

COMPRESSED ECDSA SIGNATURES

FIELD OF THE INVENTION:

[0001] The present invention relates to cryptographic schemes and has particular utility in digital signature algorithms.

DESCRIPTION OF THE PRIOR ART

[0002] A digital signature of a message is a number dependent on some secret known only to the signer, and, additionally, on the content of the message being signed. Signatures are meant to be verifiable. If a dispute arises as to whether a party signed a document (caused by either a signer trying to repudiate a signature it did create, or a fraudulent claimant), an unbiased third party should be able to resolve the matter equitably, without requiring access to the signer's secret information (e.g. a private key).

[0003] Digital signatures have many applications in information security, in particular, as they are used in cryptographic schemes. Some applications include authentication, data integrity, and non-repudiation. One particularly significant application of digital signatures is the certification of public keys in large networks. Certification is a means for a trusted third party to bind the identity of a user to a public key, so that at some later time, other entities can authenticate a public key without assistance from the trusted third party.

[0004] A cryptographic scheme known as the Digital Signature Algorithm (DSA) is based on the well known and often discussed intractability of the discrete logarithm problem. The DSA was proposed by the U.S. National Institute of Standards and Technology (NIST) in 1991 and has become a U.S. Federal Information Processing Standard (FIPS 186) called the Digital Signature Standard (DSS). The algorithm is a variant of the well known ElGamal signature scheme, and can be classified as a digital signature with appendix (i.e. one that relies on cryptographic hash functions rather than customized redundancy functions).

[0005] The Elliptic Curve Digital Signature Algorithm (ECDSA) is a signature scheme that may be used in elliptic curve cryptosystem and has attributes similar to the DSA. It is generally regarded as the most widely standardized elliptic curve-based signature scheme, appearing in the ANSI X9.62, FIPS 186-2, IEEE 1363-2000 and ISO/IEC 15946-2 standards as well as several draft standards.

- 1 **[0006]** ECDSA signature generation operates on several domain parameters, a private
2 key d , and a message m . The outputs are the signature (r,s) , where the signature components
3 r and s are integers, and proceeds as follows.
- 4 1. Select a random integer $k \in_R [1, n-1]$, n being one of the domain parameters.
 - 5 2. Compute $kP = (x_1, y_1)$ and convert x_1 to an integer $\bar{x}_1$, where P is a point on an
6 elliptic curve E and is one of the domain parameters.
 - 7 3. Compute $r = \bar{x}_1 \bmod n$, wherein if $r = 0$, then go back to step 1.
 - 8 4. Compute $e = H(m)$, where H denotes a cryptographic hash function whose outputs
9 have a bit length no more than that of n (if this condition is not satisfied, then the
10 outputs of H can be truncated).
 - 11 5. Compute $s = k^{-1}(e + \alpha r) \bmod n$, where α is a long term private key of the signor.
12 If
13 $s = 0$, then go back to step 1.
 - 14 6. Output the pair (r, s) as the ECDSA signature of the message m .
- 15 **[0007]** ECDSA signature verification operates on several domain parameters, a long term
16 public key Q where $Q = \alpha P$, the message m , and the signature (r, s) derived above. ECDSA
17 signature verification outputs a rejection or acceptance of the signature, and proceeds as
18 follows.
- 19 1. Verify that r and s are integers in the interval $[1, n-1]$. If any verification fails
20 then a rejection is returned.
 - 21 2. Compute $e = H(m)$.
 - 22 3. Compute $w = s^{-1} \bmod n$.
 - 23 4. Compute $u_1 = ew \bmod n$ and $u_2 = rw \bmod n$.
 - 24 5. Compute $R = u_1P + u_2Q = s^{-1} (eP + rQ)$ (from 3 and 4 above)

1 6. If $R = \infty$ then the signature is rejected.

2 7. Convert the x-coordinate x_1 of R to an integer $\bar{x}_1$; compute $v = \bar{x}_1 \bmod n$.

3 8. If $v = r$ then the signature is accepted, if not then the signature is rejected.

4 **[0008]** To improve the efficiency of ECDSA signature verification, in particular step 5
5 above that includes an inversion of s , the ECDSA signature has been known to be
6 compressed by truncating s by omitting $2b$ bits. Such compression is at the cost of additional
7 verification steps, which has been known to cost the verifier approximately 2^{2b} extra elliptic
8 curve group operations.

9 **[0009]** Signature compression is particularly desirable in cryptographic applications
10 where bandwidth conservation is of paramount importance, and additional cryptographic
11 operations can be readily handled by the verifier. An example is a two-dimensional barcode,
12 where bandwidth is very limited, but the verifier processor may be fast. Another example is
13 RFID tags, which need power from a radio frequency field in order to transmit data, and
14 therefore low transmission bandwidth is very desirable.

15 **[0010]** A scheme for ECDSA signature compression is needed that has a cost to the
16 verifier that is less than such previous compression schemes.

17 **[0011]** It is therefore an object of the present invention to obviate or mitigate at least one
18 of the above-mentioned disadvantages.

19 SUMMARY OF THE INVENTION

20 **[0012]** In one aspect, there is provided a method of compressing a digital signature of a
21 message, the signature comprising a pair of signature components r, s , the method comprising
22 obtaining a pair of values c, d , related mathematically to s and with one of the values being
23 smaller than s , substituting the one value for the signature component s , in the digital
24 signature and forwarding the signature to a recipient.

25 **[0013]** In another aspect, there is provided, a cryptographic system for generating a
26 compressed signature from a pair of signature components r, s , the system having an

1 arithmetic unit to provide a pair of values c, d mathematically related to the component s , and
2 a signature generator to substitute one of the values for the signature s .

3 [0014] In yet another aspect, there is provided a cryptographic system for verifying a
4 signature r, c received from a sender using a system as defined above comprising an
5 arithmetic unit to recover the other of the values and compare the other value with predefined
6 criteria.

7 [0015] In yet another aspect, a method of compressing a digital signature (r, s) is
8 provided that includes the steps of substituting the value s with a smaller value c , the value c
9 being derived from s and another value d , the value d being small enough such that c is
10 smaller than s ; and substituting the value s with the value c to obtain a compressed signature
11 (r, c) .

12 [0016] In yet another aspect, a method of verifying a compressed signature is provided,
13 the compressed signature including a value c substituted for a value s of a full signature (r, s) ,
14 the method comprising the steps of computing a value d using parameters of the compressed
15 signature and a message, the value c being derived from the value d and the value s ; and
16 verifying the compressed signature if a value for d can be found according to predetermined
17 criteria.

18 BRIEF DESCRIPTION OF THE DRAWINGS

19 [0017] An embodiment of the invention will now be described by way of example only
20 with reference to the appended drawings wherein:

21 [0018] Figure 1 is a cryptographic communication system;

22 [0019] Figure 2 is a flow chart illustrating one embodiment of a signature compression
23 scheme and a signature verification scheme of a compressed signature; and

24 [0020] Figure 3 is flow chart illustrating another embodiment of a signature compression
25 scheme and a signature verification scheme of a compressed signature.

1 DETAILED DESCRIPTION OF THE INVENTION

2 [0021] Referring therefore to Figure 1, a cryptographic communication system is
3 generally denoted by numeral 10. The system 10 has a first correspondent 12 and a second
4 correspondent 14 that may communicate with each other over a communication channel 16.
5 The communication channel 16 may or may not be secure. Each correspondent has a
6 cryptographic module 18 and 20 respectively, for performing cryptographic operations.

7 [0022] Each cryptographic module 18 and 20 is capable of performing elliptic curve
8 cryptographic operations such as ECDSA signature generation and verification schemes
9 operating on the elliptic curve E defined over a field $\mathbb{F}_q$. The embodiments described herein
10 are particularly suitable for an ECDSA algorithm where, for example, the integer s in the
11 signature (r, s) can be compressed at the cost of the verifier needing to perform additional
12 cryptographic operations.

13 [0023] In a first embodiment exemplified in Figure 2, the correspondent 12 may be
14 referred to as a "signer", and the correspondent 14 may be referred to as a "verifier". An
15 ECDSA signature (r, s) , generated by the signer 12 for a message m , is produced as described
16 above. To reduce bandwidth, the signature can be compressed by substituting, for example s ,
17 by a smaller value c . The values s and c in this example are related by the expression
18 $s \equiv \frac{c}{d} \pmod{n}$, the value of d being chosen such that c is a smaller value than s . The possible
19 range of values or 'bounds' for d is part of the system parameters and is used in the
20 verification step for determining if a recovered d is acceptable.

21 [0024] Values for c and d may be obtained by using a variant of the extended Euclidean
22 algorithm to find an equation of the form $ds + un = c$. More precisely, the intermediate steps
23 in the extended Euclidean algorithm compute values x, y, z such that $xs + yn = z$. Normally,
24 the extended Euclidean algorithm begins with small x and y (valued at 0 or 1) and large z (as
25 large as n or s), and ends with large x and y (about the size of n and s respectively) and small
26 z (usually 1, unless n and s have a common factor which will not occur for the choice of n
27 and s in ECDSA). In the present embodiment, the extended Euclidean algorithm is stopped
28 part way, to obtain values of x and y that are intermediate in size, and meet the requirements
29 for d and c , respectively.

1 **[0025]** The value obtained for c is substituted for s in the signature to provide the
2 compressed signature (r, c) . This is then sent from the signer to a recipient.

3 **[0026]** The compressed signature (r, c) may be verified by a recipient by computing a
4 point R , where R can be recovered from r . Recovering R from r may provide several
5 possibilities for R , in which case, the following verification scheme may be attempted by the
6 verifier 14 for each such R . Alternatively, extra information may be sent with, or embedded
7 in, the signature or message m to indicate which of the possible values is the correct choice
8 for R . This may be, for example, the first bit of the value of the y co-ordinate of R or a
9 similar technique. For each such R , the full signature (r, s) is valid, by definition, if and only
10 if $R = s^{-1}(eP + rQ)$, which according to the above notation, is equivalent to
11 $cR = d(eP + rQ)$.

12 **[0027]** To verify the signature (r, c) , the verifier 14 first computes $W = eP + rQ$ which
13 can be done using public information available to the recipient. As discussed above, e is
14 generally computed as a hash of the message m , e.g. $e = H(m)$. The verifier 14 then attempts
15 to compute $d = \log_w(cR)$, using knowledge that d is smaller than a predetermined bound
16 agreed by the signer and verifier for purposes of signature compression. If no such d can be
17 found within the bound, then the compressed signature (r, c) is rejected as being invalid.
18 Similarly, if a value of d is obtained that meets the bounds agreed, the signature may be
19 considered verified. Such discrete logarithm algorithms generally take time proportional to
20 $\sqrt{d}$. If $\sqrt{d}$ is small enough, then it is quite practical for the verifier 14 to use such an
21 algorithm. Once (and if) d is obtained by the verifier 14, the full signature (r, s) can be
22 recovered by computing $s = c / d \bmod n$, allowing the verifier 14 to also use or verify the full
23 signature if he wishes.

24 **[0028]** In another embodiment shown in Figure 3, the compressed signature may be $(r,$
25 $d)$, where d is the value d used in the above notation, and in this case, a recovered value of c
26 is required to meet a particular range of sizes, i.e. be "small enough".

27 **[0029]** Similar to the above embodiment, the value $W = eP + rQ$ is first computed, and
28 then the verifier 14 attempts to compute $c = \log_R(dW)$ using any suitable method for

1 choosing R , which can be done if c is small enough. If no such c can be found, then the
2 compressed signature (r, d) is rejected as being invalid. Once (and if) c is obtained, the
3 signature may be considered to be verified although the full signature (r, s) can be recovered
4 by computing $s = c/d \bmod n$, if the verifier 14 wishes to use or verify the full signature (r, s) .

5 **[0030]** In many practical applications, the choice of R can often be narrowed down to a
6 choice between two values, e.g. R and $-R$, given r alone. In general, algorithms for solving
7 discrete logarithms between R and some point W will also find a logarithm between $-R$ and
8 W , because if the first logarithm is, e.g., u , the other is $-u$. Typically, it is easy to check that $-$
9 u is small enough, so it is generally sufficient to compute one discrete logarithm per pair $(R, -$
10 $R)$ of candidates.

11 **[0031]** The above compression scheme may effectively compress an ECDSA signature
12 by removal of $2b$ bits at the cost of the verifier 14 performing an extra 2^b elliptic curve group
13 operations, where b is a predetermined value selected by the signer. With known
14 compression techniques the cost of saving $2b$ bits was 2^{2b} extra signature verifications, which
15 is considerably more costly for moderate sizes of b .

16 **[0032]** It should be noted that verification, compression and decompression of an ECDSA
17 signature (r, s) can be done without using the private key. From a security perspective, this
18 means that a compressed ECDSA signature is largely guaranteed to be as secure as a full
19 signature, since the private key is not needed to compress or decompress the full signature.
20 From a practical perspective, this means that third parties can provide services using methods
21 that may include the schemes described above to verify a compressed signature. For example,
22 a CA may act as an intermediary to compress signatures created by a signor and forward
23 those to recipients, where they may be verified.

24 **[0033]** Although the invention has been described with reference to certain specific
25 embodiments, various modifications thereof will be apparent to those skilled in the art
26 without departing from the spirit and scope of the invention as outlined in the claims
27 appended hereto. For example, the technique may be used with other discrete log signature
28 algorithms where an ephemeral private key is used to generate a first signature component

- 1 that is then bound to the message and the long term private of the signer to produce a second
- 2 signature component.

1 **Claims:**

2 1. A method of compressing a digital signature of a message, said signature comprising a
3 pair of signature components r , s , said method comprising obtaining a pair of values c , d
4 related mathematically to s and with one of said values being smaller than s , substituting
5 said one value for the signature component s , in said digital signature and forwarding said
6 signature to a recipient.

7 2. A method according to claim 1 wherein both said values c , d meet predetermined criteria.

8

9 3. A method according to claim 2 wherein said value of d is required to fall within
10 predefined bounds.

11

12 4. A method according to claim 3 wherein said value c is smaller than said component s .

13

14 5. A method according to claim 4 wherein said components r , s represent an ECDSA
15 signature.

16

17 6. A method according to claim 1 wherein s , c , and d are related such that $s=c/d \bmod n$.

18

19 7. A method according to claim 6 where said values c , d are obtained to meet predetermined
20 criteria.

21

22 8. A method according to claim 7 wherein said values c , d are obtained by application of an
23 extended Euclidean algorithm and iterations of said algorithm are terminated when said
24 predetermined criteria are met.

25

26 9. A method according to claim 6 wherein said one value corresponds to c .

27

28 10. A method according to claim 6 wherein said one value corresponds to d .

29

- 1 11. A method of verifying a signature generated in accordance with claim 1 by recovering
2 from said signature a value equivalent to the other of said values and determining if it
3 meets defined criteria.
4
- 5 12. A method according to claim 11 wherein recovery of said other value is obtained from
6 combining said signature components.
7
- 8 13. A method according to claim 12 wherein an intermediate value is obtained from said
9 message and combined with values obtained from said signature components to recover
10 said other value.
11
- 12 14. A method according to claim 11 wherein said other value is required to fall within
13 defined bounds.
14
- 15 15. A method according to claim 11 including the step of rejecting said signature if said other
16 value does not meet said predefined criteria.
17
- 18 16. A method according to claim 11 including the step of accepting said signature if said
19 other value meets said predefined criteria.
20
- 21 17. A method according to claim 16 wherein a further verification is performed on an original
22 signature obtained from application of said one value and said other value recovered by
23 said recipient to said signature received by said recipient.
24
- 25 18. A cryptographic system for generating a compressed signature from a pair of signature
26 components r , s , said system having an arithmetic unit to provide a pair of values c , d
27 mathematically related to said component s , and a signature generator to substitute one of
28 said values for said signature s .
29
- 30 19. A cryptographic system for verifying a signature r , c received from a sender using a
31 system as claimed in claim 18 comprising an arithmetic unit to recover the other of said
32 values and compare said other value with predefined criteria.