Claims:

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

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

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

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

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

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

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

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

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

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

11. A method of verifying a signature generated in accordance with claim 1 by recovering from said signature a value equivalent to the other of said values and determining if it meets defined criteria.

12. A method according to claim 11 wherein recovery of said other value is obtained from combining said signature components.

13. A method according to claim 12 wherein an intermediate value is obtained from said message and combined with values obtained from said signature components to recover said other value.

14. A method according to claim 11 wherein said other value is required to fall within defined bounds.

15. A method according to claim 11 including the step of rejecting said signature if said other value does not meet said predefined criteria.

16. A method according to claim 11 including the step of accepting said signature if said other value meets said predefined criteria.

17. A method according to claim 16 wherein a further verification is performed on an original signature obtained from application of said one value and said other value recovered by said recipient to said signature received by said recipient.

18. A cryptographic system for generating a compressed signature from a pair of signature components r, s, said system having an arithmetic unit to provide a pair of values c, d mathematically related to said component s, and a signature generator to substitute one of said values for said signature s.

19. A cryptographic system for verifying a signature r, c received from a sender using a system as claimed in claim 18 comprising an arithmetic unit to recover the other of said values and compare said other value with predefined criteria.

The invention claimed is:

1. A method of compressing a digital signature of a message, said signature comprising a pair of signature components r, s, said method being performed by a correspondent in a data communication system, the correspondent having a cryptographic module for performing cryptographic operations, said method comprising:

said cryptographic module obtaining a pair of values c, d related mathematically to s, one of said values being smaller than s and said one of said values having a smaller number of bits than s, the other of said values being required to fall within predefined bounds;

said cryptographic module generating a compressed signature by substituting said one of said values for the signature component s, in said digital signature; and

said correspondent forwarding said compressed signature to a recipient.

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

3. The method according to claim 1 wherein said value c is smaller than said component s.

4. The method according to claim 3 wherein said components r, s represent an ECDSA signature.

5. The method according to claim 1 wherein s, c, and d are related such that $s \equiv c/d \bmod n$.

6. The method according to claim 5 where said values c, d are obtained to meet predetermined criteria.

7. The method according to claim 6 wherein said values c, d are obtained by application of an extended Euclidean algorithm and iterations of said algorithm are terminated when said predetermined criteria are met.

8. The method according to claim 5 wherein said one of said values corresponds to c.

9. The method according to claim 5 wherein said one of said values corresponds to d.

10. The method according to claim 1, wherein said signature component r is obtained from an integer k and said signature component s binds said integer k, a long term private key α and said signature component r to said message.

11. A method of verifying a compressed signature, said method of verifying said compressed signature being performed by a correspondent in a data communication system, the correspondent having a cryptographic module for performing cryptographic operations, said method of verifying said compressed signature comprising:

said cryptographic module obtaining said compressed signature, said compressed signature generated from a digital signature of a message, said digital signature having signature components r,s, said compressed signature having signature components r and one of a pair of values c,d, said values c,d related mathematically to s, one of said values being smaller than s and said one of said values having a smaller number of bits than s, the other of said values being required to fall within predefined bounds;

said cryptographic module recovering from said compressed signature said other of said values; and

said cryptographic module determining whether said recovered other of said values meets predefined criteria.

12. The method of verifying a compressed signature according to claim 11 wherein recovery of said other of said values is obtained from combining said signature components of said compressed signature.

13. The method of verifying a compressed signature according to claim 12 wherein an intermediate value is obtained from said message and combined with values obtained from said signature components of said compressed signature to recover said other of said values.

14. The method of verifying a compressed signature according to claim 11 wherein said predefined criteria comprises said recovered other of said values being required to fall within the predefined bounds.

15. The method of verifying a compressed signature according to claim 11 further comprising:

said cryptographic module rejecting said compressed signature if said recovered other of said values does not meet said predefined criteria; and

said cryptographic module accepting said compressed signature if said recovered other of said values meets said predefined criteria.

16. The method of verifying a compressed signature according to claim 15 wherein a further verification is performed on an original signature obtained from application of said one of said values and said recovered other of said values to said compressed signature.

17. A cryptographic system for generating a compressed signature from a digital signature, said digital signature comprising a pair of signature components r, s, said system comprising:

an arithmetic unit to provide a pair of values c, d mathematically related to said component s, one of said values being smaller than s and said one of said values having a smaller number of bits than s, the other of said values being required to fall within predefined bounds; and

a signature generator to substitute said one of said values for said signature component s, in said digital signature.

18. A cryptographic system for verifying a compressed signature sender generated using the system according to claim 17, said cryptographic system comprising an arithmetic unit to recover said other of said values and compare said other of said values with predefined criteria.

19. The cryptographic system according to claim 17, wherein said signature component r is obtained from an integer k and said signature component s binds said integer k, a long term private key α and said signature component r to said message.