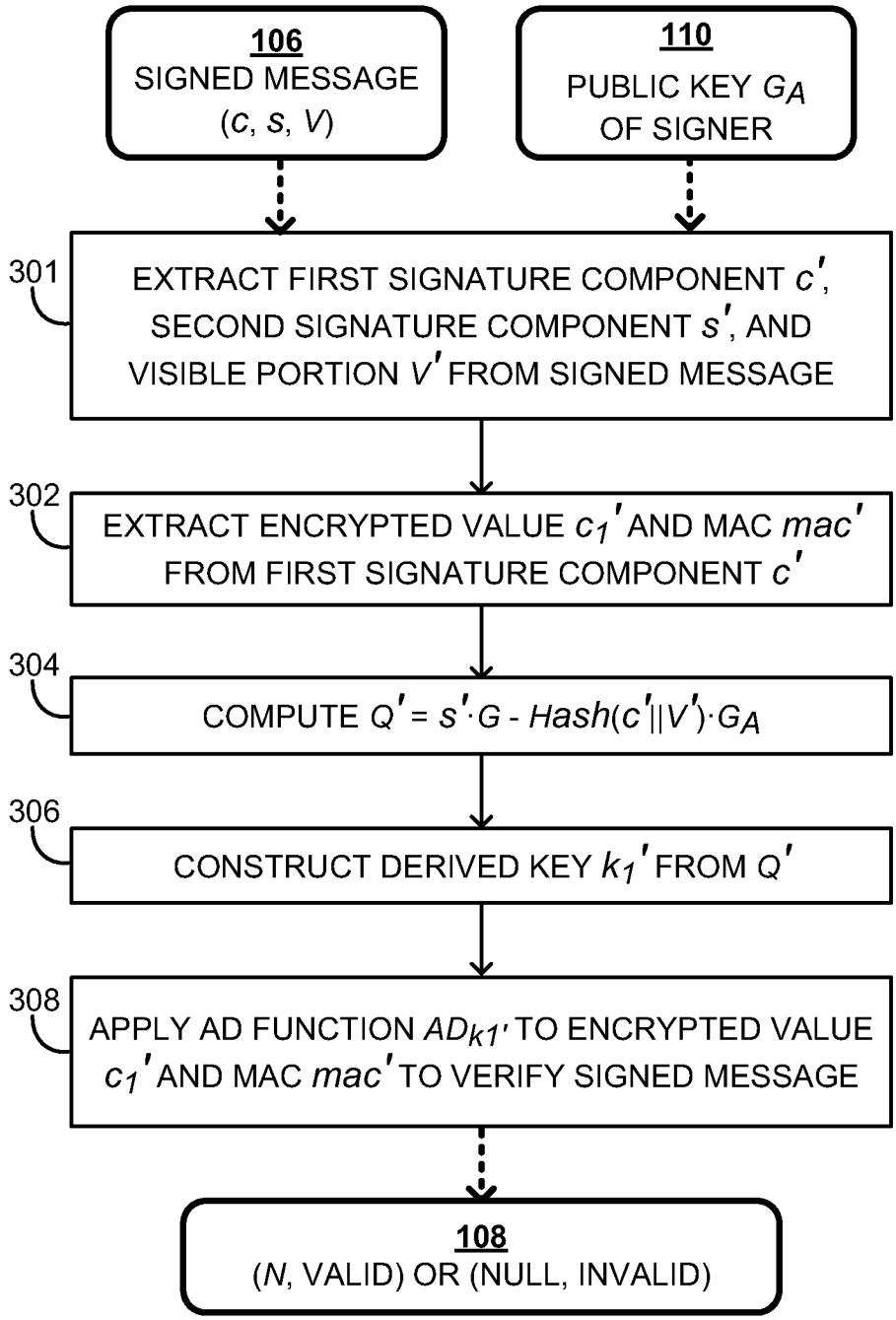
106
SIGNED MESSAGE
(c, s, V)
110
PUBLIC KEY G_A
OF SIGNER
301
EXTRACT FIRST SIGNATURE COMPONENT c',
SECOND SIGNATURE COMPONENT s', AND
VISIBLE PORTION V' FROM SIGNED MESSAGE
302
EXTRACT ENCRYPTED VALUE c_1' AND MAC mac'
FROM FIRST SIGNATURE COMPONENT c'
304
COMPUTE $Q' = s' \cdot G - Hash(c' || V') \cdot G_A$
306
CONSTRUCT DERIVED KEY k_1' FROM Q'
308
APPLY AD FUNCTION $AD_{k1'}$ TO ENCRYPTED VALUE
c_1' AND MAC mac' TO VERIFY SIGNED MESSAGE
108
(N, VALID) OR (NULL, INVALID)

FIG. 3

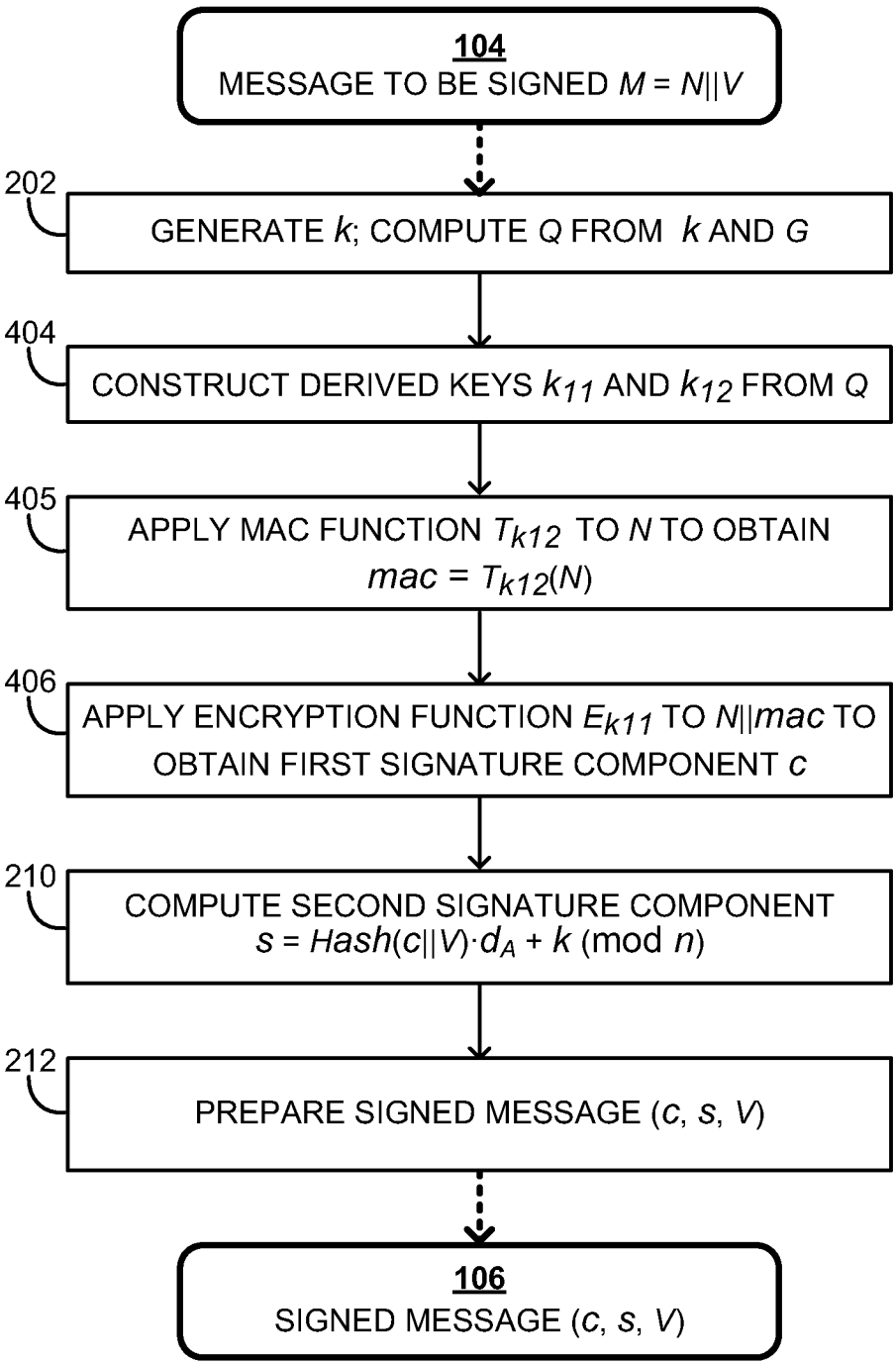
104
MESSAGE TO BE SIGNED M = N||V
202
GENERATE k; COMPUTE Q FROM k AND G
404
CONSTRUCT DERIVED KEYS k11 AND k12 FROM Q
405
APPLY MAC FUNCTION Tk12 TO N TO OBTAIN
mac = Tk12(N)
406
APPLY ENCRYPTION FUNCTION Ek11 TO N||mac TO
OBTAIN FIRST SIGNATURE COMPONENT c
210
COMPUTE SECOND SIGNATURE COMPONENT
s = Hash(c||V)·dA + k (mod n)
212
PREPARE SIGNED MESSAGE (c, s, V)
106
SIGNED MESSAGE (c, s, V)

FIG. 4

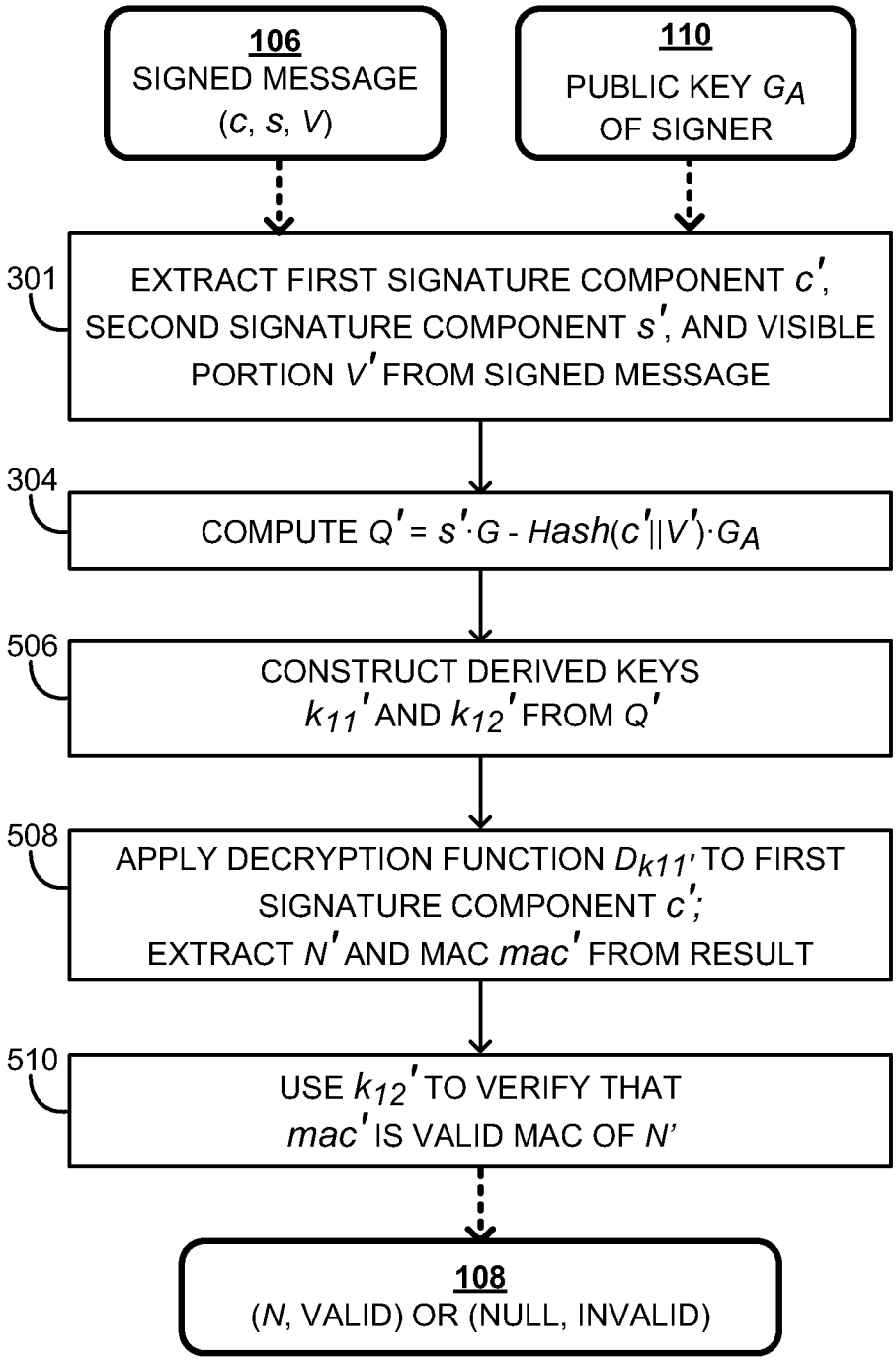
106
SIGNED MESSAGE
(c, s, V)
110
PUBLIC KEY G_A
OF SIGNER
301
EXTRACT FIRST SIGNATURE COMPONENT c',
SECOND SIGNATURE COMPONENT s', AND VISIBLE
PORTION V' FROM SIGNED MESSAGE
304
COMPUTE $Q' = s' \cdot G - Hash(c' || V') \cdot G_A$
506
CONSTRUCT DERIVED KEYS
k_{11}' AND k_{12}' FROM Q'
508
APPLY DECRYPTION FUNCTION $D_{k11'}$ TO FIRST
SIGNATURE COMPONENT c';
EXTRACT N' AND MAC mac' FROM RESULT
510
USE k_{12}' TO VERIFY THAT
mac' IS VALID MAC OF N'
108
(N, VALID) OR (NULL, INVALID)

FIG. 5

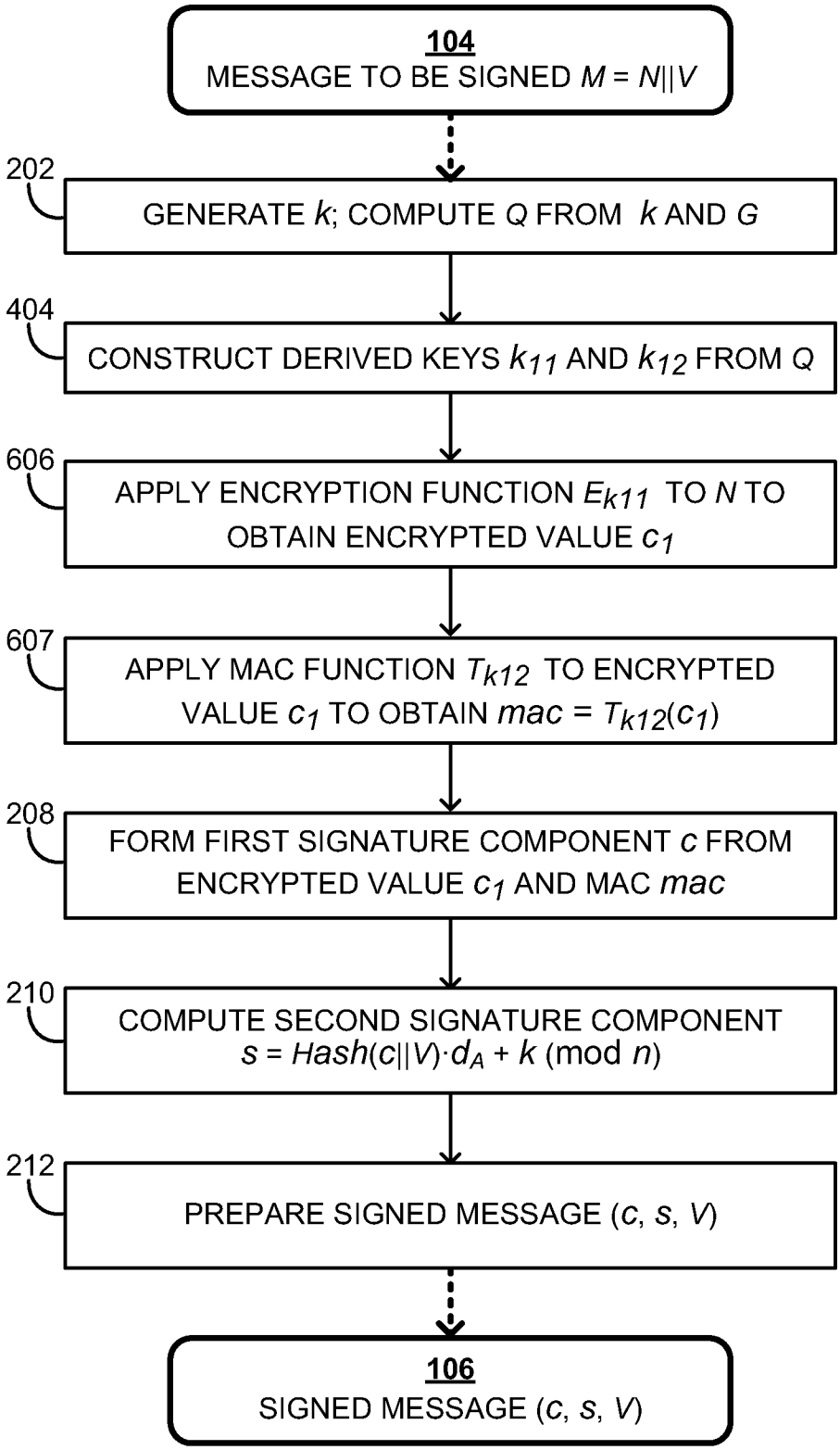
104
MESSAGE TO BE SIGNED $M = N||V$
202
GENERATE k; COMPUTE Q FROM k AND G
404
CONSTRUCT DERIVED KEYS k_{11} AND k_{12} FROM Q
606
APPLY ENCRYPTION FUNCTION E_{k11} TO N TO OBTAIN ENCRYPTED VALUE c_1
607
APPLY MAC FUNCTION T_{k12} TO ENCRYPTED VALUE c_1 TO OBTAIN $mac = T_{k12}(c_1)$
208
FORM FIRST SIGNATURE COMPONENT c FROM ENCRYPTED VALUE c_1 AND MAC mac
210
COMPUTE SECOND SIGNATURE COMPONENT $s = Hash(c||V) \cdot d_A + k \pmod{n}$
212
PREPARE SIGNED MESSAGE (c, s, V)
106
SIGNED MESSAGE (c, s, V)

FIG. 6

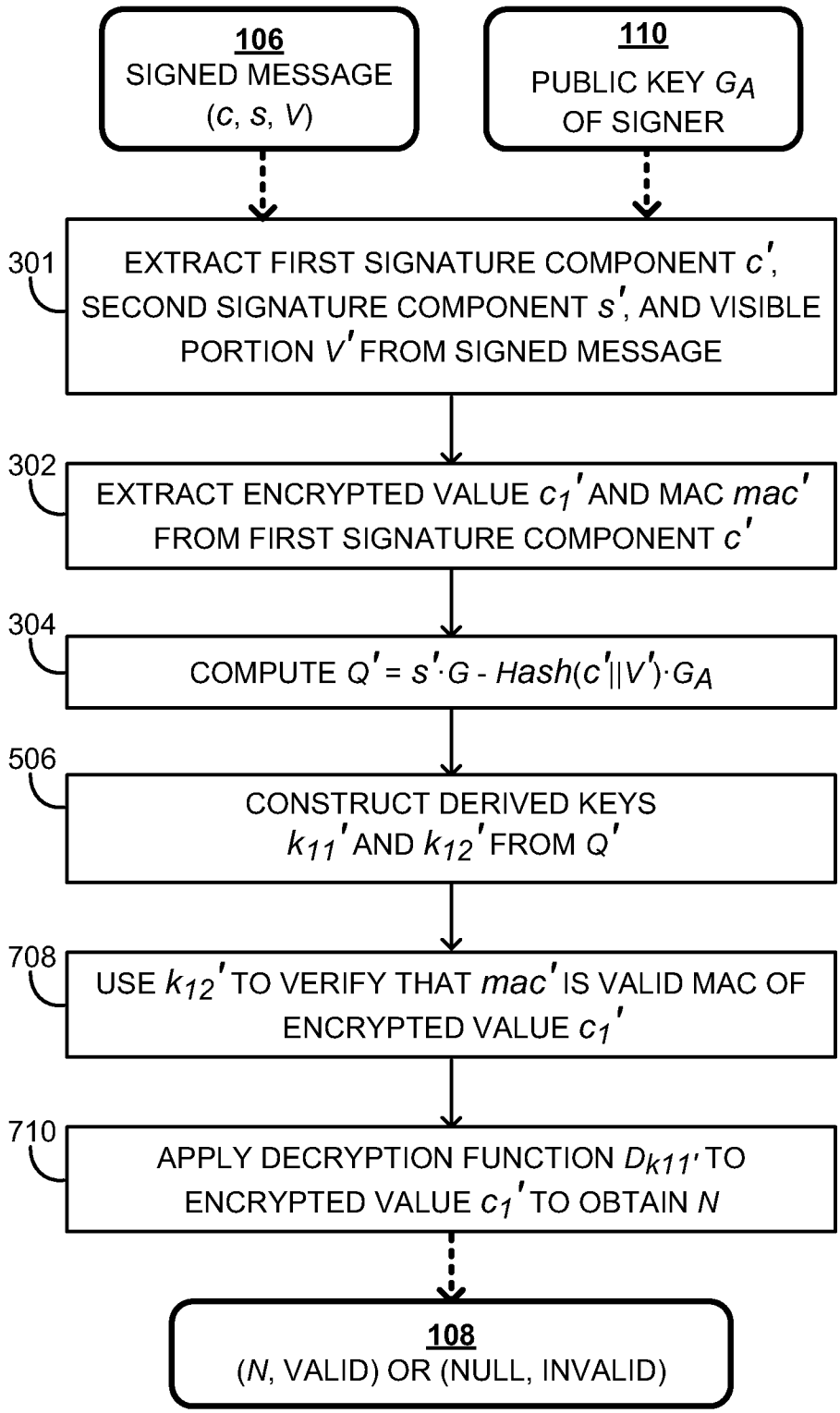
106
SIGNED MESSAGE
(c, s, V)
110
PUBLIC KEY G_A
OF SIGNER
301
EXTRACT FIRST SIGNATURE COMPONENT c',
SECOND SIGNATURE COMPONENT s', AND VISIBLE
PORTION V' FROM SIGNED MESSAGE
302
EXTRACT ENCRYPTED VALUE c_1' AND MAC mac'
FROM FIRST SIGNATURE COMPONENT c'
304
COMPUTE $Q' = s' \cdot G - Hash(c' || V') \cdot G_A$
506
CONSTRUCT DERIVED KEYS
k_{11}' AND k_{12}' FROM Q'
708
USE k_{12}' TO VERIFY THAT mac' IS VALID MAC OF
ENCRYPTED VALUE c_1'
710
APPLY DECRYPTION FUNCTION $D_{k11'}$ TO
ENCRYPTED VALUE c_1' TO OBTAIN N
108
(N, VALID) OR (NULL, INVALID)

FIG. 7

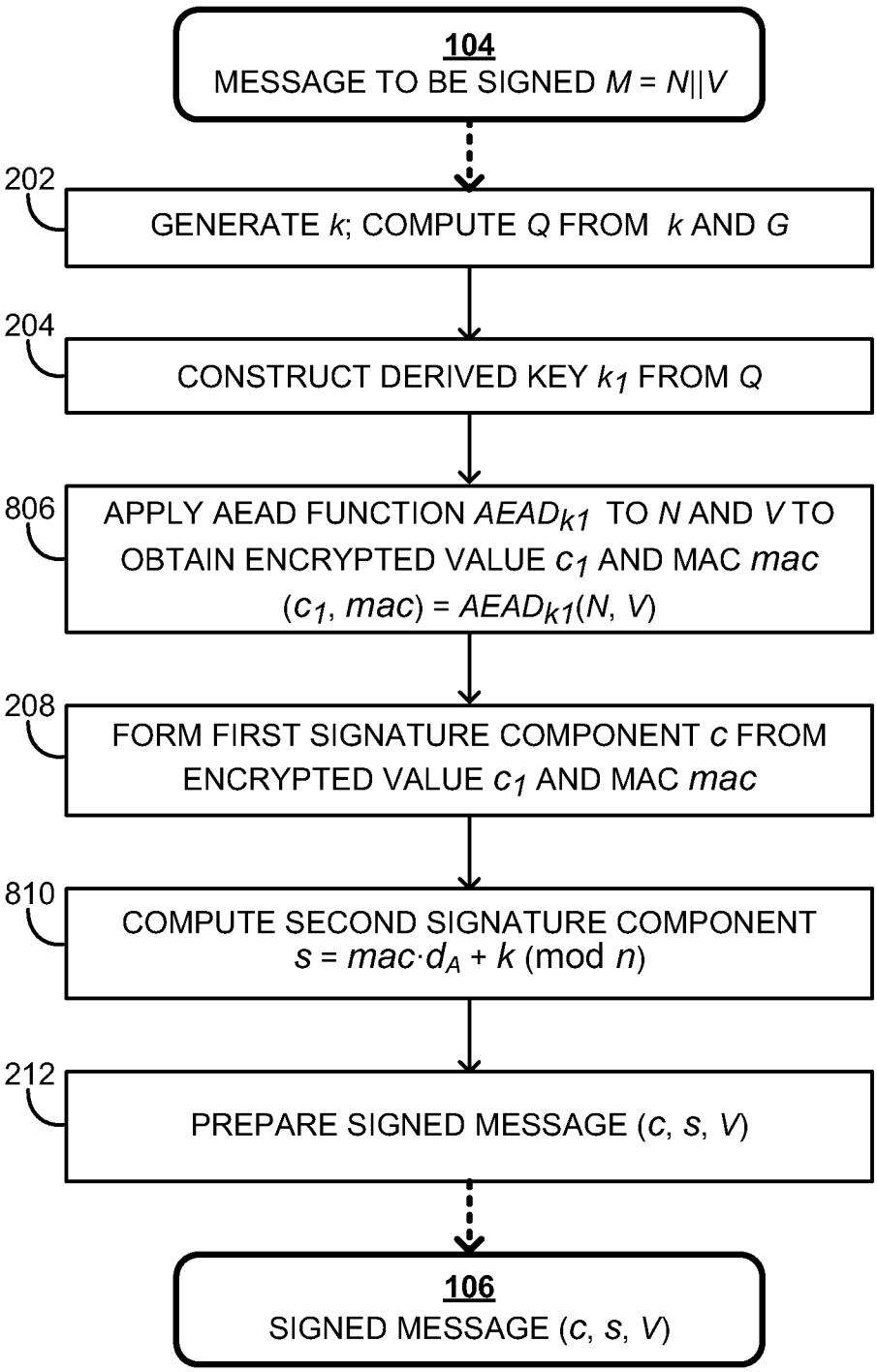
104
MESSAGE TO BE SIGNED M = N||V
202
GENERATE k; COMPUTE Q FROM k AND G
204
CONSTRUCT DERIVED KEY k1 FROM Q
806
APPLY AEAD FUNCTION AEADk1 TO N AND V TO OBTAIN ENCRYPTED VALUE c1 AND MAC mac
(c1, mac) = AEADk1(N, V)
208
FORM FIRST SIGNATURE COMPONENT c FROM ENCRYPTED VALUE c1 AND MAC mac
810
COMPUTE SECOND SIGNATURE COMPONENT
s = mac·dA + k (mod n)
212
PREPARE SIGNED MESSAGE (c, s, V)
106
SIGNED MESSAGE (c, s, V)

FIG. 8

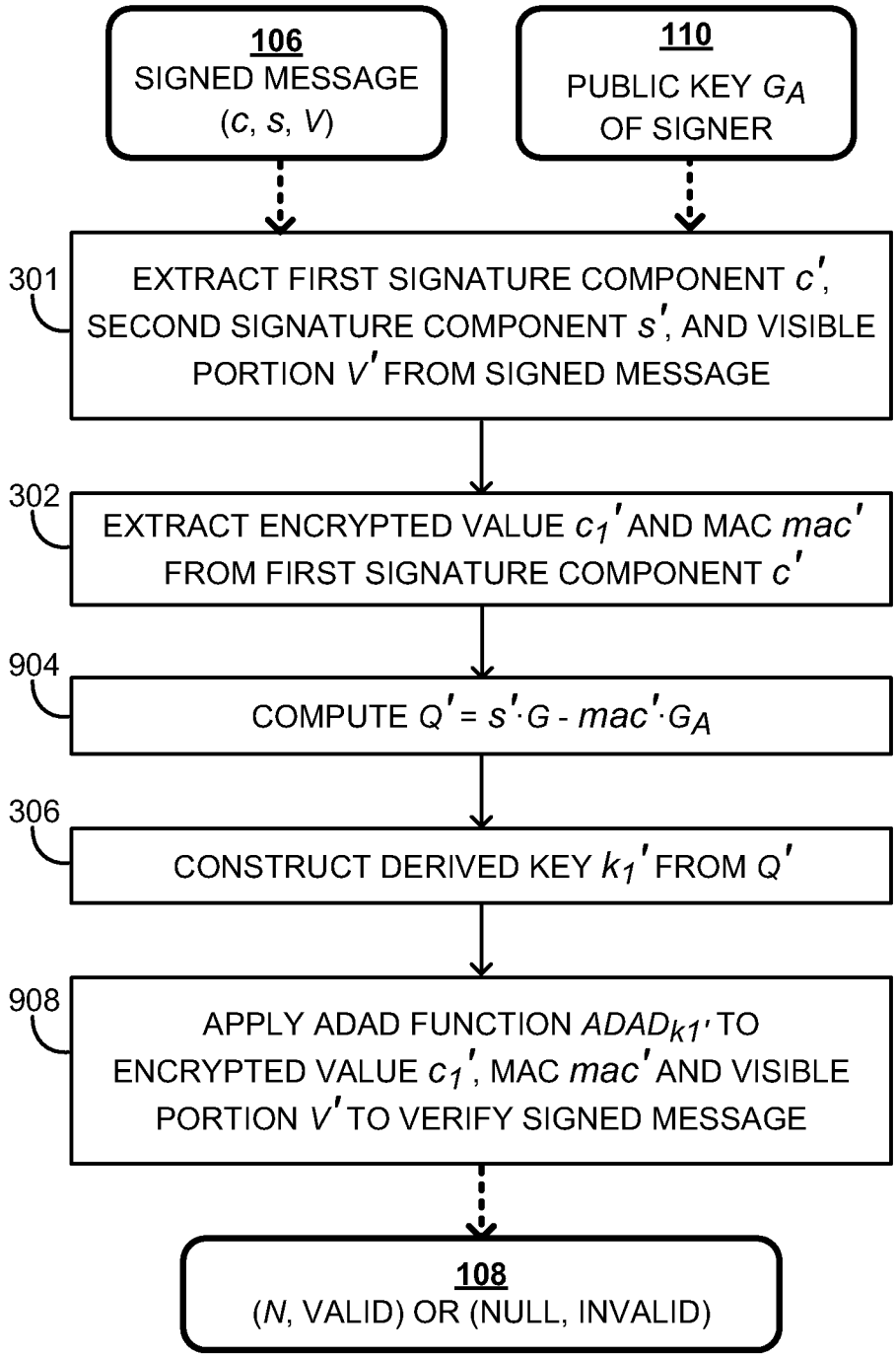
106
SIGNED MESSAGE
(c, s, V)
110
PUBLIC KEY G_A
OF SIGNER
301
EXTRACT FIRST SIGNATURE COMPONENT c', SECOND SIGNATURE COMPONENT s', AND VISIBLE PORTION V' FROM SIGNED MESSAGE
302
EXTRACT ENCRYPTED VALUE c_1' AND MAC mac' FROM FIRST SIGNATURE COMPONENT c'
904
COMPUTE $Q' = s' \cdot G - mac' \cdot G_A$
306
CONSTRUCT DERIVED KEY k_1' FROM Q'
908
APPLY ADAD FUNCTION $ADAD_{k1'}$ TO ENCRYPTED VALUE c_1', MAC mac' AND VISIBLE PORTION V' TO VERIFY SIGNED MESSAGE
108
(N, VALID) OR (NULL, INVALID)

FIG. 9

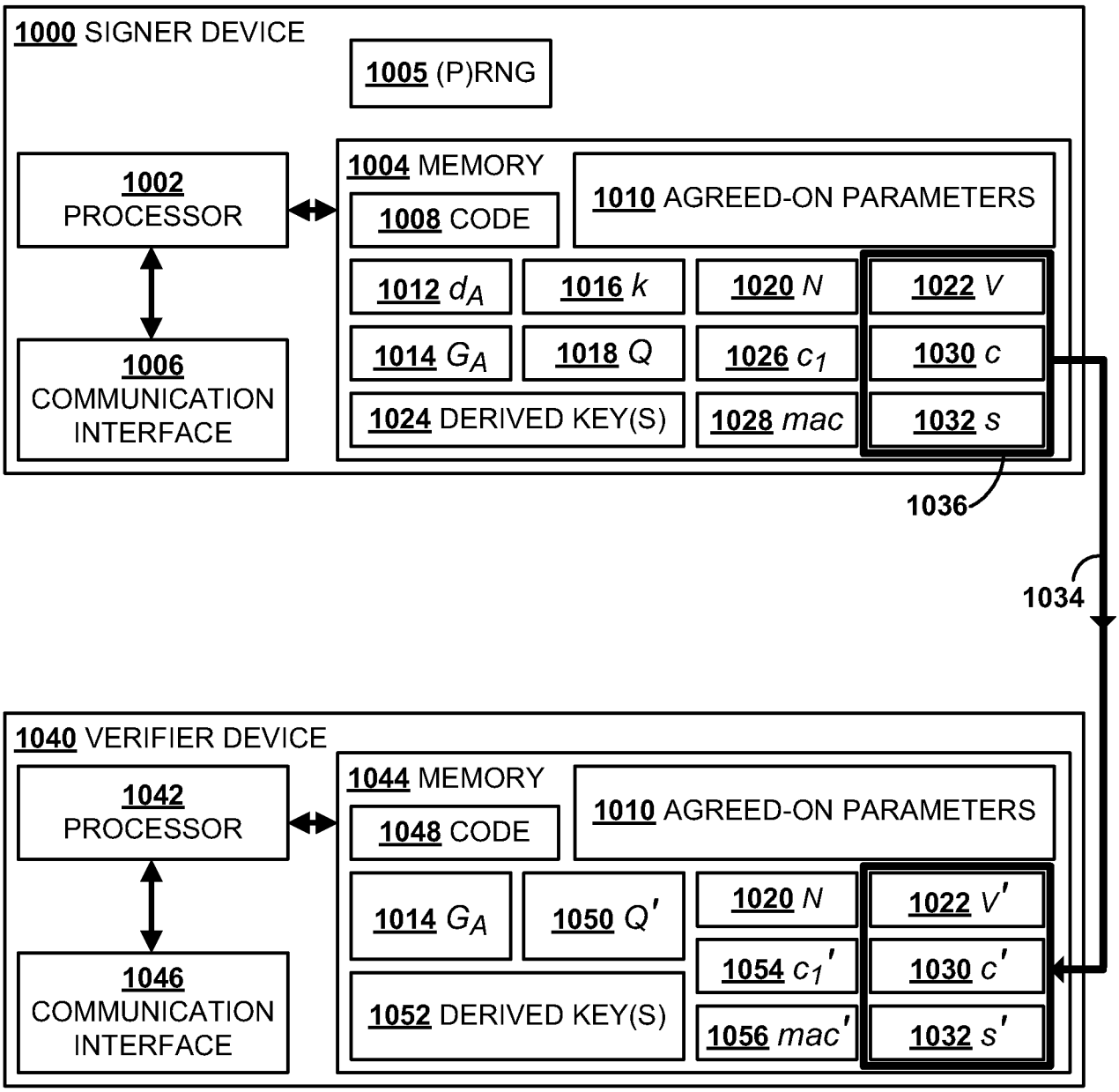
1000 SIGNER DEVICE
1005 (P)RNG
1002 PROCESSOR
1004 MEMORY
1008 CODE
1010 AGREED-ON PARAMETERS
1012 d_A
1016 k
1020 N
1022 V
1014 G_A
1018 Q
1026 c_1
1030 c
1024 DERIVED KEY(S)
1028 mac
1032 s
1006 COMMUNICATION INTERFACE
1036
1034
1040 VERIFIER DEVICE
1042 PROCESSOR
1044 MEMORY
1048 CODE
1010 AGREED-ON PARAMETERS
1014 G_A
1050 Q'
1020 N
1022 V'
1054 c_1'
1030 c'
1052 DERIVED KEY(S)
1056 mac'
1032 s'
1046 COMMUNICATION INTERFACE

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2011/054490

A. CLASSIFICATION OF SUBJECT MATTER
IPC: ***H04L 9/32*** (2006.01) , ***H04L 12/58*** (2006.01) , ***H04L 9/00*** (2006.01)
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 (2006.01)

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

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
EPOQUE, Google, Google Scholar.
Keywords: signature, key, first_portion, second_portion, encryption, derived key, finite cyclic and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2005/0271246A1 (Sharma et al.) 08 December 2005 (08-12-2005) * see whole document	1 to 22
A	US 7,286,665B1 (Wang) 23 October 2007 (23-10-2007) * see whole document	1 to 22
A	US 2005/0262351A1 (Levy) 24 November 2005 (24-11-2005) * see whole document	1 to 22

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

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 January 2012 (18-01-2012)	6 February 2012 (06-02-2012)

Name and mailing address of the ISA/CA	Authorized officer
Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001-819-953-2476	Arthur Winnik (819) 934-7880

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IB2011/054490

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US2005271246A1	08 December 2005 (08-12-2005)	US2005271246A1	08 December 2005 (08-12-2005)
		AT199469T	15 March 2001 (15-03-2001)
		AT216546T	15 May 2002 (15-05-2002)
		AT230539T	15 January 2003 (15-01-2003)
		AT237197T	15 April 2003 (15-04-2003)
		AT245328T	15 August 2003 (15-08-2003)
		AT261225T	15 March 2004 (15-03-2004)
		AT287176T	15 January 2005 (15-01-2005)
		AT289435T	15 March 2005 (15-03-2005)
		AT304727T	15 September 2005 (15-09-2005)
		AT358850T	15 April 2007 (15-04-2007)
		AT372559T	15 September 2007 (15-09-2007)
		AT383617T	15 January 2008 (15-01-2008)
		AT387807T	15 March 2008 (15-03-2008)
		AT418233T	15 January 2009 (15-01-2009)
		AT420529T	15 January 2009 (15-01-2009)
		AT435757T	15 July 2009 (15-07-2009)
		AT485677T	15 November 2010 (15-11-2010)
		AT491190T	15 December 2010 (15-12-2010)
		AT502354T	15 April 2011 (15-04-2011)
		AT522081T	15 September 2011 (15-09-2011)
		AU747372B2	16 May 2002 (16-05-2002)
		AU761566B2	05 June 2003 (05-06-2003)
		AU1102201A	06 June 2001 (06-06-2001)
		AU1163402A	22 April 2002 (22-04-2002)
		AU1232001A	14 May 2001 (14-05-2001)
		AU1232101A	14 May 2001 (14-05-2001)
		AU1624800A	13 June 2000 (13-06-2000)
		AU1809300A	22 May 2000 (22-05-2000)
		AU1935001A	12 June 2001 (12-06-2001)
		AU2295701A	16 July 2001 (16-07-2001)
		AU2296502A	30 January 2002 (30-01-2002)
		AU2297302A	30 January 2002 (30-01-2002)
		AU2369500A	03 July 2000 (03-07-2000)
		AU2463499A	02 August 1999 (02-08-1999)
		AU2559302A	29 April 2002 (29-04-2002)
		AU2593101A	09 July 2001 (09-07-2001)
		AU2936201A	24 July 2001 (24-07-2001)
		AU2940201A	24 July 2001 (24-07-2001)
		AU3008697A	05 December 1997 (05-12-1997)
		AU3281702A	01 July 2002 (01-07-2002)
		AU3293402A	06 May 2002 (06-05-2002)
		AU3458101A	07 August 2001 (07-08-2001)
		AU3523102A	01 July 2002 (01-07-2002)
		AU3562999A	01 November 1999 (01-11-1999)
		AU3667802A	21 May 2002 (21-05-2002)
		AU3701701A	27 August 2001 (27-08-2001)
		AU3736800A	28 September 2000 (28-09-2000)
		AU3801301A	14 August 2001 (14-08-2001)
		AU3966002A	01 July 2002 (01-07-2002)
		AU4010501A	24 September 2001 (24-09-2001)
		AU4745701A	03 October 2001 (03-10-2001)
		AU4836799A	21 February 2000 (21-02-2000)
		AU4851300A	05 December 2000 (05-12-2000)
		AU5145700A	05 December 2000 (05-12-2000)
		AU5544501A	30 October 2001 (30-10-2001)
		AU5544601A	07 November 2001 (07-11-2001)
		AU5931301A	12 November 2001 (12-11-2001)
		AU5965201A	20 November 2001 (20-11-2001)
		AU6022396A	29 November 1996 (29-11-1996)
		AU6694901A	02 January 2002 (02-01-2002)
		AU7318401A	13 February 2002 (13-02-2002)
		AU7704701A	05 February 2002 (05-02-2002)
		AU7714701A	05 February 2002 (05-02-2002)

AU8307301A	18 February 2002 (18-02-2002)
AU9033098A	16 March 1999 (16-03-1999)
AU9082201A	26 March 2002 (26-03-2002)
AU9265901A	26 March 2002 (26-03-2002)
AU9634301A	08 April 2002 (08-04-2002)
AU2001277047B2	06 September 2007 (06-09-2007)
AU2001277147B2	18 May 2006 (18-05-2006)
AU2002305304A1	11 November 2002 (11-11-2002)
AU2002353174A1	15 July 2003 (15-07-2003)
AU2002364036A1	15 July 2003 (15-07-2003)
AU2002364255A1	15 July 2003 (15-07-2003)
AU2003210625A1	02 September 2003 (02-09-2003)
AU2003217642A1	09 September 2003 (09-09-2003)
AU2003217642A8	09 September 2003 (09-09-2003)
AU2003220245A1	29 September 2003 (29-09-2003)
AU2003221894A1	27 October 2003 (27-10-2003)
AU2003221894A8	27 October 2003 (27-10-2003)
AU2003285891A1	04 May 2004 (04-05-2004)
AU2003293087A1	23 June 2004 (23-06-2004)
AU2005205804A1	29 September 2005 (29-09-2005)
AU2009200468A1	26 February 2009 (26-02-2009)
AU2009200468B2	31 March 2011 (31-03-2011)
AU2009202090A1	18 June 2009 (18-06-2009)
BR9907105A	30 April 2002 (30-04-2002)
CA2174413A1	26 May 1995 (26-05-1995)
CA2174413C	09 June 2009 (09-06-2009)
CA2218957A1	14 November 1996 (14-11-1996)
CA2218957C	25 January 2005 (25-01-2005)
CA2301218A1	04 March 1999 (04-03-1999)
CA2318564A1	22 July 1999 (22-07-1999)
CA2318564C	21 July 2009 (21-07-2009)
CA2326565A1	21 October 1999 (21-10-1999)
CA2326565C	15 September 2009 (15-09-2009)
CA2338618A1	10 February 2000 (10-02-2000)
CA2338618C	04 July 2006 (04-07-2006)
CA2347179A1	11 May 2000 (11-05-2000)
CA2355715A1	22 June 2000 (22-06-2000)
CA2364433A1	14 September 2000 (14-09-2000)
CA2364433C	19 July 2011 (19-07-2011)
CA2373208A1	23 November 2000 (23-11-2000)
CA2373511A1	23 November 2000 (23-11-2000)
CA2416530A1	31 January 2002 (31-01-2002)
CA2416530C	21 October 2008 (21-10-2008)
CA2416532A1	31 January 2002 (31-01-2002)
CA2422081A1	02 May 2002 (02-05-2002)
CA2422081C	21 August 2007 (21-08-2007)
CA2422412A1	18 April 2002 (18-04-2002)
CA2469938A1	10 July 2003 (10-07-2003)
CA2469938C	15 September 2009 (15-09-2009)
CA2470547A1	10 July 2003 (10-07-2003)
CA2470547C	20 May 2008 (20-05-2008)
CA2471457A1	10 July 2003 (10-07-2003)
CA2471457C	02 August 2011 (02-08-2011)
CA2476895A1	28 August 2003 (28-08-2003)
CA2483419A1	14 November 1996 (14-11-1996)
CA2502232A1	29 April 2004 (29-04-2004)
CA2522551A1	04 November 2004 (04-11-2004)
CA2522551C	22 December 2009 (22-12-2009)
CA2532296A1	03 February 2005 (03-02-2005)
CA2666703A1	22 July 1999 (22-07-1999)
CA2671998A1	10 July 2003 (10-07-2003)
CN1628318A	15 June 2005 (15-06-2005)
CN1316421C	16 May 2007 (16-05-2007)
CN1631030A	22 June 2005 (22-06-2005)
CN100364309C	23 January 2008 (23-01-2008)
CN101159799A	09 April 2008 (09-04-2008)
DE60127689D1	16 May 2007 (16-05-2007)
DE60127689T2	06 September 2007 (06-09-2007)
DE60144222D1	28 April 2011 (28-04-2011)
DE60232918D1	20 August 2009 (20-08-2009)

DE69426787D1	05 April 2001 (05-04-2001)
DE69426787T2	30 August 2001 (30-08-2001)
DE69432480D1	15 May 2003 (15-05-2003)
DE69432480T2	18 March 2004 (18-03-2004)
DE69434237D1	17 February 2005 (17-02-2005)
DE69434237T2	08 December 2005 (08-12-2005)
DE69435076D1	10 April 2008 (10-04-2008)
DE69435076T2	26 March 2009 (26-03-2009)
DE69435317D1	02 December 2010 (02-12-2010)
DE69620751D1	23 May 2002 (23-05-2002)
DE69620751T2	31 October 2002 (31-10-2002)
DE69625626D1	06 February 2003 (06-02-2003)
DE69625626T2	16 October 2003 (16-10-2003)
DE69629134D1	21 August 2003 (21-08-2003)
DE69629134T2	15 April 2004 (15-04-2004)
DE69631806D1	08 April 2004 (08-04-2004)
DE69631806T2	03 February 2005 (03-02-2005)
DE69637782D1	29 January 2009 (29-01-2009)
DE69739209D1	26 February 2009 (26-02-2009)
DE69923781D1	24 March 2005 (24-03-2005)
DE69923781T2	07 July 2005 (07-07-2005)
DE69927218D1	20 October 2005 (20-10-2005)
DE69927218T2	12 January 2006 (12-01-2006)
DE69937044D1	18 October 2007 (18-10-2007)
DE69937044T2	03 January 2008 (03-01-2008)
DE69937972D1	21 February 2008 (21-02-2008)
DE69937972T2	08 January 2009 (08-01-2009)
DE602004030434D1	20 January 2011 (20-01-2011)
EP0737387A1	16 October 1996 (16-10-1996)
EP0737387B1	09 April 2003 (09-04-2003)
EP0824821A2	25 February 1998 (25-02-1998)
EP0824821B1	17 April 2002 (17-04-2002)
EP0959620A1	24 November 1999 (24-11-1999)
EP0959620B1	12 January 2005 (12-01-2005)
EP0959621A1	24 November 1999 (24-11-1999)
EP0959621B1	28 February 2001 (28-02-2001)
EP0961239A2	01 December 1999 (01-12-1999)
EP0961239A3	28 February 2001 (28-02-2001)
EP0981113A2	23 February 2000 (23-02-2000)
EP0981113A3	14 March 2001 (14-03-2001)
EP0981113B1	14 September 2005 (14-09-2005)
EP0987855A2	22 March 2000 (22-03-2000)
EP1003324A2	24 May 2000 (24-05-2000)
EP1003324A3	31 May 2000 (31-05-2000)
EP1003324B1	16 July 2003 (16-07-2003)
EP1008097A1	14 June 2000 (14-06-2000)
EP1008097A4	21 March 2001 (21-03-2001)
EP1019868A2	19 July 2000 (19-07-2000)
EP1019868A4	07 February 2001 (07-02-2001)
EP1019868B1	07 January 2009 (07-01-2009)
EP1049320A1	02 November 2000 (02-11-2000)
EP1049320A8	02 May 2001 (02-05-2001)
EP1049320B1	02 January 2003 (02-01-2003)
EP1050005A2	08 November 2000 (08-11-2000)
EP1050005A4	18 July 2001 (18-07-2001)
EP1050005B1	05 September 2007 (05-09-2007)
EP1054335A2	22 November 2000 (22-11-2000)
EP1054335A3	17 December 2003 (17-12-2003)
EP1131769A2	12 September 2001 (12-09-2001)
EP1131769A4	19 March 2003 (19-03-2003)
EP1131769B1	16 February 2005 (16-02-2005)
EP1137251A2	26 September 2001 (26-09-2001)
EP1137251A3	06 March 2002 (06-03-2002)
EP1137251B1	03 March 2004 (03-03-2004)
EP1137975A1	04 October 2001 (04-10-2001)
EP1142190A1	10 October 2001 (10-10-2001)
EP1142190A4	25 May 2005 (25-05-2005)
EP1157499A1	28 November 2001 (28-11-2001)

EP1157499A4	09 July 2003 (09-07-2003)
EP1185967A1	13 March 2002 (13-03-2002)
EP1185967A4	03 November 2004 (03-11-2004)
EP1208499A1	29 May 2002 (29-05-2002)
EP1208499A4	07 November 2007 (07-11-2007)
EP1232472A1	21 August 2002 (21-08-2002)
EP1249002A1	16 October 2002 (16-10-2002)
EP1249002A4	13 September 2006 (13-09-2006)
EP1249002B1	16 March 2011 (16-03-2011)
EP1257921A1	20 November 2002 (20-11-2002)
EP1257921A4	20 September 2006 (20-09-2006)
EP1257931A1	20 November 2002 (20-11-2002)
EP1257931A4	22 November 2006 (22-11-2006)
EP1264268A1	11 December 2002 (11-12-2002)
EP1266475A1	18 December 2002 (18-12-2002)
EP1266475A4	27 July 2005 (27-07-2005)
EP1311973A1	21 May 2003 (21-05-2003)
EP1311973A4	20 October 2004 (20-10-2004)
EP1311973B1	04 April 2007 (04-04-2007)
EP1312030A2	21 May 2003 (21-05-2003)
EP1312030A4	11 July 2007 (11-07-2007)
EP1312030B1	24 August 2011 (24-08-2011)
EP1325464A1	09 July 2003 (09-07-2003)
EP1330698A2	30 July 2003 (30-07-2003)
EP1330698A4	14 March 2007 (14-03-2007)
EP1372334A2	17 December 2003 (17-12-2003)
EP1372334A3	31 March 2004 (31-03-2004)
EP1372334B1	17 December 2008 (17-12-2008)
EP1389011A2	11 February 2004 (11-02-2004)
EP1389011A3	25 February 2004 (25-02-2004)
EP1389011B1	27 February 2008 (27-02-2008)
EP1410313A1	21 April 2004 (21-04-2004)
EP1410313A4	22 December 2010 (22-12-2010)
EP1444823A2	11 August 2004 (11-08-2004)
EP1444823A4	27 May 2009 (27-05-2009)
EP1459239A1	22 September 2004 (22-09-2004)
EP1459239A4	07 June 2006 (07-06-2006)
EP1467834A1	20 October 2004 (20-10-2004)
EP1467834A4	06 April 2005 (06-04-2005)
EP1481347A2	01 December 2004 (01-12-2004)
EP1481347A4	26 August 2009 (26-08-2009)
EP1484710A2	08 December 2004 (08-12-2004)
EP1484710A3	12 July 2006 (12-07-2006)
EP1484710B1	09 January 2008 (09-01-2008)
EP1522990A2	13 April 2005 (13-04-2005)
EP1522990A3	19 November 2008 (19-11-2008)
EP1522990B1	20 October 2010 (20-10-2010)
EP1550077A2	06 July 2005 (06-07-2005)
EP1550077A4	05 July 2006 (05-07-2006)
EP1550077B1	08 July 2009 (08-07-2009)
EP1551644A1	13 July 2005 (13-07-2005)
EP1551644A4	02 January 2008 (02-01-2008)
EP1552441A2	13 July 2005 (13-07-2005)
EP1552441A4	23 November 2005 (23-11-2005)
EP1579622A1	28 September 2005 (28-09-2005)
EP1579622A4	30 May 2007 (30-05-2007)
EP1599825A2	30 November 2005 (30-11-2005)
EP1614064A2	11 January 2006 (11-01-2006)
EP1614064A4	23 April 2008 (23-04-2008)
EP1614064B1	08 December 2010 (08-12-2010)
EP1646966A2	19 April 2006 (19-04-2006)
EP1646966A4	31 December 2008 (31-12-2008)
EP1726117A2	29 November 2006 (29-11-2006)
EP1751690A2	14 February 2007 (14-02-2007)
EP1785890A2	16 May 2007 (16-05-2007)
EP1785890A3	30 May 2007 (30-05-2007)
EP1923830A2	21 May 2008 (21-05-2008)
EP1923830A3	27 August 2008 (27-08-2008)

EP1968301A2	10 September 2008 (10-09-2008)
EP1968301A3	22 October 2008 (22-10-2008)
EP2040453A2	25 March 2009 (25-03-2009)
EP2040453A3	01 April 2009 (01-04-2009)
EP2278497A2	26 January 2011 (26-01-2011)
EP2278497A3	27 April 2011 (27-04-2011)
EP2352111A1	03 August 2011 (03-08-2011)
EP2352120A1	03 August 2011 (03-08-2011)
ES2156456T3	16 June 2001 (16-06-2001)
ES2236999T3	16 July 2005 (16-07-2005)
ES2302888T3	01 August 2008 (01-08-2008)
GB0023204D0	01 November 2000 (01-11-2000)
GB2353168A	14 February 2001 (14-02-2001)
GB2353168A8	15 June 2001 (15-06-2001)
GB2353168B	16 October 2002 (16-10-2002)
GB0219190D0	25 September 2002 (25-09-2002)
GB2375254A	06 November 2002 (06-11-2002)
GB2375254B	24 December 2002 (24-12-2002)
HK1026796A1	09 July 2004 (09-07-2004)
HK1026968A1	29 May 2009 (29-05-2009)
HK1030122A1	09 May 2003 (09-05-2003)
HK1031013A1	21 February 2003 (21-02-2003)
HK1032464A1	07 December 2007 (07-12-2007)
HK1077147A1	09 May 2008 (09-05-2008)
HK1079597A1	25 January 2008 (25-01-2008)
IL137370D0	24 July 2001 (24-07-2001)
JP3649731B2	18 May 2005 (18-05-2005)
JP2005051793A	24 February 2005 (24-02-2005)
JP3949679B2	25 July 2007 (25-07-2007)
JP2001514453A	11 September 2001 (11-09-2001)
JP4068301B2	26 March 2008 (26-03-2008)
JP2006314111A	16 November 2006 (16-11-2006)
JP4071261B2	02 April 2008 (02-04-2008)
JP2006270972A	05 October 2006 (05-10-2006)
JP4187749B2	26 November 2008 (26-11-2008)
JP2004511938A	15 April 2004 (15-04-2004)
JP4199540B2	17 December 2008 (17-12-2008)
JP2004343722A	02 December 2004 (02-12-2004)
JP4205624B2	07 January 2009 (07-01-2009)
JP2007329907A	20 December 2007 (20-12-2007)
JP4417979B2	17 February 2010 (17-02-2010)
JP2006510329A	23 March 2006 (23-03-2006)
JP4510643B2	28 July 2010 (28-07-2010)
JP2002544627A	24 December 2002 (24-12-2002)
JP4598279B2	15 December 2010 (15-12-2010)
JP2003523697A	05 August 2003 (05-08-2003)
JP4682276B2	11 May 2011 (11-05-2011)
JP4785168B2	05 October 2011 (05-10-2011)
JP4785317B2	05 October 2011 (05-10-2011)
JP4800553B2	26 October 2011 (26-10-2011)
JP4808850B2	02 November 2011 (02-11-2011)
JP4823890B2	24 November 2011 (24-11-2011)
JP4829455B2	07 December 2011 (07-12-2011)
JPH09509795A	30 September 1997 (30-09-1997)
JP2002504272A	05 February 2002 (05-02-2002)
JP2002511685A	16 April 2002 (16-04-2002)
JP2002532812A	02 October 2002 (02-10-2002)
JP2002539487A	19 November 2002 (19-11-2002)
JP2002539647A	19 November 2002 (19-11-2002)
JP2002544637A	24 December 2002 (24-12-2002)
JP2003518658A	10 June 2003 (10-06-2003)
JP2003520008A	24 June 2003 (24-06-2003)
JP2003524199A	12 August 2003 (12-08-2003)
JP2003524911A	19 August 2003 (19-08-2003)
JP2003528538A	24 September 2003 (24-09-2003)
JP2003529225A	30 September 2003 (30-09-2003)
JP2004504954A	19 February 2004 (19-02-2004)
JP2004505349A	19 February 2004 (19-02-2004)

JP2004512611A	22 April 2004 (22-04-2004)
JP2005151561A	09 June 2005 (09-06-2005)
JP2006524840A	02 November 2006 (02-11-2006)
JP2007202163A	09 August 2007 (09-08-2007)
JP2007312383A	29 November 2007 (29-11-2007)
JP2007528644A	11 October 2007 (11-10-2007)
JP2008178081A	31 July 2008 (31-07-2008)
JP2008510327A	03 April 2008 (03-04-2008)
JP2010182323A	19 August 2010 (19-08-2010)
JP2010267292A	25 November 2010 (25-11-2010)
KR20060022316A	09 March 2006 (09-03-2006)
KR100799477B1	31 January 2008 (31-01-2008)
KR20070086674A	27 August 2007 (27-08-2007)
KR100878338B1	14 January 2009 (14-01-2009)
KR20080089665A	07 October 2008 (07-10-2008)
KR100920320B1	07 October 2009 (07-10-2009)
KR20090038942A	21 April 2009 (21-04-2009)
KR100960232B1	01 June 2010 (01-06-2010)
KR20100039459A	15 April 2010 (15-04-2010)
KR101041515B1	16 June 2011 (16-06-2011)
KR20050103977A	01 November 2005 (01-11-2005)
MXPA05003984A	22 June 2005 (22-06-2005)
USRE40919E1	22 September 2009 (22-09-2009)
US5636292A	03 June 1997 (03-06-1997)
US5636292C1	18 June 2002 (18-06-2002)
US5710834A	20 January 1998 (20-01-1998)
US5745604A	28 April 1998 (28-04-1998)
US5748763A	05 May 1998 (05-05-1998)
US5748783A	05 May 1998 (05-05-1998)
US5768426A	16 June 1998 (16-06-1998)
US5822436A	13 October 1998 (13-10-1998)
US5832119A	03 November 1998 (03-11-1998)
US5832119C1	05 March 2002 (05-03-2002)
US5841886A	24 November 1998 (24-11-1998)
US5841978A	24 November 1998 (24-11-1998)
US5850481A	15 December 1998 (15-12-1998)
US5850481C1	16 July 2002 (16-07-2002)
US5862260A	19 January 1999 (19-01-1999)
US6026193A	15 February 2000 (15-02-2000)
US6064737A	16 May 2000 (16-05-2000)
US6111954A	29 August 2000 (29-08-2000)
US6122392A	19 September 2000 (19-09-2000)
US6122403A	19 September 2000 (19-09-2000)
US6229924B1	08 May 2001 (08-05-2001)
US6252963B1	26 June 2001 (26-06-2001)
US6266430B1	24 July 2001 (24-07-2001)
US6278781B1	21 August 2001 (21-08-2001)
US6285776B1	04 September 2001 (04-09-2001)
US6286036B1	04 September 2001 (04-09-2001)
US6289108B1	11 September 2001 (11-09-2001)
US6307949B1	23 October 2001 (23-10-2001)
US6311214B1	30 October 2001 (30-10-2001)
US6324573B1	27 November 2001 (27-11-2001)
US6330335B1	11 December 2001 (11-12-2001)
US6332031B1	18 December 2001 (18-12-2001)
US6343138B1	29 January 2002 (29-01-2002)
US6345104B1	05 February 2002 (05-02-2002)
US6353672B1	05 March 2002 (05-03-2002)
US6363159B1	26 March 2002 (26-03-2002)
US6381341B1	30 April 2002 (30-04-2002)
US6385329B1	07 May 2002 (07-05-2002)
US6389151B1	14 May 2002 (14-05-2002)
US6400827B1	04 June 2002 (04-06-2002)
US6404898B1	11 June 2002 (11-06-2002)
US6408082B1	18 June 2002 (18-06-2002)
US6408331B1	18 June 2002 (18-06-2002)
US6411725B1	25 June 2002 (25-06-2002)
US6421070B1	16 July 2002 (16-07-2002)

US6424725B1	23 July 2002 (23-07-2002)
US6427020B1	30 July 2002 (30-07-2002)
US6430302B2	06 August 2002 (06-08-2002)
US6438231B1	20 August 2002 (20-08-2002)
US6442284B1	27 August 2002 (27-08-2002)
US6442285B2	27 August 2002 (27-08-2002)
US6449377B1	10 September 2002 (10-09-2002)
US6449379B1	10 September 2002 (10-09-2002)
US6496591B1	17 December 2002 (17-12-2002)
US6505160B1	07 January 2003 (07-01-2003)
US6513717B2	04 February 2003 (04-02-2003)
US6516079B1	04 February 2003 (04-02-2003)
US6519352B2	11 February 2003 (11-02-2003)
US6522769B1	18 February 2003 (18-02-2003)
US6522770B1	18 February 2003 (18-02-2003)
US6522771B2	18 February 2003 (18-02-2003)
US6535617B1	18 March 2003 (18-03-2003)
US6535618B1	18 March 2003 (18-03-2003)
US6539095B1	25 March 2003 (25-03-2003)
US6542618B1	01 April 2003 (01-04-2003)
US6542620B1	01 April 2003 (01-04-2003)
US6542927B2	01 April 2003 (01-04-2003)
US6546112B1	08 April 2003 (08-04-2003)
US6549638B2	15 April 2003 (15-04-2003)
US6553129B1	22 April 2003 (22-04-2003)
US6560349B1	06 May 2003 (06-05-2003)
US6560350B2	06 May 2003 (06-05-2003)
US6567533B1	20 May 2003 (20-05-2003)
US6567534B1	20 May 2003 (20-05-2003)
US6567535B2	20 May 2003 (20-05-2003)
US6567780B2	20 May 2003 (20-05-2003)
US6574350B1	03 June 2003 (03-06-2003)
US6577746B1	10 June 2003 (10-06-2003)
US6580808B2	17 June 2003 (17-06-2003)
US6580819B1	17 June 2003 (17-06-2003)
US6587821B1	01 July 2003 (01-07-2003)
US6590996B1	08 July 2003 (08-07-2003)
US6590997B2	08 July 2003 (08-07-2003)
US6590998B2	08 July 2003 (08-07-2003)
US6608911B2	19 August 2003 (19-08-2003)
US6611607B1	26 August 2003 (26-08-2003)
US6614914B1	02 September 2003 (02-09-2003)
US6636615B1	21 October 2003 (21-10-2003)
US6647128B1	11 November 2003 (11-11-2003)
US6647129B2	11 November 2003 (11-11-2003)
US6647130B2	11 November 2003 (11-11-2003)
US6650761B1	18 November 2003 (18-11-2003)
US6654480B2	25 November 2003 (25-11-2003)
US6654887B2	25 November 2003 (25-11-2003)
US6664976B2	16 December 2003 (16-12-2003)
US6674886B2	06 January 2004 (06-01-2004)
US6675146B2	06 January 2004 (06-01-2004)
US6681028B2	20 January 2004 (20-01-2004)
US6681029B1	20 January 2004 (20-01-2004)
US6681030B2	20 January 2004 (20-01-2004)
US6760464B2	06 July 2004 (06-07-2004)
US6694041B1	17 February 2004 (17-02-2004)
US6694042B2	17 February 2004 (17-02-2004)
US6694043B2	17 February 2004 (17-02-2004)
US6700990B1	02 March 2004 (02-03-2004)
US6700995B2	02 March 2004 (02-03-2004)
US6704869B2	09 March 2004 (09-03-2004)
US6718046B2	06 April 2004 (06-04-2004)
US6718047B2	06 April 2004 (06-04-2004)
US6721440B2	13 April 2004 (13-04-2004)
US6724912B1	20 April 2004 (20-04-2004)
US6728390B2	27 April 2004 (27-04-2004)
US6738495B2	18 May 2004 (18-05-2004)

US6744906B2	01 June 2004 (01-06-2004)
US6744907B2	01 June 2004 (01-06-2004)
US6750985B2	15 June 2004 (15-06-2004)
US6751320B2	15 June 2004 (15-06-2004)
US6754377B2	22 June 2004 (22-06-2004)
US6757406B2	29 June 2004 (29-06-2004)
US6760463B2	06 July 2004 (06-07-2004)
US6763122B1	13 July 2004 (13-07-2004)
US6763123B2	13 July 2004 (13-07-2004)
US6763124B2	13 July 2004 (13-07-2004)
US6768808B2	27 July 2004 (27-07-2004)
US6768809B2	27 July 2004 (27-07-2004)
US6771796B2	03 August 2004 (03-08-2004)
US6775392B1	10 August 2004 (10-08-2004)
US6778682B2	17 August 2004 (17-08-2004)
US6782115B2	24 August 2004 (24-08-2004)
US6788800B1	07 September 2004 (07-09-2004)
US6798894B2	28 September 2004 (28-09-2004)
US6804376B2	12 October 2004 (12-10-2004)
US6804377B2	12 October 2004 (12-10-2004)
US6804378B2	12 October 2004 (12-10-2004)
US6804379B2	12 October 2004 (12-10-2004)
US6813366B1	02 November 2004 (02-11-2004)
US6823075B2	23 November 2004 (23-11-2004)
US6829368B2	07 December 2004 (07-12-2004)
US6850626B2	01 February 2005 (01-02-2005)
US6868497B1	15 March 2005 (15-03-2005)
US6869023B2	22 March 2005 (22-03-2005)
US6879701B1	12 April 2005 (12-04-2005)
US6882737B2	19 April 2005 (19-04-2005)
US6882738B2	19 April 2005 (19-04-2005)
US6891959B2	10 May 2005 (10-05-2005)
US6912295B2	28 June 2005 (28-06-2005)
US6917691B2	12 July 2005 (12-07-2005)
US6917724B2	12 July 2005 (12-07-2005)
US6920232B2	19 July 2005 (19-07-2005)
US6922480B2	26 July 2005 (26-07-2005)
US6944298B1	13 September 2005 (13-09-2005)
US6947571B1	20 September 2005 (20-09-2005)
US6950519B2	27 September 2005 (27-09-2005)
US6959100B2	25 October 2005 (25-10-2005)
US6959386B2	25 October 2005 (25-10-2005)
US6961442B2	01 November 2005 (01-11-2005)
US6961444B2	01 November 2005 (01-11-2005)
US6963884B1	08 November 2005 (08-11-2005)
US6965682B1	15 November 2005 (15-11-2005)
US6965683B2	15 November 2005 (15-11-2005)
US6965873B1	15 November 2005 (15-11-2005)
US6968057B2	22 November 2005 (22-11-2005)
US6970573B2	29 November 2005 (29-11-2005)
US6973197B2	06 December 2005 (06-12-2005)
US6975744B2	13 December 2005 (13-12-2005)
US6975746B2	13 December 2005 (13-12-2005)
US6978036B2	20 December 2005 (20-12-2005)
US6983051B1	03 January 2006 (03-01-2006)
US6985600B2	10 January 2006 (10-01-2006)
US6987862B2	17 January 2006 (17-01-2006)
US6988202B1	17 January 2006 (17-01-2006)
US6993149B2	31 January 2006 (31-01-2006)
US6993150B2	31 January 2006 (31-01-2006)
US6993152B2	31 January 2006 (31-01-2006)
US6993154B2	31 January 2006 (31-01-2006)
US6996252B2	07 February 2006 (07-02-2006)
US7003132B2	21 February 2006 (21-02-2006)
US7003731B1	21 February 2006 (21-02-2006)
US7006661B2	28 February 2006 (28-02-2006)
US7010144B1	07 March 2006 (07-03-2006)
US7013021B2	14 March 2006 (14-03-2006)

US7016516B2	21 March 2006 (21-03-2006)
US7020303B2	28 March 2006 (28-03-2006)
US7020304B2	28 March 2006 (28-03-2006)
US7020349B2	28 March 2006 (28-03-2006)
US7022194B2	04 April 2006 (04-04-2006)
US7024016B2	04 April 2006 (04-04-2006)
US7027612B2	11 April 2006 (11-04-2006)
US7027614B2	11 April 2006 (11-04-2006)
US7035427B2	25 April 2006 (25-04-2006)
US7039214B2	02 May 2006 (02-05-2006)
US7042470B2	09 May 2006 (09-05-2006)
US7043052B2	09 May 2006 (09-05-2006)
US7044395B1	16 May 2006 (16-05-2006)
US7050603B2	23 May 2006 (23-05-2006)
US7051086B2	23 May 2006 (23-05-2006)
US7054462B2	30 May 2006 (30-05-2006)
US7054463B2	30 May 2006 (30-05-2006)
US7054465B2	30 May 2006 (30-05-2006)
US7055034B1	30 May 2006 (30-05-2006)
US7058697B2	06 June 2006 (06-06-2006)
US7061510B2	13 June 2006 (13-06-2006)
US7062069B2	13 June 2006 (13-06-2006)
US7063264B2	20 June 2006 (20-06-2006)
US7065228B2	20 June 2006 (20-06-2006)
US7076084B2	11 July 2006 (11-07-2006)
US7095871B2	22 August 2006 (22-08-2006)
US7098931B2	29 August 2006 (29-08-2006)
US7099492B2	29 August 2006 (29-08-2006)
US7103197B2	05 September 2006 (05-09-2006)
US7111168B2	19 September 2006 (19-09-2006)
US7111170B2	19 September 2006 (19-09-2006)
US7113596B2	26 September 2006 (26-09-2006)
US7113614B2	26 September 2006 (26-09-2006)
US7113615B2	26 September 2006 (26-09-2006)
US7116781B2	03 October 2006 (03-10-2006)
US7123740B2	17 October 2006 (17-10-2006)
US7130087B2	31 October 2006 (31-10-2006)
US7136502B2	14 November 2006 (14-11-2006)
US7139408B2	21 November 2006 (21-11-2006)
US7142691B2	28 November 2006 (28-11-2006)
US7143949B1	05 December 2006 (05-12-2006)
US7152021B2	19 December 2006 (19-12-2006)
US7152786B2	26 December 2006 (26-12-2006)
US7158654B2	02 January 2007 (02-01-2007)
US7162052B2	09 January 2007 (09-01-2007)
US7164413B2	16 January 2007 (16-01-2007)
US7164780B2	16 January 2007 (16-01-2007)
US7171016B1	30 January 2007 (30-01-2007)
US7171018B2	30 January 2007 (30-01-2007)
US7171020B2	30 January 2007 (30-01-2007)
US7174031B2	06 February 2007 (06-02-2007)
US7177443B2	13 February 2007 (13-02-2007)
US7181022B2	20 February 2007 (20-02-2007)
US7184570B2	27 February 2007 (27-02-2007)
US7184572B2	27 February 2007 (27-02-2007)
US7185201B2	27 February 2007 (27-02-2007)
US7191156B1	13 March 2007 (13-03-2007)
US7197156B1	27 March 2007 (27-03-2007)
US7197160B2	27 March 2007 (27-03-2007)
US7197164B2	27 March 2007 (27-03-2007)
US7206820B1	17 April 2007 (17-04-2007)
US7207494B2	24 April 2007 (24-04-2007)
US7209571B2	24 April 2007 (24-04-2007)
US7209573B2	24 April 2007 (24-04-2007)
US7213757B2	08 May 2007 (08-05-2007)
US7224819B2	29 May 2007 (29-05-2007)
US7224995B2	29 May 2007 (29-05-2007)
US7225991B2	05 June 2007 (05-06-2007)

US7239734B2	03 July 2007 (03-07-2007)
US7242790B2	10 July 2007 (10-07-2007)
US7246239B2	17 July 2007 (17-07-2007)
US7248715B2	24 July 2007 (24-07-2007)
US7248717B2	24 July 2007 (24-07-2007)
US7249257B2	24 July 2007 (24-07-2007)
US7254249B2	07 August 2007 (07-08-2007)
US7261612B1	28 August 2007 (28-08-2007)
US7263203B2	28 August 2007 (28-08-2007)
US7266217B2	04 September 2007 (04-09-2007)
US7266704B2	04 September 2007 (04-09-2007)
US7269275B2	11 September 2007 (11-09-2007)
US7273836B2	25 September 2007 (25-09-2007)
US7277468B2	02 October 2007 (02-10-2007)
US7286684B2	23 October 2007 (23-10-2007)
US7286685B2	23 October 2007 (23-10-2007)
US7289643B2	30 October 2007 (30-10-2007)
US7298864B2	20 November 2007 (20-11-2007)
US7302574B2	27 November 2007 (27-11-2007)
US7305104B2	04 December 2007 (04-12-2007)
US7305117B2	04 December 2007 (04-12-2007)
US7308110B2	11 December 2007 (11-12-2007)
US7313251B2	25 December 2007 (25-12-2007)
US7313253B2	25 December 2007 (25-12-2007)
US7319775B2	15 January 2008 (15-01-2008)
US7321667B2	22 January 2008 (22-01-2008)
US7330563B2	12 February 2008 (12-02-2008)
US7330564B2	12 February 2008 (12-02-2008)
US7333957B2	19 February 2008 (19-02-2008)
US7340076B2	04 March 2008 (04-03-2008)
US7346776B2	18 March 2008 (18-03-2008)
US7349552B2	25 March 2008 (25-03-2008)
US7349555B2	25 March 2008 (25-03-2008)
US7359528B2	15 April 2008 (15-04-2008)
US7362781B2	22 April 2008 (22-04-2008)
US7362879B2	22 April 2008 (22-04-2008)
US7369676B2	06 May 2008 (06-05-2008)
US7369678B2	06 May 2008 (06-05-2008)
US7372976B2	13 May 2008 (13-05-2008)
US7373513B2	13 May 2008 (13-05-2008)
US7377421B2	27 May 2008 (27-05-2008)
US7391880B2	24 June 2008 (24-06-2008)
US7400743B2	15 July 2008 (15-07-2008)
US7403633B2	22 July 2008 (22-07-2008)
US7406214B2	29 July 2008 (29-07-2008)
US7412072B2	12 August 2008 (12-08-2008)
US7415129B2	19 August 2008 (19-08-2008)
US7418111B2	26 August 2008 (26-08-2008)
US7424131B2	09 September 2008 (09-09-2008)
US7424132B2	09 September 2008 (09-09-2008)
US7427030B2	23 September 2008 (23-09-2008)
US7433491B2	07 October 2008 (07-10-2008)
US7436976B2	14 October 2008 (14-10-2008)
US7437430B2	14 October 2008 (14-10-2008)
US7444000B2	28 October 2008 (28-10-2008)
US7444392B2	28 October 2008 (28-10-2008)
US7450734B2	11 November 2008 (11-11-2008)
US7454035B2	18 November 2008 (18-11-2008)
US7460726B2	02 December 2008 (02-12-2008)
US7461136B2	02 December 2008 (02-12-2008)
US7466840B2	16 December 2008 (16-12-2008)
US7486799B2	03 February 2009 (03-02-2009)
US7499564B2	03 March 2009 (03-03-2009)
US7499566B2	03 March 2009 (03-03-2009)
US7502489B2	10 March 2009 (10-03-2009)
US7502490B2	10 March 2009 (10-03-2009)
US7502759B2	10 March 2009 (10-03-2009)
US7502937B2	10 March 2009 (10-03-2009)

		US7505605B2	17 March 2009 (17-03-2009)
		US7506169B2	17 March 2009 (17-03-2009)
		US7508955B2	24 March 2009 (24-03-2009)
		US7515733B2	07 April 2009 (07-04-2009)
		US7522728B1	21 April 2009 (21-04-2009)
		US7529647B2	05 May 2009 (05-05-2009)
		US7532740B2	12 May 2009 (12-05-2009)
		US7532741B2	12 May 2009 (12-05-2009)
		US7536034B2	19 May 2009 (19-05-2009)
		US7536555B2	19 May 2009 (19-05-2009)
		US7537170B2	26 May 2009 (26-05-2009)
		US7539325B2	26 May 2009 (26-05-2009)
		US7545951B2	09 June 2009 (09-06-2009)
		US7545952B2	09 June 2009 (09-06-2009)
		US7548643B2	16 June 2009 (16-06-2009)
		US7555139B2	30 June 2009 (30-06-2009)
		US7555785B2	30 June 2009 (30-06-2009)
		US7562392B1	14 July 2009 (14-07-2009)
		US7564992B2	21 July 2009 (21-07-2009)
		US7565294B2	21 July 2009 (21-07-2009)
		US7567686B2	28 July 2009 (28-07-2009)
		US7567721B2	28 July 2009 (28-07-2009)
		US7570781B2	04 August 2009 (04-08-2009)
US7286665B1	23 October 2007 (23-10-2007)	AT320122T	15 March 2006 (15-03-2006)
		AT322779T	15 April 2006 (15-04-2006)
		AT330391T	15 July 2006 (15-07-2006)
		AT397337T	15 June 2008 (15-06-2008)
		DE60026439D1	04 May 2006 (04-05-2006)
		DE60026439T2	24 August 2006 (24-08-2006)
		DE60027119D1	18 May 2006 (18-05-2006)
		DE60027119T2	07 September 2006 (07-09-2006)
		DE60028645D1	27 July 2006 (27-07-2006)
		DE60028645T2	12 October 2006 (12-10-2006)
		DE60039022D1	10 July 2008 (10-07-2008)
		EP1043864A2	11 October 2000 (11-10-2000)
		EP1043864A3	10 September 2003 (10-09-2003)
		EP1043864B1	14 June 2006 (14-06-2006)
		EP1111838A2	27 June 2001 (27-06-2001)
		EP1111838A3	24 September 2003 (24-09-2003)
		EP1111838B1	05 April 2006 (05-04-2006)
		EP1113617A2	04 July 2001 (04-07-2001)
		EP1113617A3	27 August 2003 (27-08-2003)
		EP1113617B1	28 May 2008 (28-05-2008)
		EP1130843A2	05 September 2001 (05-09-2001)
		EP1130843A3	23 July 2003 (23-07-2003)
		EP1130843B1	08 March 2006 (08-03-2006)
		EP1699162A2	06 September 2006 (06-09-2006)
		EP1699162A3	20 September 2006 (20-09-2006)
		ES2259592T3	16 October 2006 (16-10-2006)
		ES2261135T3	16 November 2006 (16-11-2006)
		ES2265826T3	01 March 2007 (01-03-2007)
		ES2304929T3	01 November 2008 (01-11-2008)
		JP2001202010A	27 July 2001 (27-07-2001)
		JP4010766B2	21 November 2007 (21-11-2007)
		JP2001209306A	03 August 2001 (03-08-2001)
		US6859533B1	22 February 2005 (22-02-2005)
		US6937726B1	30 August 2005 (30-08-2005)
		US7356688B1	08 April 2008 (08-04-2008)
US2005262351A1	24 November 2005 (24-11-2005)	US2005262351A1	24 November 2005 (24-11-2005)
		AT199469T	15 March 2001 (15-03-2001)
		AT216546T	15 May 2002 (15-05-2002)
		AT230539T	15 January 2003 (15-01-2003)
		AT237197T	15 April 2003 (15-04-2003)
		AT245328T	15 August 2003 (15-08-2003)

AT261225T	15 March 2004 (15-03-2004)
AT287176T	15 January 2005 (15-01-2005)
AT289435T	15 March 2005 (15-03-2005)
AT304727T	15 September 2005 (15-09-2005)
AT358850T	15 April 2007 (15-04-2007)
AT372559T	15 September 2007 (15-09-2007)
AT383617T	15 January 2008 (15-01-2008)
AT387807T	15 March 2008 (15-03-2008)
AT418233T	15 January 2009 (15-01-2009)
AT420529T	15 January 2009 (15-01-2009)
AT435757T	15 July 2009 (15-07-2009)
AT485677T	15 November 2010 (15-11-2010)
AT491190T	15 December 2010 (15-12-2010)
AT502354T	15 April 2011 (15-04-2011)
AT522081T	15 September 2011 (15-09-2011)
AU747372B2	16 May 2002 (16-05-2002)
AU761566B2	05 June 2003 (05-06-2003)
AU1102201A	06 June 2001 (06-06-2001)
AU1163402A	22 April 2002 (22-04-2002)
AU1232001A	14 May 2001 (14-05-2001)
AU1232101A	14 May 2001 (14-05-2001)
AU1624800A	13 June 2000 (13-06-2000)
AU1809300A	22 May 2000 (22-05-2000)
AU1935001A	12 June 2001 (12-06-2001)
AU2295701A	16 July 2001 (16-07-2001)
AU2296502A	30 January 2002 (30-01-2002)
AU2297302A	30 January 2002 (30-01-2002)
AU2369500A	03 July 2000 (03-07-2000)
AU2463499A	02 August 1999 (02-08-1999)
AU2559302A	29 April 2002 (29-04-2002)
AU2593101A	09 July 2001 (09-07-2001)
AU2936201A	24 July 2001 (24-07-2001)
AU2940201A	24 July 2001 (24-07-2001)
AU3008697A	05 December 1997 (05-12-1997)
AU3281702A	01 July 2002 (01-07-2002)
AU3293402A	06 May 2002 (06-05-2002)
AU3458101A	07 August 2001 (07-08-2001)
AU3523102A	01 July 2002 (01-07-2002)
AU3562999A	01 November 1999 (01-11-1999)
AU3667802A	21 May 2002 (21-05-2002)
AU3701701A	27 August 2001 (27-08-2001)
AU3736800A	28 September 2000 (28-09-2000)
AU3801301A	14 August 2001 (14-08-2001)
AU3966002A	01 July 2002 (01-07-2002)
AU4010501A	24 September 2001 (24-09-2001)
AU4745701A	03 October 2001 (03-10-2001)
AU4836799A	21 February 2000 (21-02-2000)
AU4851300A	05 December 2000 (05-12-2000)
AU5145700A	05 December 2000 (05-12-2000)
AU5544501A	30 October 2001 (30-10-2001)
AU5544601A	07 November 2001 (07-11-2001)
AU5931301A	12 November 2001 (12-11-2001)
AU5965201A	20 November 2001 (20-11-2001)
AU6022396A	29 November 1996 (29-11-1996)
AU6694901A	02 January 2002 (02-01-2002)
AU7318401A	13 February 2002 (13-02-2002)
AU7704701A	05 February 2002 (05-02-2002)
AU7714701A	05 February 2002 (05-02-2002)
AU8307301A	18 February 2002 (18-02-2002)
AU9033098A	16 March 1999 (16-03-1999)
AU9082201A	26 March 2002 (26-03-2002)
AU9265901A	26 March 2002 (26-03-2002)
AU9634301A	08 April 2002 (08-04-2002)
AU2001277047B2	06 September 2007 (06-09-2007)
AU2001277147B2	18 May 2006 (18-05-2006)
AU2002305304A1	11 November 2002 (11-11-2002)
AU2002353174A1	15 July 2003 (15-07-2003)
AU2002364036A1	15 July 2003 (15-07-2003)

AU2002364255A1	15 July 2003 (15-07-2003)
AU2003210625A1	02 September 2003 (02-09-2003)
AU2003217642A1	09 September 2003 (09-09-2003)
AU2003217642A8	09 September 2003 (09-09-2003)
AU2003220245A1	29 September 2003 (29-09-2003)
AU2003221894A1	27 October 2003 (27-10-2003)
AU2003221894A8	27 October 2003 (27-10-2003)
AU2003285891A1	04 May 2004 (04-05-2004)
AU2003293087A1	23 June 2004 (23-06-2004)
AU2005205804A1	29 September 2005 (29-09-2005)
AU2009200468A1	26 February 2009 (26-02-2009)
AU2009200468B2	31 March 2011 (31-03-2011)
AU2009202090A1	18 June 2009 (18-06-2009)
BR9907105A	30 April 2002 (30-04-2002)
CA2174413A1	26 May 1995 (26-05-1995)
CA2174413C	09 June 2009 (09-06-2009)
CA2218957A1	14 November 1996 (14-11-1996)
CA2218957C	25 January 2005 (25-01-2005)
CA2301218A1	04 March 1999 (04-03-1999)
CA2318564A1	22 July 1999 (22-07-1999)
CA2318564C	21 July 2009 (21-07-2009)
CA2326565A1	21 October 1999 (21-10-1999)
CA2326565C	15 September 2009 (15-09-2009)
CA2338618A1	10 February 2000 (10-02-2000)
CA2338618C	04 July 2006 (04-07-2006)
CA2347179A1	11 May 2000 (11-05-2000)
CA2355715A1	22 June 2000 (22-06-2000)
CA2364433A1	14 September 2000 (14-09-2000)
CA2364433C	19 July 2011 (19-07-2011)
CA2373208A1	23 November 2000 (23-11-2000)
CA2373511A1	23 November 2000 (23-11-2000)
CA2416530A1	31 January 2002 (31-01-2002)
CA2416530C	21 October 2008 (21-10-2008)
CA2416532A1	31 January 2002 (31-01-2002)
CA2422081A1	02 May 2002 (02-05-2002)
CA2422081C	21 August 2007 (21-08-2007)
CA2422412A1	18 April 2002 (18-04-2002)
CA2469938A1	10 July 2003 (10-07-2003)
CA2469938C	15 September 2009 (15-09-2009)
CA2470547A1	10 July 2003 (10-07-2003)
CA2470547C	20 May 2008 (20-05-2008)
CA2471457A1	10 July 2003 (10-07-2003)
CA2471457C	02 August 2011 (02-08-2011)
CA2476895A1	28 August 2003 (28-08-2003)
CA2483419A1	14 November 1996 (14-11-1996)
CA2502232A1	29 April 2004 (29-04-2004)
CA2522551A1	04 November 2004 (04-11-2004)
CA2522551C	22 December 2009 (22-12-2009)
CA2532296A1	03 February 2005 (03-02-2005)
CA2666703A1	22 July 1999 (22-07-1999)
CA2671998A1	10 July 2003 (10-07-2003)
CN1628318A	15 June 2005 (15-06-2005)
CN1316421C	16 May 2007 (16-05-2007)
CN1631030A	22 June 2005 (22-06-2005)
CN100364309C	23 January 2008 (23-01-2008)
CN101159799A	09 April 2008 (09-04-2008)
DE60127689D1	16 May 2007 (16-05-2007)
DE60127689T2	06 September 2007 (06-09-2007)
DE60144222D1	28 April 2011 (28-04-2011)
DE60232918D1	20 August 2009 (20-08-2009)
DE69426787D1	05 April 2001 (05-04-2001)
DE69426787T2	30 August 2001 (30-08-2001)
DE69432480D1	15 May 2003 (15-05-2003)
DE69432480T2	18 March 2004 (18-03-2004)
DE69434237D1	17 February 2005 (17-02-2005)
DE69434237T2	08 December 2005 (08-12-2005)
DE69435076D1	10 April 2008 (10-04-2008)
DE69435076T2	26 March 2009 (26-03-2009)

DE69435317D1	02 December 2010 (02-12-2010)
DE69620751D1	23 May 2002 (23-05-2002)
DE69620751T2	31 October 2002 (31-10-2002)
DE69625626D1	06 February 2003 (06-02-2003)
DE69625626T2	16 October 2003 (16-10-2003)
DE69629134D1	21 August 2003 (21-08-2003)
DE69629134T2	15 April 2004 (15-04-2004)
DE69631806D1	08 April 2004 (08-04-2004)
DE69631806T2	03 February 2005 (03-02-2005)
DE69637782D1	29 January 2009 (29-01-2009)
DE69739209D1	26 February 2009 (26-02-2009)
DE69923781D1	24 March 2005 (24-03-2005)
DE69923781T2	07 July 2005 (07-07-2005)
DE69927218D1	20 October 2005 (20-10-2005)
DE69927218T2	12 January 2006 (12-01-2006)
DE69937044D1	18 October 2007 (18-10-2007)
DE69937044T2	03 January 2008 (03-01-2008)
DE69937972D1	21 February 2008 (21-02-2008)
DE69937972T2	08 January 2009 (08-01-2009)
DE602004030434D1	20 January 2011 (20-01-2011)
EP0737387A1	16 October 1996 (16-10-1996)
EP0737387B1	09 April 2003 (09-04-2003)
EP0824821A2	25 February 1998 (25-02-1998)
EP0824821B1	17 April 2002 (17-04-2002)
EP0959620A1	24 November 1999 (24-11-1999)
EP0959620B1	12 January 2005 (12-01-2005)
EP0959621A1	24 November 1999 (24-11-1999)
EP0959621B1	28 February 2001 (28-02-2001)
EP0961239A2	01 December 1999 (01-12-1999)
EP0961239A3	28 February 2001 (28-02-2001)
EP0981113A2	23 February 2000 (23-02-2000)
EP0981113A3	14 March 2001 (14-03-2001)
EP0981113B1	14 September 2005 (14-09-2005)
EP0987855A2	22 March 2000 (22-03-2000)
EP1003324A2	24 May 2000 (24-05-2000)
EP1003324A3	31 May 2000 (31-05-2000)
EP1003324B1	16 July 2003 (16-07-2003)
EP1008097A1	14 June 2000 (14-06-2000)
EP1008097A4	21 March 2001 (21-03-2001)
EP1019868A2	19 July 2000 (19-07-2000)
EP1019868A4	07 February 2001 (07-02-2001)
EP1019868B1	07 January 2009 (07-01-2009)
EP1049320A1	02 November 2000 (02-11-2000)
EP1049320A8	02 May 2001 (02-05-2001)
EP1049320B1	02 January 2003 (02-01-2003)
EP1050005A2	08 November 2000 (08-11-2000)
EP1050005A4	18 July 2001 (18-07-2001)
EP1050005B1	05 September 2007 (05-09-2007)
EP1054335A2	22 November 2000 (22-11-2000)
EP1054335A3	17 December 2003 (17-12-2003)
EP1131769A2	12 September 2001 (12-09-2001)
EP1131769A4	19 March 2003 (19-03-2003)
EP1131769B1	16 February 2005 (16-02-2005)
EP1137251A2	26 September 2001 (26-09-2001)
EP1137251A3	06 March 2002 (06-03-2002)
EP1137251B1	03 March 2004 (03-03-2004)
EP1137975A1	04 October 2001 (04-10-2001)
EP1142190A1	10 October 2001 (10-10-2001)
EP1142190A4	25 May 2005 (25-05-2005)
EP1157499A1	28 November 2001 (28-11-2001)
EP1157499A4	09 July 2003 (09-07-2003)
EP1185967A1	13 March 2002 (13-03-2002)
EP1185967A4	03 November 2004 (03-11-2004)
EP1208499A1	29 May 2002 (29-05-2002)
EP1208499A4	07 November 2007 (07-11-2007)
EP1232472A1	21 August 2002 (21-08-2002)
EP1249002A1	16 October 2002 (16-10-2002)
EP1249002A4	13 September 2006 (13-09-2006)

EP1249002B1	16 March 2011 (16-03-2011)
EP1257921A1	20 November 2002 (20-11-2002)
EP1257921A4	20 September 2006 (20-09-2006)
EP1257931A1	20 November 2002 (20-11-2002)
EP1257931A4	22 November 2006 (22-11-2006)
EP1264268A1	11 December 2002 (11-12-2002)
EP1266475A1	18 December 2002 (18-12-2002)
EP1266475A4	27 July 2005 (27-07-2005)
EP1311973A1	21 May 2003 (21-05-2003)
EP1311973A4	20 October 2004 (20-10-2004)
EP1311973B1	04 April 2007 (04-04-2007)
EP1312030A2	21 May 2003 (21-05-2003)
EP1312030A4	11 July 2007 (11-07-2007)
EP1312030B1	24 August 2011 (24-08-2011)
EP1325464A1	09 July 2003 (09-07-2003)
EP1330698A2	30 July 2003 (30-07-2003)
EP1330698A4	14 March 2007 (14-03-2007)
EP1372334A2	17 December 2003 (17-12-2003)
EP1372334A3	31 March 2004 (31-03-2004)
EP1372334B1	17 December 2008 (17-12-2008)
EP1389011A2	11 February 2004 (11-02-2004)
EP1389011A3	25 February 2004 (25-02-2004)
EP1389011B1	27 February 2008 (27-02-2008)
EP1410313A1	21 April 2004 (21-04-2004)
EP1410313A4	22 December 2010 (22-12-2010)
EP1444823A2	11 August 2004 (11-08-2004)
EP1444823A4	27 May 2009 (27-05-2009)
EP1459239A1	22 September 2004 (22-09-2004)
EP1459239A4	07 June 2006 (07-06-2006)
EP1467834A1	20 October 2004 (20-10-2004)
EP1467834A4	06 April 2005 (06-04-2005)
EP1481347A2	01 December 2004 (01-12-2004)
EP1481347A4	26 August 2009 (26-08-2009)
EP1484710A2	08 December 2004 (08-12-2004)
EP1484710A3	12 July 2006 (12-07-2006)
EP1484710B1	09 January 2008 (09-01-2008)
EP1522990A2	13 April 2005 (13-04-2005)
EP1522990A3	19 November 2008 (19-11-2008)
EP1522990B1	20 October 2010 (20-10-2010)
EP1550077A2	06 July 2005 (06-07-2005)
EP1550077A4	05 July 2006 (05-07-2006)
EP1550077B1	08 July 2009 (08-07-2009)
EP1551644A1	13 July 2005 (13-07-2005)
EP1551644A4	02 January 2008 (02-01-2008)
EP1552441A2	13 July 2005 (13-07-2005)
EP1552441A4	23 November 2005 (23-11-2005)
EP1579622A1	28 September 2005 (28-09-2005)
EP1579622A4	30 May 2007 (30-05-2007)
EP1599825A2	30 November 2005 (30-11-2005)
EP1614064A2	11 January 2006 (11-01-2006)
EP1614064A4	23 April 2008 (23-04-2008)
EP1614064B1	08 December 2010 (08-12-2010)
EP1646966A2	19 April 2006 (19-04-2006)
EP1646966A4	31 December 2008 (31-12-2008)
EP1726117A2	29 November 2006 (29-11-2006)
EP1751690A2	14 February 2007 (14-02-2007)
EP1785890A2	16 May 2007 (16-05-2007)
EP1785890A3	30 May 2007 (30-05-2007)
EP1923830A2	21 May 2008 (21-05-2008)
EP1923830A3	27 August 2008 (27-08-2008)
EP1968301A2	10 September 2008 (10-09-2008)
EP1968301A3	22 October 2008 (22-10-2008)
EP2040453A2	25 March 2009 (25-03-2009)
EP2040453A3	01 April 2009 (01-04-2009)
EP2278497A2	26 January 2011 (26-01-2011)
EP2278497A3	27 April 2011 (27-04-2011)
EP2352111A1	03 August 2011 (03-08-2011)
EP2352120A1	03 August 2011 (03-08-2011)

ES2156456T3	16 June 2001 (16-06-2001)
ES2236999T3	16 July 2005 (16-07-2005)
ES2302888T3	01 August 2008 (01-08-2008)
GB0023204D0	01 November 2000 (01-11-2000)
GB2353168A	14 February 2001 (14-02-2001)
GB2353168A8	15 June 2001 (15-06-2001)
GB2353168B	16 October 2002 (16-10-2002)
GB0219190D0	25 September 2002 (25-09-2002)
GB2375254A	06 November 2002 (06-11-2002)
GB2375254B	24 December 2002 (24-12-2002)
HK1026796A1	09 July 2004 (09-07-2004)
HK1026968A1	29 May 2009 (29-05-2009)
HK1030122A1	09 May 2003 (09-05-2003)
HK1031013A1	21 February 2003 (21-02-2003)
HK1032464A1	07 December 2007 (07-12-2007)
HK1077147A1	09 May 2008 (09-05-2008)
HK1079597A1	25 January 2008 (25-01-2008)
IL137370D0	24 July 2001 (24-07-2001)
JP3649731B2	18 May 2005 (18-05-2005)
JP2005051793A	24 February 2005 (24-02-2005)
JP3949679B2	25 July 2007 (25-07-2007)
JP2001514453A	11 September 2001 (11-09-2001)
JP4068301B2	26 March 2008 (26-03-2008)
JP2006314111A	16 November 2006 (16-11-2006)
JP4071261B2	02 April 2008 (02-04-2008)
JP2006270972A	05 October 2006 (05-10-2006)
JP4187749B2	26 November 2008 (26-11-2008)
JP2004511938A	15 April 2004 (15-04-2004)
JP4199540B2	17 December 2008 (17-12-2008)
JP2004343722A	02 December 2004 (02-12-2004)
JP4205624B2	07 January 2009 (07-01-2009)
JP2007329907A	20 December 2007 (20-12-2007)
JP4417979B2	17 February 2010 (17-02-2010)
JP2006510329A	23 March 2006 (23-03-2006)
JP4510643B2	28 July 2010 (28-07-2010)
JP2002544627A	24 December 2002 (24-12-2002)
JP4598279B2	15 December 2010 (15-12-2010)
JP2003523697A	05 August 2003 (05-08-2003)
JP4682276B2	11 May 2011 (11-05-2011)
JP4785168B2	05 October 2011 (05-10-2011)
JP4785317B2	05 October 2011 (05-10-2011)
JP4800553B2	26 October 2011 (26-10-2011)
JP4808850B2	02 November 2011 (02-11-2011)
JP4823890B2	24 November 2011 (24-11-2011)
JP4829455B2	07 December 2011 (07-12-2011)
JPH09509795A	30 September 1997 (30-09-1997)
JP2002504272A	05 February 2002 (05-02-2002)
JP2002511685A	16 April 2002 (16-04-2002)
JP2002532812A	02 October 2002 (02-10-2002)
JP2002539487A	19 November 2002 (19-11-2002)
JP2002539647A	19 November 2002 (19-11-2002)
JP2002544637A	24 December 2002 (24-12-2002)
JP2003518658A	10 June 2003 (10-06-2003)
JP2003520008A	24 June 2003 (24-06-2003)
JP2003524199A	12 August 2003 (12-08-2003)
JP2003524911A	19 August 2003 (19-08-2003)
JP2003528538A	24 September 2003 (24-09-2003)
JP2003529225A	30 September 2003 (30-09-2003)
JP2004504954A	19 February 2004 (19-02-2004)
JP2004505349A	19 February 2004 (19-02-2004)
JP2004512611A	22 April 2004 (22-04-2004)
JP2005151561A	09 June 2005 (09-06-2005)
JP2006524840A	02 November 2006 (02-11-2006)
JP2007202163A	09 August 2007 (09-08-2007)
JP2007312383A	29 November 2007 (29-11-2007)
JP2007528644A	11 October 2007 (11-10-2007)
JP2008178081A	31 July 2008 (31-07-2008)
JP2008510327A	03 April 2008 (03-04-2008)

JP2010182323A	19 August 2010 (19-08-2010)
JP2010267292A	25 November 2010 (25-11-2010)
KR20060022316A	09 March 2006 (09-03-2006)
KR100799477B1	31 January 2008 (31-01-2008)
KR20070086674A	27 August 2007 (27-08-2007)
KR100878338B1	14 January 2009 (14-01-2009)
KR20080089665A	07 October 2008 (07-10-2008)
KR100920320B1	07 October 2009 (07-10-2009)
KR20090038942A	21 April 2009 (21-04-2009)
KR100960232B1	01 June 2010 (01-06-2010)
KR20100039459A	15 April 2010 (15-04-2010)
KR101041515B1	16 June 2011 (16-06-2011)
KR20050103977A	01 November 2005 (01-11-2005)
MXPA05003984A	22 June 2005 (22-06-2005)
USRE40919E1	22 September 2009 (22-09-2009)
US5636292A	03 June 1997 (03-06-1997)
US5636292C1	18 June 2002 (18-06-2002)
US5710834A	20 January 1998 (20-01-1998)
US5745604A	28 April 1998 (28-04-1998)
US5748763A	05 May 1998 (05-05-1998)
US5748783A	05 May 1998 (05-05-1998)
US5768426A	16 June 1998 (16-06-1998)
US5822436A	13 October 1998 (13-10-1998)
US5832119A	03 November 1998 (03-11-1998)
US5832119C1	05 March 2002 (05-03-2002)
US5841886A	24 November 1998 (24-11-1998)
US5841978A	24 November 1998 (24-11-1998)
US5850481A	15 December 1998 (15-12-1998)
US5850481C1	16 July 2002 (16-07-2002)
US5862260A	19 January 1999 (19-01-1999)
US6026193A	15 February 2000 (15-02-2000)
US6064737A	16 May 2000 (16-05-2000)
US6111954A	29 August 2000 (29-08-2000)
US6122392A	19 September 2000 (19-09-2000)
US6122403A	19 September 2000 (19-09-2000)
US6229924B1	08 May 2001 (08-05-2001)
US6252963B1	26 June 2001 (26-06-2001)
US6266430B1	24 July 2001 (24-07-2001)
US6278781B1	21 August 2001 (21-08-2001)
US6285776B1	04 September 2001 (04-09-2001)
US6286036B1	04 September 2001 (04-09-2001)
US6289108B1	11 September 2001 (11-09-2001)
US6307949B1	23 October 2001 (23-10-2001)
US6311214B1	30 October 2001 (30-10-2001)
US6324573B1	27 November 2001 (27-11-2001)
US6330335B1	11 December 2001 (11-12-2001)
US6332031B1	18 December 2001 (18-12-2001)
US6343138B1	29 January 2002 (29-01-2002)
US6345104B1	05 February 2002 (05-02-2002)
US6353672B1	05 March 2002 (05-03-2002)
US6363159B1	26 March 2002 (26-03-2002)
US6381341B1	30 April 2002 (30-04-2002)
US6385329B1	07 May 2002 (07-05-2002)
US6389151B1	14 May 2002 (14-05-2002)
US6400827B1	04 June 2002 (04-06-2002)
US6404898B1	11 June 2002 (11-06-2002)
US6408082B1	18 June 2002 (18-06-2002)
US6408331B1	18 June 2002 (18-06-2002)
US6411725B1	25 June 2002 (25-06-2002)
US6421070B1	16 July 2002 (16-07-2002)
US6424725B1	23 July 2002 (23-07-2002)
US6427020B1	30 July 2002 (30-07-2002)
US6430302B2	06 August 2002 (06-08-2002)
US6438231B1	20 August 2002 (20-08-2002)
US6442284B1	27 August 2002 (27-08-2002)
US6442285B2	27 August 2002 (27-08-2002)
US6449377B1	10 September 2002 (10-09-2002)
US6449379B1	10 September 2002 (10-09-2002)

US6496591B1	17 December 2002 (17-12-2002)
US6505160B1	07 January 2003 (07-01-2003)
US6513717B2	04 February 2003 (04-02-2003)
US6516079B1	04 February 2003 (04-02-2003)
US6519352B2	11 February 2003 (11-02-2003)
US6522769B1	18 February 2003 (18-02-2003)
US6522770B1	18 February 2003 (18-02-2003)
US6522771B2	18 February 2003 (18-02-2003)
US6535617B1	18 March 2003 (18-03-2003)
US6535618B1	18 March 2003 (18-03-2003)
US6539095B1	25 March 2003 (25-03-2003)
US6542618B1	01 April 2003 (01-04-2003)
US6542620B1	01 April 2003 (01-04-2003)
US6542927B2	01 April 2003 (01-04-2003)
US6546112B1	08 April 2003 (08-04-2003)
US6549638B2	15 April 2003 (15-04-2003)
US6553129B1	22 April 2003 (22-04-2003)
US6560349B1	06 May 2003 (06-05-2003)
US6560350B2	06 May 2003 (06-05-2003)
US6567533B1	20 May 2003 (20-05-2003)
US6567534B1	20 May 2003 (20-05-2003)
US6567535B2	20 May 2003 (20-05-2003)
US6567780B2	20 May 2003 (20-05-2003)
US6574350B1	03 June 2003 (03-06-2003)
US6577746B1	10 June 2003 (10-06-2003)
US6580808B2	17 June 2003 (17-06-2003)
US6580819B1	17 June 2003 (17-06-2003)
US6587821B1	01 July 2003 (01-07-2003)
US6590996B1	08 July 2003 (08-07-2003)
US6590997B2	08 July 2003 (08-07-2003)
US6590998B2	08 July 2003 (08-07-2003)
US6608911B2	19 August 2003 (19-08-2003)
US6611607B1	26 August 2003 (26-08-2003)
US6614914B1	02 September 2003 (02-09-2003)
US6636615B1	21 October 2003 (21-10-2003)
US6647128B1	11 November 2003 (11-11-2003)
US6647129B2	11 November 2003 (11-11-2003)
US6647130B2	11 November 2003 (11-11-2003)
US6650761B1	18 November 2003 (18-11-2003)
US6654480B2	25 November 2003 (25-11-2003)
US6654887B2	25 November 2003 (25-11-2003)
US6664976B2	16 December 2003 (16-12-2003)
US6674886B2	06 January 2004 (06-01-2004)
US6675146B2	06 January 2004 (06-01-2004)
US6681028B2	20 January 2004 (20-01-2004)
US6681029B1	20 January 2004 (20-01-2004)
US6681030B2	20 January 2004 (20-01-2004)
US6760464B2	06 July 2004 (06-07-2004)
US6694041B1	17 February 2004 (17-02-2004)
US6694042B2	17 February 2004 (17-02-2004)
US6694043B2	17 February 2004 (17-02-2004)
US6700990B1	02 March 2004 (02-03-2004)
US6700995B2	02 March 2004 (02-03-2004)
US6704869B2	09 March 2004 (09-03-2004)
US6718046B2	06 April 2004 (06-04-2004)
US6718047B2	06 April 2004 (06-04-2004)
US6721440B2	13 April 2004 (13-04-2004)
US6724912B1	20 April 2004 (20-04-2004)
US6728390B2	27 April 2004 (27-04-2004)
US6738495B2	18 May 2004 (18-05-2004)
US6744906B2	01 June 2004 (01-06-2004)
US6744907B2	01 June 2004 (01-06-2004)
US6750985B2	15 June 2004 (15-06-2004)
US6751320B2	15 June 2004 (15-06-2004)
US6754377B2	22 June 2004 (22-06-2004)
US6757406B2	29 June 2004 (29-06-2004)
US6760463B2	06 July 2004 (06-07-2004)
US6763122B1	13 July 2004 (13-07-2004)

US6763123B2	13 July 2004 (13-07-2004)
US6763124B2	13 July 2004 (13-07-2004)
US6768808B2	27 July 2004 (27-07-2004)
US6768809B2	27 July 2004 (27-07-2004)
US6771796B2	03 August 2004 (03-08-2004)
US6775392B1	10 August 2004 (10-08-2004)
US6778682B2	17 August 2004 (17-08-2004)
US6782115B2	24 August 2004 (24-08-2004)
US6788800B1	07 September 2004 (07-09-2004)
US6798894B2	28 September 2004 (28-09-2004)
US6804376B2	12 October 2004 (12-10-2004)
US6804377B2	12 October 2004 (12-10-2004)
US6804378B2	12 October 2004 (12-10-2004)
US6804379B2	12 October 2004 (12-10-2004)
US6813366B1	02 November 2004 (02-11-2004)
US6823075B2	23 November 2004 (23-11-2004)
US6829368B2	07 December 2004 (07-12-2004)
US6850626B2	01 February 2005 (01-02-2005)
US6868497B1	15 March 2005 (15-03-2005)
US6869023B2	22 March 2005 (22-03-2005)
US6879701B1	12 April 2005 (12-04-2005)
US6882737B2	19 April 2005 (19-04-2005)
US6882738B2	19 April 2005 (19-04-2005)
US6891959B2	10 May 2005 (10-05-2005)
US6912295B2	28 June 2005 (28-06-2005)
US6917691B2	12 July 2005 (12-07-2005)
US6917724B2	12 July 2005 (12-07-2005)
US6920232B2	19 July 2005 (19-07-2005)
US6922480B2	26 July 2005 (26-07-2005)
US6944298B1	13 September 2005 (13-09-2005)
US6947571B1	20 September 2005 (20-09-2005)
US6950519B2	27 September 2005 (27-09-2005)
US6959100B2	25 October 2005 (25-10-2005)
US6959386B2	25 October 2005 (25-10-2005)
US6961442B2	01 November 2005 (01-11-2005)
US6961444B2	01 November 2005 (01-11-2005)
US6963884B1	08 November 2005 (08-11-2005)
US6965682B1	15 November 2005 (15-11-2005)
US6965683B2	15 November 2005 (15-11-2005)
US6965873B1	15 November 2005 (15-11-2005)
US6968057B2	22 November 2005 (22-11-2005)
US6970573B2	29 November 2005 (29-11-2005)
US6973197B2	06 December 2005 (06-12-2005)
US6975744B2	13 December 2005 (13-12-2005)
US6975746B2	13 December 2005 (13-12-2005)
US6978036B2	20 December 2005 (20-12-2005)
US6983051B1	03 January 2006 (03-01-2006)
US6985600B2	10 January 2006 (10-01-2006)
US6987862B2	17 January 2006 (17-01-2006)
US6988202B1	17 January 2006 (17-01-2006)
US6993149B2	31 January 2006 (31-01-2006)
US6993150B2	31 January 2006 (31-01-2006)
US6993152B2	31 January 2006 (31-01-2006)
US6993154B2	31 January 2006 (31-01-2006)
US6996252B2	07 February 2006 (07-02-2006)
US7003132B2	21 February 2006 (21-02-2006)
US7003731B1	21 February 2006 (21-02-2006)
US7006661B2	28 February 2006 (28-02-2006)
US7010144B1	07 March 2006 (07-03-2006)
US7013021B2	14 March 2006 (14-03-2006)
US7016516B2	21 March 2006 (21-03-2006)
US7020303B2	28 March 2006 (28-03-2006)
US7020304B2	28 March 2006 (28-03-2006)
US7020349B2	28 March 2006 (28-03-2006)
US7022194B2	04 April 2006 (04-04-2006)
US7024016B2	04 April 2006 (04-04-2006)
US7027612B2	11 April 2006 (11-04-2006)
US7027614B2	11 April 2006 (11-04-2006)

US7035427B2	25 April 2006 (25-04-2006)
US7039214B2	02 May 2006 (02-05-2006)
US7042470B2	09 May 2006 (09-05-2006)
US7043052B2	09 May 2006 (09-05-2006)
US7044395B1	16 May 2006 (16-05-2006)
US7050603B2	23 May 2006 (23-05-2006)
US7051086B2	23 May 2006 (23-05-2006)
US7054462B2	30 May 2006 (30-05-2006)
US7054463B2	30 May 2006 (30-05-2006)
US7054465B2	30 May 2006 (30-05-2006)
US7055034B1	30 May 2006 (30-05-2006)
US7058697B2	06 June 2006 (06-06-2006)
US7061510B2	13 June 2006 (13-06-2006)
US7062069B2	13 June 2006 (13-06-2006)
US7063264B2	20 June 2006 (20-06-2006)
US7065228B2	20 June 2006 (20-06-2006)
US7076084B2	11 July 2006 (11-07-2006)
US7095871B2	22 August 2006 (22-08-2006)
US7098931B2	29 August 2006 (29-08-2006)
US7099492B2	29 August 2006 (29-08-2006)
US7103197B2	05 September 2006 (05-09-2006)
US7111168B2	19 September 2006 (19-09-2006)
US7111170B2	19 September 2006 (19-09-2006)
US7113596B2	26 September 2006 (26-09-2006)
US7113614B2	26 September 2006 (26-09-2006)
US7113615B2	26 September 2006 (26-09-2006)
US7116781B2	03 October 2006 (03-10-2006)
US7123740B2	17 October 2006 (17-10-2006)
US7130087B2	31 October 2006 (31-10-2006)
US7136502B2	14 November 2006 (14-11-2006)
US7139408B2	21 November 2006 (21-11-2006)
US7142691B2	28 November 2006 (28-11-2006)
US7143949B1	05 December 2006 (05-12-2006)
US7152021B2	19 December 2006 (19-12-2006)
US7152786B2	26 December 2006 (26-12-2006)
US7158654B2	02 January 2007 (02-01-2007)
US7162052B2	09 January 2007 (09-01-2007)
US7164413B2	16 January 2007 (16-01-2007)
US7164780B2	16 January 2007 (16-01-2007)
US7171016B1	30 January 2007 (30-01-2007)
US7171018B2	30 January 2007 (30-01-2007)
US7171020B2	30 January 2007 (30-01-2007)
US7174031B2	06 February 2007 (06-02-2007)
US7177443B2	13 February 2007 (13-02-2007)
US7181022B2	20 February 2007 (20-02-2007)
US7184570B2	27 February 2007 (27-02-2007)
US7184572B2	27 February 2007 (27-02-2007)
US7185201B2	27 February 2007 (27-02-2007)
US7191156B1	13 March 2007 (13-03-2007)
US7197156B1	27 March 2007 (27-03-2007)
US7197160B2	27 March 2007 (27-03-2007)
US7197164B2	27 March 2007 (27-03-2007)
US7206820B1	17 April 2007 (17-04-2007)
US7207494B2	24 April 2007 (24-04-2007)
US7209571B2	24 April 2007 (24-04-2007)
US7209573B2	24 April 2007 (24-04-2007)
US7213757B2	08 May 2007 (08-05-2007)
US7224819B2	29 May 2007 (29-05-2007)
US7224995B2	29 May 2007 (29-05-2007)
US7225991B2	05 June 2007 (05-06-2007)
US7239734B2	03 July 2007 (03-07-2007)
US7242790B2	10 July 2007 (10-07-2007)
US7246239B2	17 July 2007 (17-07-2007)
US7248715B2	24 July 2007 (24-07-2007)
US7248717B2	24 July 2007 (24-07-2007)
US7249257B2	24 July 2007 (24-07-2007)
US7254249B2	07 August 2007 (07-08-2007)
US7261612B1	28 August 2007 (28-08-2007)

US7263203B2	28 August 2007 (28-08-2007)
US7266217B2	04 September 2007 (04-09-2007)
US7266704B2	04 September 2007 (04-09-2007)
US7269275B2	11 September 2007 (11-09-2007)
US7273836B2	25 September 2007 (25-09-2007)
US7277468B2	02 October 2007 (02-10-2007)
US7286684B2	23 October 2007 (23-10-2007)
US7286685B2	23 October 2007 (23-10-2007)
US7289643B2	30 October 2007 (30-10-2007)
US7298864B2	20 November 2007 (20-11-2007)
US7302574B2	27 November 2007 (27-11-2007)
US7305104B2	04 December 2007 (04-12-2007)
US7305117B2	04 December 2007 (04-12-2007)
US7308110B2	11 December 2007 (11-12-2007)
US7313251B2	25 December 2007 (25-12-2007)
US7313253B2	25 December 2007 (25-12-2007)
US7319775B2	15 January 2008 (15-01-2008)
US7321667B2	22 January 2008 (22-01-2008)
US7330563B2	12 February 2008 (12-02-2008)
US7330564B2	12 February 2008 (12-02-2008)
US7333957B2	19 February 2008 (19-02-2008)
US7340076B2	04 March 2008 (04-03-2008)
US7346776B2	18 March 2008 (18-03-2008)
US7349552B2	25 March 2008 (25-03-2008)
US7349555B2	25 March 2008 (25-03-2008)
US7359528B2	15 April 2008 (15-04-2008)
US7362781B2	22 April 2008 (22-04-2008)
US7362879B2	22 April 2008 (22-04-2008)
US7369676B2	06 May 2008 (06-05-2008)
US7369678B2	06 May 2008 (06-05-2008)
US7372976B2	13 May 2008 (13-05-2008)
US7373513B2	13 May 2008 (13-05-2008)
US7377421B2	27 May 2008 (27-05-2008)
US7391880B2	24 June 2008 (24-06-2008)
US7400743B2	15 July 2008 (15-07-2008)
US7403633B2	22 July 2008 (22-07-2008)
US7406214B2	29 July 2008 (29-07-2008)
US7412072B2	12 August 2008 (12-08-2008)
US7415129B2	19 August 2008 (19-08-2008)
US7418111B2	26 August 2008 (26-08-2008)
US7424131B2	09 September 2008 (09-09-2008)
US7424132B2	09 September 2008 (09-09-2008)
US7427030B2	23 September 2008 (23-09-2008)
US7433491B2	07 October 2008 (07-10-2008)
US7436976B2	14 October 2008 (14-10-2008)
US7437430B2	14 October 2008 (14-10-2008)
US7444000B2	28 October 2008 (28-10-2008)
US7444392B2	28 October 2008 (28-10-2008)
US7450734B2	11 November 2008 (11-11-2008)
US7454035B2	18 November 2008 (18-11-2008)
US7460726B2	02 December 2008 (02-12-2008)
US7461136B2	02 December 2008 (02-12-2008)
US7466840B2	16 December 2008 (16-12-2008)
US7486799B2	03 February 2009 (03-02-2009)
US7499564B2	03 March 2009 (03-03-2009)
US7499566B2	03 March 2009 (03-03-2009)
US7502489B2	10 March 2009 (10-03-2009)
US7502490B2	10 March 2009 (10-03-2009)
US7502759B2	10 March 2009 (10-03-2009)
US7502937B2	10 March 2009 (10-03-2009)
US7505605B2	17 March 2009 (17-03-2009)
US7506169B2	17 March 2009 (17-03-2009)
US7508955B2	24 March 2009 (24-03-2009)
US7515733B2	07 April 2009 (07-04-2009)
US7522728B1	21 April 2009 (21-04-2009)
US7529647B2	05 May 2009 (05-05-2009)
US7532740B2	12 May 2009 (12-05-2009)
US7532741B2	12 May 2009 (12-05-2009)

US7536034B2	19 May 2009 (19-05-2009)
US7536555B2	19 May 2009 (19-05-2009)
US7537170B2	26 May 2009 (26-05-2009)
US7539325B2	26 May 2009 (26-05-2009)
US7545951B2	09 June 2009 (09-06-2009)
US7545952B2	09 June 2009 (09-06-2009)
US7548643B2	16 June 2009 (16-06-2009)
US7555139B2	30 June 2009 (30-06-2009)
US7555785B2	30 June 2009 (30-06-2009)
US7562392B1	14 July 2009 (14-07-2009)
US7564992B2	21 July 2009 (21-07-2009)
US7565294B2	21 July 2009 (21-07-2009)
US7567686B2	28 July 2009 (28-07-2009)
US7567721B2	28 July 2009 (28-07-2009)
US7570781B2	04 August 2009 (04-08-2009)