

UNITED STATES DISTRICT COURT

EASTERN

District of

MARSHALL

CERTICOM CORP. and CERTICOM PATENT
HOLDING CORP.

SUMMONS IN A CIVIL ACTION

V.
SONY CORPORATION, ET AL.

CASE NUMBER: 2:07-cv-216

TO: (Name and address of Defendant)

Sony DADC US, Inc., by and through its registered agent of service,
Corporation Service Company, 2711 Centerville Rd., Suite 400,
Wilmington, DE 19808.

YOU ARE HEREBY SUMMONED and required to serve on PLAINTIFF'S ATTORNEY (name and address)

Robert C. Morgan
Ropes & Gray LLP
1211 Avenue of the Americas
New York, NY 10036-8704

an answer to the complaint which is served on you with this summons, within 20 days after service of this summons on you, exclusive of the day of service. If you fail to do so, judgment by default will be taken against you for the relief demanded in the complaint. Any answer that you serve on the parties to this action must be filed with the Clerk of this Court within a reasonable period of time after service.

DAVID MALAND, CLERK

MAY 31 2007

CLERK OF COURT

DATE



RETURN OF SERVICE

Service of the Summons and complaint was made by me ⁽¹⁾	DATE
NAME OF SERVER (<i>PRINT</i>)	TITLE

Check one box below to indicate appropriate method of service

- Served personally upon the defendant. Place where served:

- Left copies thereof at the defendant's dwelling house or usual place of abode with a person of suitable age and discretion then residing therein.
 Name of person with whom the summons and complaint were left:

- Returned unexecuted:

- Other (specify):

STATEMENT OF SERVICE FEES

TRAVEL	SERVICES	TOTAL \$0.00
--------	----------	--------------

DECLARATION OF SERVER

I declare under penalty of perjury under the laws of the United States of America that the foregoing information contained in the Return of Service and Statement of Service Fees is true and correct.

Executed on _____ Date _____ Signature of Server _____

Address of Server

(1) As to who may serve a summons see Rule 4 of the Federal Rules of Civil Procedure.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

FILED-CLERK
U.S. DISTRICT COURT
2007 MAY 30 AM 9:23
TX EASTERN-MARSHALL

CERTICOM CORP. and CERTICOM)
PATENT HOLDING CORP.,)
)
Plaintiffs,)
)
v.)
)
SONY CORPORATION, SONY)
CORPORATION OF AMERICA, SONY)
COMPUTER ENTERTAINMENT INC.,)
SONY COMPUTER ENTERTAINMENT)
AMERICA INC., SONY PICTURES)
ENTERTAINMENT INC., SONY)
ELECTRONICS INC. and SONY DADC)
US INC.)
)
Defendants.)

BY _____

Civil Action No. 2 - 07 C V - 216 - TJW

JURY

COMPLAINT

Plaintiffs Certicom Corp. and Certicom Patent Holding Corp. ("CPH") (collectively, Certicom Corp. and CPH are "Certicom") hereby file this complaint for patent infringement against Sony Corporation ("Sony Japan"), Sony Corporation of America ("Sony America"), Sony Computer Entertainment Inc. ("SCE Japan"), Sony Computer Entertainment America Inc. ("SCE America"), Sony Pictures Entertainment Inc. ("Sony Pictures"), Sony Electronics Inc. ("Sony Electronics"), and Sony DADC US Inc. ("Sony DADC") (collectively, Sony Japan, Sony America, SCE Japan, SCE America, Sony Pictures, and Sony DADC are "Defendants") and states as follows:

THE PARTIES

1. Certicom Corp. is a Canadian corporation with its principal executive offices at 5520 Explorer Drive, Mississauga, Ontario, Canada L4W 5L1. Certicom Corp. has offices in Reston, Virginia and Foster City, California and does business in the State of Texas.

2. CPH is an Ontario corporation with its principal place of business at 5520 Explorer Drive, Mississauga, Ontario, Canada L4W 5L1. CPH is a wholly-owned subsidiary of Certicom Corp. and holds certain rights relating to U.S. Patent Nos. 6,563,928 and 6,704,870.

3. Certicom Corp. is a leader in providing the strong, efficient cryptography increasingly required by government, multinational companies, content providers, systems integrators and device manufacturers, to embed security into their products. The company's expertise is also recognized through industry and leadership awards. Most recently, Certicom Corp. received the 2006 Private Sector Leadership in Advanced Technology Award for innovation, expertise and leadership in security from the Canadian Advanced Technology Alliance (CATA).

4. Certicom Corp's Elliptic Curve Cryptography (ECC)-based solutions provide exceptional security and have been adopted by the U.S. Government's National Security Agency (NSA). In 2003, the NSA paid \$25 million to Certicom Corp. for the non-exclusive, worldwide license of 26 Certicom ECC patents, including the patents-in-suit (Certicom's U.S. Patent Nos. 6,563,928 and 6,704,870), for classified government communications. In February 2005, the NSA named ECC as the approved technology for key agreement and digital signature standards for the U.S. Government.

5. Certicom's U.S. Patent Nos. 6,563,928 and 6,704,870 have enjoyed great commercial success. In addition to being licensed by the NSA, they also have been licensed by

major companies. In addition, numerous companies have licensed and received from Certicom encryption solution software which implements these patents.

6. On information and belief, Sony Japan is a Japanese corporation with a place of business at 6-7-35 Kita-Shinagawa, Shinagawa-ku, Tokyo, Japan. On information and belief, Sony Japan, directly and indirectly, with and through its wholly owned subsidiaries, manufactures and imports into the United States, and distributes, sells and offers to sell in the United States, including in the State of Texas and this judicial district, products that utilize encryption systems in accordance with the Advanced Access Content System (AACS) specification and the Digital Transmission Content Protection (DTCP) specification ("Sony Japan Products").

7. The Sony Japan Products include, but are not limited to, all products that utilize Sony's DTCP-enabled i.LINK™, DTCP-IP and/or Blu-ray technology.

8. The Sony Japan Products include, but are not limited to, the following products: Sony BDP-S1 Blu-ray disc player, Sony BWU-100A Blu-ray disc rewritable drive, Sony PlayStation 3 console, Sony PlayStation 3 software distributed on Blu-ray discs, motion pictures and television shows distributed on Blu-ray discs, Blu-ray discs, Sony VAIO computers with i.LINK™ ports, DTCP-IP and/or Blu-ray drives, Sony KDL-32XBR950 television, Sony KDL-42XBR950 television, Sony KDF-60XBR950 television, Sony KDF-70XBR950 television, Sony KDP-51WS550 television, Sony KDP-57WS550 television, Sony KDP-65WS550 television, Sony KDE-42BR950 television, Sony KDE-50BR950 television, Sony KDE-61BR950 television, Sony KDS-R50XBR1 television, Sony KDS-60XBR1 television, Sony VAIO i.LINK DVD+/-R DL/DVD+/-RW Drive External, Sony RDR-GX330 DVD player, Sony DRD-VX555 DVD player, Sony DVP-NS9100ES/B DVD player, Sony HDW-D1800 (with HKDW-105

board) VTR, Sony STR-DA9000ES home theater receiver, Sony SCD-XA9000ES super audio CD player, Sony VGX-XL3 VAIO digital living system, and Sony VGX-TP1 VAIO living room PC.

9. The Sony Japan Products are sold and offered for sale in Sony Style stores in the State of Texas, through the World Wide Web at www.Sonystyle.com, and at retail stores located within this judicial district. Sony Japan has voluntarily and purposely placed the Sony Japan Products into the stream of commerce with the expectation that they will be offered for sale and sold in the State of Texas, including this judicial district.

10. On information and belief, Sony America is a New York corporation with its principal place of business at 550 Madison Avenue, New York, New York 10022-3211. On information and belief, Sony America is a wholly owned subsidiary of Sony Japan. On information and belief, Sony America markets, sells, offers for sale and distributes in the United States, including in the State of Texas and this judicial district, products that utilize encryption systems in accordance with the AAC3 specification and the DTCP specification ("Sony America Products").

11. The Sony America Products include, but are not limited to, all products that utilize Sony's DTCP-enabled i.LINK™, DTCP-IP and/or Blu-ray technology.

12. The Sony America Products include, but are not limited to, the following products: Sony BDP-S1 Blu-ray disc player, Sony BWU-100A Blu-ray disc rewritable drive, Sony PlayStation 3 console, Sony PlayStation 3 software distributed on Blu-ray discs, motion pictures and television shows distributed on Blu-ray discs, Blu-ray discs, Sony VAIO computers with i.LINK™ ports, DTCP-IP and/or Blu-ray drives, Sony KDL-32XBR950 television, Sony KDL-42XBR950 television, Sony KDF-60XBR950 television, Sony KDF-70XBR950

television, Sony KDP-51WS550 television, Sony KDP-57WS550 television, Sony KDP-65WS550 television, Sony KDE-42BR950 television, Sony KDE-50BR950 television, Sony KDE-61BR950 television, Sony KDS-R50XBR1 television, Sony KDS-60XBR1 television, Sony VAIO i.LINK DVD+/-R DL/DVD+/-RW Drive External, Sony RDR-GX330 DVD player, Sony DRD-VX555 DVD player, Sony DVP-NS9100ES/B DVD player, Sony HDW-D1800 (with HKDW-105 board) VTR, Sony STR-DA9000ES home theater receiver, Sony SCD-XA9000ES super audio CD player, Sony VGX-XL3 VAIO digital living system, and Sony VGX-TPI VAIO living room PC.

13. The Sony America Products are sold and offered for sale in Sony Style stores in the State of Texas, through the World Wide Web at www.Sonystyle.com, and at retail stores located within this judicial district. Sony America has voluntarily and purposely placed the Sony America Products into the stream of commerce with the expectation that they will be offered for sale and sold in the State of Texas, including this judicial district.

14. On information and belief, SCE Japan is a Japanese corporation with a place of business at 2-6-21 Minami-Aoyama, Minato-Ku, Tokyo, 107-0062, Japan. On information and belief, SCE Japan is a wholly owned subsidiary of Sony Japan. On information and belief, SCE Japan, directly and indirectly, with and through other Sony entities, manufactures and imports into the United States and distributes, sells and offers to sell in the United States, including in the State of Texas and this judicial district, products that utilize encryption systems in accordance with the AACS specification and the DTCP specification ("SCE Japan Products").

15. The SCE Japan Products include, but are not limited to, all products that utilize Sony's DTCP-enabled i.LINK™, DTCP-IP and/or Blu-ray technology.

16. The SCE Japan Products include, but are not limited to, the Sony PlayStation 3 console and Sony PlayStation 3 software distributed on Blu-ray discs.

17. The SCE Japan Products are sold and offered for sale in Sony Style stores in the State of Texas, through the World Wide Web at www.Sonystyle.com, and at retail stores located in this judicial district. SCE Japan has voluntarily and purposely placed the SCE Japan Products into the stream of commerce with the expectation that they will be offered for sale and sold in the State of Texas, including this judicial district.

18. On information and belief, SCE America is a Delaware corporation with its headquarters at 919 East Hillsdale Boulevard, 2nd Floor, Foster City, California 94404. On information and belief, SCE America is a wholly owned subsidiary of SCE Japan and is the marketing and sales arm of SCE Japan in the United States. On information and belief, SCE America markets, sells, offers for sale and distributes in the United States, including in the State of Texas and this judicial district, products that utilize encryption systems in accordance with the AAC3 specification and the DTCP specification ("SCE America Products").

19. The SCE America Products include, but are not limited to, all products that utilize Sony's DTCP-enabled i.LINK™, DTCP-IP and/or Blu-ray technology.

20. The SCE America products include, but are not limited to, the Sony PlayStation 3 console and Sony PlayStation 3 software distributed on Blu-ray discs.

21. The SCE America Products are sold and offered for sale in Sony Style stores in the State of Texas, through the World Wide Web at www.Sonystyle.com, and at retail stores located in this judicial district. SCE America has voluntarily and purposely placed the SCE America Products into the stream of commerce with the expectation that they will be offered for sale and sold in the State of Texas, including this judicial district.

22. On information and belief, Sony Electronics is a Delaware corporation with its principal place of business at 16450 West Bernardo Street, San Diego, California 92127. On information and belief, Sony Electronics is a wholly owned subsidiary of Sony America. On information and belief, Sony Electronics markets, sells, offers for sale and distributes in the United States, including in the State of Texas and this judicial district, products that utilize encryption systems in accordance with the AAC3 specification and the DTCP specification ("Sony Electronics Products").

23. The Sony Electronics Products include, but are not limited to, all products that utilize Sony's DTCP-enabled i.LINK™, DTCP-IP and/or Blu-ray technology.

24. The Sony Electronics Products include, but are not limited to, the following products: Sony BDP-S1 Blu-ray disc player, Sony BWU-100A Blu-ray disc rewritable drive, Sony VAIO computers with i.LINK™ ports, DTCP-IP and/or Blu-ray drives, Sony KDL-32XBR950 television, Sony KDL-42XBR950 television, Sony KDF-60XBR950 television, Sony KDF-70XBR950 television, Sony KDP-51WS550 television, Sony KDP-57WS550 television, Sony KDP-65WS550 television, Sony KDE-42BR950 television, Sony KDE-50BR950 television, Sony KDE-61BR950 television, Sony KDS-R50XBRI television, Sony KDS-60XBRI television, Sony VAIO i.LINK DVD+/-R DL/DVD+/-RW Drive External, Sony RDR-GX330 DVD player, Sony DRD-VX555 DVD player, Sony DVP-NS9100ES/B DVD player, Sony HDW-D1800 (with HKDW-105 board) VTR, Sony STR-DA9000ES home theater receiver, Sony SCD-XA9000ES super audio CD player, Sony VGX-XL3 VAIO digital living system, and Sony VGX-TP1 VAIO living room PC.

25. The Sony Electronics Products are sold and/or offered for sale in Sony Style stores in the State of Texas, through the World Wide Web at www.Sonystyle.com, and at retail

stores located in this judicial district. Sony Electronics has voluntarily and purposely placed the Sony Electronics Products into the stream of commerce with the expectation that they will be offered for sale and sold in the State of Texas, including this judicial district.

26. On information and belief, Sony Pictures is a Delaware corporation with a principal place of business at 10202 West Washington Boulevard, Culver City, California 90232. On information and belief Sony Pictures is a wholly owned subsidiary of Sony America. On information and belief, Sony Pictures markets, sells, offers for sale and distributes in the United States, including in the State of Texas and this judicial district, products that utilize encryption systems in accordance with the AACCS specification ("Sony Pictures Products").

27. The Sony Pictures Products include, but are not limited to, all products that utilize Sony's Blu-ray technology.

28. The Sony Pictures Products include, but are not limited to, motion pictures and television shows distributed on Blu-ray discs. The Sony Pictures Products are sold and offered for sale in Sony Style stores in the State of Texas, through the World Wide Web at www.Sonystyle.com, and at retail stores located in this judicial district. Sony Pictures has voluntarily and purposely placed the Sony Pictures Products into the stream of commerce with the expectation that they will be offered for sale and sold in the State of Texas, including this judicial district.

29. On information and belief, Sony DADC is a Delaware corporation with a principal place of business in Terre Haute, Indiana. On information and belief, Sony DADC is a wholly owned subsidiary of Sony America. On information and belief, Sony DADC manufactures, markets, sells, offers for sale and distributes in the United States, including in the

State of Texas and this judicial district, products that utilize encryption systems in accordance with the AACS specification (“Sony DADC Products”).

30. The Sony DADC Products include, but are not limited to, all products that utilize Sony’s Blu-ray technology.

31. The Sony DADC Products include, but are not limited to, Blu-ray discs.

32. On information and belief, the Sony DADC Products are sold and offered for sale in Sony Style stores in the State of Texas, through the World Wide Web at www.Sonystyle.com, and at retail stores located in this judicial district. Sony DADC has voluntarily and purposely placed the Sony DADC Products into the stream of commerce with the expectation that they will be offered for sale and sold in the State of Texas, including this judicial district.

JURISDICTION AND VENUE

33. This is an action for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code. This Court has subject-matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

34. As stated above in paragraphs 6-12, Defendants regularly and deliberately engage in activities that occur in and/or result in sales of goods and services in the State of Texas and in this judicial district that infringe United States Patents owned by Certicom. This Court has personal jurisdiction over Defendants.

35. Venue is proper in this judicial district pursuant to 28 U.S.C. §§ 1391(b)-(d) and 1400(b).

COUNT I

INFRINGEMENT OF U.S. PATENT NO. 6,563,928

36. Paragraphs 1-15 are hereby incorporated by reference as if fully set forth herein.

37. On May 13, 2003, United States Patent No. 6,563,928 (the “‘928 Patent”) entitled “Strengthened Public Key Protocol” was duly and legally issued by the United States Patent and Trademark Office with Scott A. Vanstone, Alfred John Menezes and Minghua Qu as the named inventors. A true and correct copy of the ‘928 Patent is attached hereto as Exhibit A.

38. The ‘928 Patent has been in full force and effect since its issuance. Certicom Corp. owns by assignment the entire right, title and interest in and to the ‘928 Patent. CPH holds an exclusive license to utilize and exploit for commercial purposes the ‘928 Patent, including the right to license the ‘928 Patent and the right to sue for past, present and future infringement of the ‘928 Patent. Certicom further holds a non-exclusive license and right to sub-license the ‘928 Patent. Certicom has complied with the notice provisions of 35 U.S.C. § 287 with respect to the ‘928 Patent.

39. Defendants have, and each one of them has, directly infringed, induced others to infringe, and committed acts of contributory infringement, of one or more claims of the ‘928 Patent, pursuant to one or more sections of 35 U.S.C. §§ 271(a)-(g), by making, using, selling, and offering to sell in the United States, and importing into the United States products that utilize encryption systems which infringe that patent. The infringing products are all products that utilize encryption systems in accordance with the DTCP specification and include, but are not limited to, all products which include DTCP-enabled i.LINK™ and DTCP-IP technology.

40. The infringing products include, but are not limited to, the Sony VAIO computers with i.LINK™ ports and/or DTCP-IP, Sony KDL-32XBR950 television, Sony KDL-42XBR950 television, Sony KDF-60XBR950 television, Sony KDF-70XBR950 television, Sony KDP-51WS550 television, Sony KDP-57WS550 television, Sony KDP-65WS550 television, Sony KDE-42BR950 television, Sony KDE-50BR950 television, Sony KDE-61BR950 television,

Sony KDS-R50XBR1 television, Sony KDS-60XBR1 television, Sony VAIO i.LINK DVD+/-R DL/DVD+/-RW Drive External, Sony RDR-GX330 DVD player, Sony DRD-VX555 DVD player, Sony DVP-NS9100ES/B DVD player, Sony HDW-D1800 (with HKDW-105 board) VTR, Sony STR-DA9000ES home theater receiver, Sony SCD-XA9000ES super audio CD player, Sony VGX-XL3 VAIO digital living system, and Sony VGX-TP1 VAIO living room PC.

41. On information and belief, Defendants have been aware of the existence of the '928 Patent, but have nevertheless infringed the '928 Patent. Defendants' infringement of the '928 Patent has been and continues to be deliberate and willful, thus rendering this case "exceptional" as that term is set forth in 35 U.S.C. § 285.

COUNT II

INFRINGEMENT OF U.S. PATENT NO. 6,704,870

42. Paragraphs 1-15 are hereby incorporated by reference as if fully set forth herein.

43. On March 9, 2004, United States Patent No. 6,704,870 (the "'870 Patent") entitled "Digital Signatures on a Smartcard" was duly and legally issued by the United States Patent and Trademark Office with Scott A. Vanstone and Alfred J. Menezes as the named inventors. A true and correct copy of the '870 Patent is attached hereto as Exhibit B.

44. The '870 Patent has been in full force and effect since its issuance. Certicom Corp. owns by assignment the entire right, title and interest in and to the '870 Patent. CPH holds an exclusive license to utilize and exploit for commercial purposes the '870 Patent, including the right to license the '870 Patent and the right to sue for past, present and future infringement of the '870 Patent. Certicom further holds a non-exclusive license and right to sub-license the '870 Patent. Certicom has complied with the notice provisions of 35 U.S.C. § 287 with respect to the '870 Patent.

45. Defendants have, and each one of them has, directly infringed, and induced others to infringe, and committed acts of contributory infringement, of one or more claims of the '870 Patent, pursuant to one or more sections of 35 U.S.C. §§ 271(a)-(g), by making, using, selling, and offering to sell in the United States, and/or importing into the United States products that utilize encryption systems which infringe that patent. The infringing products are all products that utilize encryption systems in accordance with the AACS specification and/or the DTCP specification and include, but are not limited to, all products which include DTCP-enabled i.LINK™, DTCP-IP and/or Blu-ray technology.

46. The infringing products include, but are not limited to, the Sony BDP-S1 Blu-ray disc player, Sony BWU-100A Blu-ray disc rewritable drive, Sony PlayStation 3 console, Sony PlayStation 3 software distributed on Blu-ray discs, motion pictures and television shows distributed on Blu-ray discs, Blu-ray discs, Sony VAIO computers with i.LINK™ ports, DTCP-IP and/or Blu-ray drives, Sony KDL-32XBR950 television, Sony KDL-42XBR950 television, Sony KDF-60XBR950 television, Sony KDF-70XBR950 television, Sony KDP-51WS550 television, Sony KDP-57WS550 television, Sony KDP-65WS550 television, Sony KDE-42BR950 television, Sony KDE-50BR950 television, Sony KDE-61BR950 television, Sony KDS-R50XBR1 television, Sony KDS-60XBR1 television, Sony VAIO i.LINK DVD+/-R DL/DVD+/-RW Drive External, Sony RDR-GX330 DVD player, Sony DRD-VX555 DVD player, Sony DVP-NS9100ES/B DVD player, Sony HDW-D1800 (with HKDW-105 board) VTR, Sony STR-DA9000ES home theater receiver, Sony SCD-XA9000ES super audio CD player, Sony VGX-XL3 VAIO digital living system, and Sony VGX-TP1 VAIO living room PC.

47. On information and belief, Defendants have been aware of the existence of the '870 Patent, but have nevertheless infringed the '870 Patent. Defendants' infringement of the

'870 Patent has been and continues to be deliberate and willful, thus rendering this case "exceptional" as that term is set forth in 35 U.S.C. § 285.

DEMAND FOR RELIEF

WHEREFORE, Certicom demands entry of judgment that:

A. Each Defendant has infringed and induced infringement of and contributed to the infringement of U.S. Patent No. 6,563,928 and U.S. Patent No. 6,704,870;

B. Each Defendant and any of its respective officers, agents, servants, employees, subsidiaries, parents, attorneys, and all persons acting in concert, on behalf of, in joint venture, or in partnership with each Defendant be enjoined from infringing, inducing to infringe and contributing to the infringement of U.S. Patent No. 6,563,928 and U.S. Patent No. 6,704,870;

C. Damages be awarded to Certicom sufficient to compensate for Defendants' infringement of U.S. Patent No. 6,563,928 and U.S. Patent No. 6,704,870;

D. Each Defendant's infringement of U.S. Patent No. 6,563,928 and U.S. Patent No. 6,704,870 is willful and deliberate;

E. This case is an exceptional case pursuant to 35 U.S.C. § 285;

F. The damages awarded to Certicom be trebled pursuant to 35 U.S.C. § 284 and that Certicom be awarded its reasonable costs and attorneys' fees incurred in connection with this action pursuant to 35 U.S.C. § 285;


G. Defendants' pay Certicom pre-judgment and post-judgment interest on the damages awarded;

H. In the event a permanent injunction against future acts of infringement is not granted by the Court, that Certicom be awarded a compulsory ongoing license fee; and

I. Certicom be granted such other and further relief as this Court may deem just and proper.

Respectfully submitted,

ROPES & GRAY LLP

By:  *Robert C. Morgan by perm. MCS*
Robert C. Morgan
Laurence S. Rogers
ROPES & GRAY LLP
1211 Avenue of the Americas
New York, New York 10036-8704
Tel.: (212) 596-9000

Dated: May 30, 2007

THE ROTH LAW FIRM
Carl R. Roth
Texas Bar No. 17312000
Michael C. Smith
Texas Bar No. 18650410
115 N. Wellington, Suite 200
Marshall, Texas 75670
Telephone: (903) 935-1665
Facsimile: (903) 935-1797

*Attorneys for Plaintiffs Certicom Corp. and
Certicom Patent Holding Corp.*

EXHIBIT A

(12) United States Patent
Vanstone et al.

(10) Patent No.: US 6,563,928 B1
(45) Date of Patent: May 13, 2003

- (54) **STRENGTHENED PUBLIC KEY PROTOCOL**
- (75) **Inventors:** Scott A. Vanstone, Waterloo (CA);
 Alfred John Menezes, Waterloo (CA);
 Minghua Qu, Waterloo (CA)
- (73) **Assignee:** Certicom Corp., Ontario (CA)
- (*) **Notice:** Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

5,497,423 A	3/1996	Miyaji	380/30
5,581,616 A	12/1996	Crandall	380/30
5,600,725 A	2/1997	Rueppel et al.	380/30
5,625,692 A	4/1997	Herzberg et al.	380/21
5,724,425 A	3/1998	Chang et al.	380/25
5,761,305 A	6/1998	Vanstone et al.	380/21
5,768,388 A	6/1998	Goldwasser et al.	380/30
5,987,131 A	11/1999	Clapp	713/171

- (21) **Appl. No.:** 09/283,658
 (22) **Filed:** Apr. 1, 1999

Related U.S. Application Data

- (63) Continuation of application No. 08/649,308, filed on May 17, 1996, now Pat. No. 5,933,504.

(30) Foreign Application Priority Data

May 18, 1995 (GB) 9510035

- (51) **Int. Cl.⁷** H04L 9/00
 (52) **U.S. Cl.** 380/30; 380/28; 380/285
 (58) **Field of Search** 380/28, 30, 44,
 380/285, 277, 282; 713/170, 171, 180

(56) References Cited

U.S. PATENT DOCUMENTS

4,351,982 A	9/1982	Miller et al.	380/30
4,405,829 A	9/1983	Rivest et al.	380/30
4,633,036 A	12/1986	Hellman et al.	380/30
4,956,863 A	9/1990	Goss	380/30
5,150,411 A	9/1992	Maurer	380/30
5,159,632 A	10/1992	Crandall	380/30
5,271,061 A	12/1993	Crandall	380/30
5,272,755 A	12/1993	Miyaji et al.	380/30
5,299,263 A	3/1994	Beller et al.	380/30
5,442,707 A	8/1995	Miyaji et al.	380/30
5,463,690 A	10/1995	Crandall	380/30

OTHER PUBLICATIONS

Abdalla, Bellare, Rogaway; DHIES: An encryption scheme based on the Diffie-Hellman Problem, Sep. 18, 2001, pp. 1-25.*
 Tilborg, Elliptic Curve Cryptosystems; too good to be true?; Sep. 2001, pp. 220-225.*
 Schroepfel, Orman, O'Malley; Fast Key exchange with Elliptic Curve Systems; Mar. 31, 1995; pp. 1-9.*
 Schneier; Applied Cryptography; second edition, 1996, pp. 513-525, 480-481.*

* cited by examiner

Primary Examiner—Gail Hayes

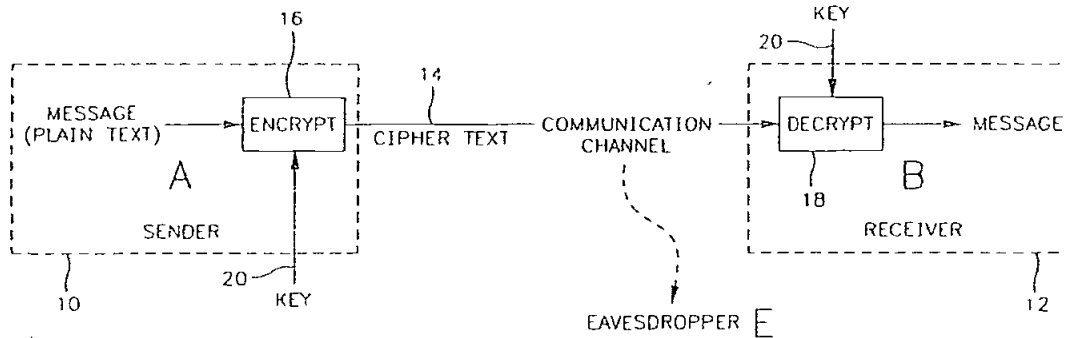
Assistant Examiner—Hosuk Song

(74) *Attorney, Agent, or Firm*—The Maxham Firm

(57) ABSTRACT

A cryptosystem utilizes the properties of discrete logs in finite groups, either in a public key message exchange or in a key exchange and generation protocol. If the group selected has subgroups of relatively small order, the message may be exponentiated by a factor of the order of the group to place the message in a subgroup of relatively small order. To inhibit such substitution, the base or generator of the cryptosystem is chosen to be a generator of a subgroup of prime order or a subgroup of an order having a number of relatively small divisors. The message may be exponentiated to each of the relatively small divisors and the result checked for the group identity. If the group identity is found, it indicates a vulnerability to substitution and is rejected.

145 Claims, 1 Drawing Sheet



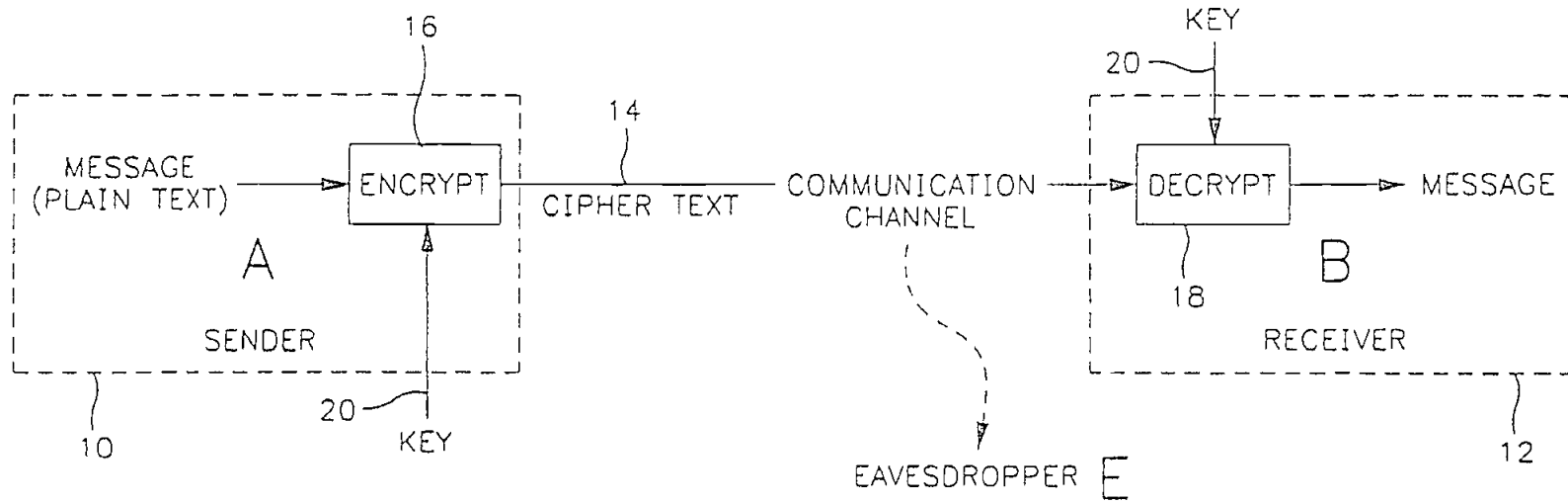


FIG. 1

STRENGTHENED PUBLIC KEY PROTOCOL

CROSS-REFERENCE TO RELATED APPLICATION

This application is a continuation of U.S. patent application Ser. No. 08/649,308 filed on May 17, 1996, now issued as U.S. Pat. No. 5,933,504.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to public key cryptography.

2. Discussion of Related Art

It is well known that data can be encrypted by utilizing a pair of keys, one of which is public and one of which is private. The keys are mathematically related such that data encrypted by the public key may only be decrypted by the private key. In this way, the public key of a recipient may be made available so that data intended for that recipient may be encrypted with the public key and only decrypted by the recipient's private key.

One well-known and accepted public key cryptosystem is that based upon discrete logarithms in finite groups. Different finite groups may be used, for example the multiplicative group Z_p^* of integers mod p where p is a prime; the multiplicative group of an arbitrary finite field e.g. $GF(2^n)$ or an elliptic curve group over a finite field.

The discrete log problem used in such cryptosystems is based on the difficulty of determining the value of an integer x from the value of α^x , even where α is known. More particularly, if α is an element of G (which is considered to be written multiplicatively) and β is a second element of G , then the discrete logarithm problem in G is that of determining whether there exists an integer x such that $\beta = \alpha^x$, and if so, of determining such a value x .

The Diffie-Hellman key exchange protocol is widely accepted and there are numerous examples of implementations of the Diffie-Hellman protocol in use around the world.

The Diffie-Hellman key agreement protocol is typically stated as follows using as an example the finite group Z_p^* :

Setup
The protocol requires a base α that generates a large number of elements of the selected group G and a pair of integers x, y that are retained confidentially by respective correspondents A, B. Select a prime number p and let α be a generator of the multiplicative group Z_p^* , i.e. the group of integers modulo p .

The Protocol

1. Correspondent A generates a random integer x , computes α^x and sends this to correspondent B.
2. Correspondent B generates a random integer y , computes α^y and sends this to correspondent A.
3. A computes $(\alpha^y)^x = \alpha^{xy}$.
4. B computes $(\alpha^x)^y = \alpha^{xy}$.

A and B now share the common key α^{xy} which may be used as a secret key in a conventional cryptosystem. A similar protocol may be used in a public key system, generally referred to as an El-Gamal protocol in which each correspondent has a secret key x and a public key α^x .

The security of these protocols seems to rest on the intractability of the discrete logarithm problem in the finite group G . It should also be noted that the protocol carries over to any finite group.

The applicants have now recognized that unless the generator α and the group G are selected carefully then the exchange of information may be weak and provide almost no security.

To explain the potential problem, consider the cryptosystem described above using the group Z_p^* . The modulus p is public information that defines the cryptosystem and can be expressed as $tQ+1$ with $t \geq 2$ and t relatively small. This is always possible since p is odd for large primes (i.e. t could be 2).

Let S be a subgroup of Z_p^* of order t (i.e. it has t elements, each of which is element of Z_p^*) and let γ be a base for S , i.e. each element of S can be expressed as an integral power of γ and raising γ to an integral power produces an element that is itself in the subgroup S . If α is a generator for Z_p^* , then we can take $\gamma = \alpha^Q$ without loss of generality.

If E is an active adversary in the key exchange protocol between two parties A and B then the attack proceeds as follows:

1. E intercepts the message α^x sent by A and replaces it by $(\alpha^x)^Q = \gamma^x$ and sends it on to entity B.
2. E intercepts the message α^y sent by B and replaces it by $(\alpha^y)^Q = \gamma^y$ and sends it on to entity B.
3. A computes $(\gamma^y)^x = \gamma^{xy}$.
4. B computes $(\gamma^x)^y = \gamma^{xy}$.
5. Although E does not know the key γ^{xy} , E knows that the common key γ^{xy} lies in the subgroup S of order t as γ is a generator of S . By definition γ^{xy} must produce an element in the subgroup S . Since S is of order t it has precisely t elements. If t is small enough then E can exhaustively check all possibilities and deduce the key. Since E selects Q , t can always be taken to be 2 and so the threat is practical.

A similar attack may be mounted with cryptosystems using groups other than Z_p^* which will be vulnerable if the element selected as a base or generator generates a subgroup which itself has a small subgroup of order t .

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide a method for checking if modification of messages has occurred or in the alternative some method to prevent the attack from being mounted.

In general terms, the present invention is based upon utilization of predefined characteristics of the order of the subgroup.

In one aspect, the base of the cryptosystem is chosen to be a generator of a subgroup of a relatively large prime order. Substitution of any other non-unit generator is of no advantage to an attacker since it does not produce an element in a smaller subgroup that can be exhaustively searched.

In another aspect, factors of the order of the group generated by the base are used to ensure that the key does not lie in or has not been modified to lie in a proper subgroup of relatively small order, i.e. one that may feasibly be exhaustively searched by an interloper.

BRIEF DESCRIPTION OF THE DRAWING

Embodiments of the invention will now be described by way of example only with reference to the accompanying drawings, in which

FIG. 1 is a schematic representation of a data communication system.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring therefore to FIG. 1, a pair of correspondents, 10, 12, denoted as correspondent A and correspondent B,

exchange information over a communication channel 14. A cryptographic unit 16,18, is interposed between each of the correspondents 10,12 and the channel 14. A key 20 is associated with each of the cryptographic units 16,18 to convert plain text carried between each unit 16,18 and its respective correspondent 10,12 into ciphertext carried on the channel 14.

In operation, a message generated by correspondent A, 10, is encrypted by the unit 16 with the key 20 and transmitted as ciphertext over channel 14 to the unit 18.

The key 20 operates upon the ciphertext in the unit 18 to generate a plaintext message for the correspondent B, 12. Provided the keys 20 correspond, the message received by the correspondent 12 will be that sent by the correspondent 10.

In order for the system shown in FIG. 1 to operate it is necessary for the keys 20 to be identical and therefore a key agreement protocol is established that allows the transfer of information in a public manner to establish the identical keys. A number of protocols are available for such key generation and most are variants of the Diffie-Hellman key exchange. Their purpose is for parties A and B to establish a secret session key K.

The system parameters for these protocols are a multiplicative group G and a generator a in the group G. Both G and a are known. Correspondent A has private key x and public key $p_A = a^x$. Correspondent B has private key y and public key $p_B = a^y$. Correspondent A and B exchange respective public keys and exponentiate with their private keys to obtain a common session key a^{xy} .

As noted above, the key exchange and therefore the ciphertext, is vulnerable if interloper E intercepts the transmission of a^x and a^y and raises each to the power Q.

In a first embodiment, the attack is foiled by defining the system parameters appropriately so that no advantage is provided to the interloper by performing a substitution. Moreover, the base or generator of the cryptosystem is selected so that tampering with the key exchange between A and B can be detected.

By way of example, for a public key system using the group Z_p , initially a subgroup S of Z_p^* is selected which has a prime order. The subgroup S of prime order q will only have subgroups of order 1 or the prime q itself. For example, if p is chosen as 139 then Z_{139}^* contains subgroups of order 1,2,3,6,23,46,69 and 138. Of these, the subgroups of order 2,3 and 23 are of prime order.

Accordingly, if the base used in the public key system is chosen to be a generator γ of a subgroup S of Z_p^* of prime order q rather than a generator x of Z_p^* itself, an attempt by the interloper to substitute a smaller subgroup may be readily detected.

For example, 34 is a generator of the subgroup of order 23 in Z_{139}^* . Therefore the base is chosen to be 34 for key exchange and generation.

The selection of the subgroup S of prime order q restricts the interloper E to an exponent of either 1 or the prime q, i.e. 23 in the example given. If the exponent is chosen to be the order q of the subgroup S then the message produced from the generator of the subgroup exponentiated to q will be the identity element, i.e. 1 in the example given. Therefore one or both correspondents may check the message and if it corresponds to the identity element it is rejected.

Selection by the interloper E of the exponent to be 1 will of course not be of use as the discrete log problem will still be intractable and provided the order of the subgroup is sufficiently large a brute force approach is impractical.

It will of course be understood that the example given of $p=139$ is for illustrative purposes only and that in practical implementations the prime p will be of the order of 10^{250} and the order of the subgroup will typically exceed 10^{10} .

In a second embodiment, the order of the subgroup need not be prime and the attack is foiled by monitoring the received message. The order of the subgroup may therefore have a number of small divisors, $1, t_1, t_2$ which are sufficiently small to render the exchange vulnerable. To foil such a substitution, at least one of the correspondents A,B takes the message received from the other correspondent, i.e. a^x for B or a^y for A and raises the message to the power t for each small divisor of $(p-1)$. If the result is 1 it indicates that a new value of the message may have been substituted, as $(a^x)^{t_1} \text{ mod } (p-1)$ will always be 1. The fact that the result is 1 is not determinative that a substitution has been made but the probability that $(a^x)^t = 1$ for large values of p is small. The key exchange can be terminated if the result is 1 and a new key exchange initiated. If with different values of private keys x and y successive key exchanges yield a result of 1 when tested above, then it is assumed that an interloper is actively monitoring the data exchange and further communication is terminated.

The determination of the value a^{xy} may be made by exponentiation of the message a^x with the possible values of t by an exhaustive search. Alternatively, given the order of the subgroup, values of the message that yield the group identity can be tabulated and a simple comparison made to determine if the message is vulnerable.

As a third embodiment, the value of p is selected to be of the form $2q+1$ where q is itself a prime. The only subgroups of Z_p^* have orders 1,2,q and 2q. The generator of the subgroup of order q is selected for the key exchange so that t can only be 1 or q. If the subgroup of order 1 is selected then the message $(a^x)^q$ will be the identity element, e.g. 1, and this can readily be checked. q will be selected to be relatively large to render an attack on the discrete log problem unfeasible.

The above techniques provide a clear indication of an attempt by an interloper to substitute a subgroup and a foil that is readily implemented by a careful selection of the generator and a check for the identity element.

The above examples have utilized the group Z_p but other groups may be used as noted above, for example, an elliptic curve group over a finite field. In the case of an elliptic curve over the field F_p elements where p is a prime power, there is an elliptic curve group G for each integral order lying between $p+1-2\sqrt{p}$ and $p+1+2\sqrt{p}$. With high probability, there is a prime q lying in this interval and by selecting this elliptic curve group, G_q , of order q for use in the cryptosystem, the group G_q will only have subgroups of order 1 and the prime q itself. Accordingly, selection of the group G_q will avoid substitution of subgroups of relatively small order and any attempt at substitution will not yield any benefits to the interloper.

A particularly convenient finite field is the field F_m which may be used for the generation of elliptic curve groups.

As an alternative approach to the selection of a group of prime order, the order of the elliptic curve may be chosen of order n, where n is not a prime and messages are monitored by at least one of the correspondents. The integrity of the message is verified by raising the message to the power d for each small divisor d of the order n. In this case, if the result is the group identity, typically 0, then it is assumed that a substitution has been made and the transmission is terminated.

Again, therefore, a group is selected that is either of prime order to inhibit substitution or a group is chosen to have an order with small divisors. In each case, substitution can be checked by monitoring the message by at least one of the correspondents.

Similar considerations will apply in other groups and careful selection of the order of the groups utilized will provide the benefits described above.

An alternative attack that may be utilized is for the interloper E to substitute a new message "e" for that transmitted from A to B and vice versa.

The new message e is chosen to be an element of a subgroup S of the group G of low order, i.e. a relatively small number of elements. When B receives the message e he exponentiates it with his secret key y to generate the session key. Similarly, when A receives the message e he exponentiates it with the secret key x to generate the session key.

Exponentiation of an element of a subgroup will produce an element within that group so that the session keys generated by A and B lie in the subgroup S. If S is of relatively low order, there is a reasonable chance that the keys generated by A and B will be identical. In that case a message encrypted with the session key may be intercepted and the small number of possibilities that exist for the key can be tried by E.

If the keys are not identical then the failure will be attributed to system errors and a new attempt will be made to establish a key. This provides E with a further opportunity to substitute a different element of the subfield S in the transmission with a real probability that a correspondence will be established. Because of the relatively small number of possible elements, the possibilities may be exhausted and a correspondence made within the normal operating parameters of the system.

To overcome this possibility, the order of the group is selected to have factors that are either large primes or provide trivial solutions that disclose themselves upon simple examination. In the case of the group Z_p^* , a suitable form is for the value of the modulus p to be of the form $2qq'+1$ where q and q' are both large primes. The subgroups S of Z_p^* will be of order 2, q or q'. Adopting a subgroup of order 2 will provide only two possible elements which can readily be checked and, if present as the session key, the session can be terminated.

The values of q and q' will not be readily ascertained due to the difficulty of factoring the products of large primes.

Even if an exhaustive attack on the subgroup of order q or q' is viable for E, such an attack will reveal itself by a large number of repeated attempts at establishing communication. Accordingly, an upper limit may be established after which communication will be terminated. The appropriate number of attempts will be based on the factors of p-1 and the nature of the communication system.

Again, therefore, the attacks by E can be resisted by checking for values of the session key that are indicative of the vulnerability of the session and by appropriate selection of the order of the group. It will be recognised that selection of the modulus of the form $2q+1$ as exemplified in the third embodiment above provides the requisite robustness for resisting a substitution attack by E.

These techniques are also effective to prevent interloper E from taking a known public key α^a , raising it to an appropriate power such that α^{aQ} is in a small subgroup. The interloper can then determine aQ, and use this as his private

key. There are situations where the interloper can use this to impersonate correspondent A and also convince a certifying authority to certify the public key α^{aQ} since the interloper E can prove he knows aQ.

In the above examples, the checking for elements lying in subgroups of relatively small order has been performed by exponentiating the message to the power of the small divisors of the order of the group. An alternative method which will indicate whether or not the message lies in a proper subgroup, without necessarily identifying the order of the subgroup, is to exponentiate the message to the order n/p where n is the order of the group G and p ranges over all prime divisors of n. If the result is the group identity (1 in the case of Z_p^*) then it indicates that the message does lie in a subgroup. Depending upon the strategy used to determine the order of the group G, it is possible either to reject the message or to test further to determine the order of the subgroup.

What is claimed is:

1. A method of determining the integrity of a message exchanged between a pair of correspondents, said message being secured by embodying said message in a function of α^x where α is an element of a finite group S of order q, said method comprising the steps of at least one of the correspondents receiving public information α^x where x is an integer selected by another of said correspondents, determining whether said public information α^x lies within a subgroup of S having less than a predetermined number of elements and rejecting messages utilizing said public information if said public information lies within such a subgroup.

2. A method according to claim 1 wherein said order q is a prime number.

3. A method according to claim 2 wherein said message is a component of a session key α^{xy} where y is an integer selected by said one correspondent.

4. A method according to claim 1 wherein said group is a multiplicative group Z_p^* of integers mod p where p is a prime.

5. A method according to claim 4 wherein said modulus p is of the form $2r+1$ and r is a prime.

6. A method according to claim 4 wherein said modulus p is of the form $nr'+1$ and r and r' are relatively large primes.

7. A method according to claim 4 wherein said message is examined by operating upon said public information by a value t where t is a divisor of q and determining whether the resultant value corresponds to the group identity.

8. A method according to claim 4 wherein said group S is a subgroup of a group G of order n.

9. A method according to claim 4 wherein said message is a component of a session key α^{xy} where y is an integer selected by said one correspondent.

10. A method according to claim 9 wherein said message is examined by operating upon said public information by a value t where t is a divisor of q and determining whether the resultant value corresponds to the group identity.

11. A method according to claim 4 wherein said modulus p is of the form $2r'+1$ and r and r' are prime.

12. A method according to claim 4 wherein said group G is an elliptical curve group over a finite field F_{2^m} .

13. A method according to claim 12 wherein said message is examined by operating upon said public information by a value t where t is a divisor of n and determining whether the resultant value corresponds to the group identity.

14. A method according to claim 13 wherein said message is a component of a session key α^{xy} where y is an integer selected by said one correspondent.

15. A method according to claim 14 wherein said message is examined by operating upon said public information by a value t where t is a divisor of n and determining whether the resultant value corresponds to the group identity.

16. A method according to claim 1 wherein said group is a multiplicative group of a finite field.

17. A method according to claim 1 wherein said group is an elliptical curve group over a finite field.

18. A method according to claim 17 wherein said group S is a subgroup of a group G of order n .

19. A method according to claim 17 wherein said message is a component of a session key α^y where y is an integer selected by said one correspondent.

20. A method according to claim 1 wherein said group is over a finite field F_{2^n} .

21. A method according to claim 20 wherein said group is an elliptic curve group.

22. A method according to claim 21 wherein said message is examined by operating upon said public information by a value t where t is a divisor of q and determining whether the resultant value corresponds to the group identity.

23. A method according to claim 21 wherein said message is a component of a session key α^y where y is an integer selected by said one correspondent.

24. A method according to claim 23 wherein said message is examined by operating upon said public information by a value t where t is a divisor of q and determining whether the resultant value corresponds to the group identity.

25. A method according to claim 19 wherein said message is examined by operating upon said public information by a value t where t is a divisor of q and determining whether the resultant value corresponds to the group identity.

26. A method according to claim 1 wherein said message is a component of a session key α^y where y is an integer selected by said one correspondent.

27. A method according to claim 26 wherein said message is examined by operating upon said public information by a value t where t is a divisor of q and determining whether the resultant value corresponds to the group identity.

28. A method according to claim 1 wherein said message is examined by operating upon said public information by a value t where t is a divisor of q and determining whether the resultant value corresponds to the group identity.

29. A method according to claim 28 wherein a plurality of values of t are utilized and each resultant value compared to the group identity.

30. A method according to claim 1 wherein said determination includes the step of operating on said message by an operator q/p where q is the order of the group S and p ranges over all prime divisors of q .

31. A method according to claim 1 wherein said group is over a finite field.

32. A method of determining the integrity of a message exchanged between a pair of correspondents, said message being secured by embodying said message in a function of α^x where α is an element of a finite group S of order q and said group S is a subgroup of a finite group G of order n , said method comprising the steps of at least one of the correspondents receiving public information α^x where x is an integer selected by another of said correspondents, determining whether said public information α^x lies within a subgroup S of G having less than a predetermined number of elements and rejecting messages utilizing said public information if said public information lies within such a subgroup.

33. A method according to claim 32 wherein q is a prime number.

34. A method according to claim 33 wherein said determination is made by operating on said message by an operator n/p where p ranges over all prime divisors of n .

35. A method according to claim 34 wherein said operation includes exponentiation of said message and said determination is made by examination for a group identity.

36. A method according to claim 33 wherein said message is examined by operating upon said public information by a value t where t is a divisor of n and determining whether the resultant value corresponds to the group identity.

37. A method according to claim 33 wherein said message is a component of a session key α^y where y is an integer selected by said one correspondent.

38. A method according to claim 37 wherein said message is a component of a session key α^y where y is an integer selected by said one correspondent.

39. A method according to claim 33 wherein said group G is a multiplicative group of a finite field.

40. A method according to claim 33 wherein said group G is a multiplicative group Z_p^* of integers mod p where p is a prime.

41. A method according to claim 40 wherein said message is examined by operating upon said public information by a value t where t is a divisor of n and determining whether the resultant value corresponds to the group identity.

42. A method according to claim 40 wherein said message is a component of a session key α^y where y is an integer selected by said one correspondent.

43. A method according to claim 42 wherein said message is examined by operating upon said public information by a value t where t is a divisor of n and determining whether the resultant value corresponds to the group identity.

44. A method according to claim 40 wherein said modulus p is of the form $2r+1$ and r is a prime.

45. A method according to claim 33 wherein said group G is an elliptical curve group over a finite field.

46. A method according to claim 45 wherein said message is examined by operating upon said public information by a value t where t is a divisor of n and determining whether the resultant value corresponds to the group identity.

47. A method according to claim 45 wherein said message is examined by operating upon said public information by a value t where t is a divisor of n and determining whether the resultant value corresponds to the group identity.

48. A method according to claim 33 wherein said group G is an elliptical curve group over a finite field F_{2^n} .

49. A method according to claim 48 wherein said message is examined by operating upon said public information by a value t where t is a divisor of n and determining whether the resultant value corresponds to the group identity.

50. A method according to claim 48 wherein said message is a component of a session key α^y where y is an integer selected by said one correspondent.

51. A method according to claim 48 wherein said message is examined by operating upon said public information by a value t where t is a divisor of n and determining whether the resultant value corresponds to the group identity.

52. A method according to claim 33 wherein said group is over a finite field.

53. A method of establishing a session key for encryption of data between a pair of correspondents comprising the steps of one of said correspondents selecting a finite group G , establishing a subgroup S having an order q of the group G , determining an element α of the subgroup S to generate greater than a predetermined number of the q elements of the subgroup S and utilizing said element α to generate a session key at said one correspondent.

54. A method according to claim 53 wherein said order q of said subgroup S is a prime.

55. A method according to claim 53 including the step of receiving at one of said correspondents a message α^x , where x is an integer selected by an other of said correspondents, exponentiating said message α^x to a value t where t is a divisor of the order of the subgroup, comparing a resultant value α^{xt} to the group identity and preventing establishment of said session key if said value corresponds to the group identity.

56. A method according to claim 55 wherein a plurality of values of t are utilized and each resultant value compared to the group identity.

57. A method according to claim 55 wherein said message is examined by operating upon said public information by a value t where t is a divisor of q and determining whether the resultant value corresponds to the group identity.

58. A method according to claim 53 wherein said order of said subgroup is of the form utilizing an integral number of a product of a plurality of large primes.

59. A method according to claim 58 wherein the order of said subgroup is of the form nrr' where n , r and r' are each integers and r and r' are each prime numbers.

60. A method according to claim 59 wherein n has a value of 2.

61. A method according to claim 53 wherein said subgroup is selected to have an order that is to be a function of the product of a pair of primes r, r' and said element α is a generator of a subgroup of an order of one of said primes r, r' .

62. A method according to claim 53 including the step of determining whether information received by one of the correspondents sharing said session key lies within a subgroup of S having less than a predetermined number of elements and rejecting said information if it lies within such a subgroup.

63. A method according to claim 53 wherein said group is an elliptical curve group G over a finite field.

64. A method according to claim 63 wherein said elliptic curve group is over the finite field F_p where p is a prime power.

65. A method according to claim 53 wherein said group is over a finite field F_{2^n} .

66. A method according to claim 65 wherein said group is an elliptic curve group.

67. A method according to claim 66 wherein the order q of said subgroup S is prime.

68. A method of establishing a session key of the form α^{xy} for encryption of data between a pair of correspondents having respective private keys x , and y comprising the steps of selecting an elliptic curve over a field of prime order p having p elements, said elliptic curve having a prime order q , to provide q points on the curve, determining an element α of a group G comprising said q points to generate the q elements of the group G and utilizing said element α to generate a session key of the form α^{xy} at each correspondent where x is an integer selected by one of the correspondents and y is an integer selected by another of said correspondents, whereby the order of the curve q is selected such that the intractability of the discrete log problem inhibits recovery of the private keys x or y .

69. A method according to claim 68 including the step of one of said correspondents determining the number of elements of the group G and terminating establishment of said session key if said number is less than a predetermined number of elements.

70. A method according to claim 68 including the step of one of said correspondents determining if the information received from the other correspondent corresponds to the group identity.

71. A method according to claim 68 including the step of checking that said order q is prime.

72. A method according to claim 71 wherein said order q is greater than 10^{10} .

73. A method of establishing by way of a discrete log key agreement scheme a session key for encryption of data between a pair of correspondents comprising the steps of selecting a finite group G , establishing a subgroup S having an order q of the group G , determining an element α of the subgroup S to generate greater than a predetermined number of the q elements of the subgroup S and utilizing said element α to generate a session key at each correspondent.

74. A method according to claim 73 wherein each of said correspondents have respective private keys x and y and said session key is of the form α^{xy} .

75. A method according to claim 74 wherein said subgroup S is of prime order.

76. A method according to claim 75 wherein at least one of said correspondents ascertains whether information received from said other correspondent corresponds to the group identity.

77. A method according to claim 74 wherein said group G is an elliptic curve group.

78. A method of establishing a session key for encryption of data between a pair of correspondents comprising the steps of selecting a finite field of order n , establishing a subgroup S having an order q of the multiplicative group of the finite field, determining an element α of the subgroup S to generate greater than a predetermined number of the q elements of the subgroup S and utilizing said element α to generate a session key at each correspondent.

79. A method according to claim 78 wherein said order q of said subgroup S is a prime.

80. A method according to claim 78 wherein said order n is a prime of the form $2q+1$ and q is prime.

81. A method according to claim 78 wherein said order n is a prime of the form $rq+1$ and r is small and q is prime.

82. A method according to claim 78 wherein said order n is a prime of the form $2qq'+1$ and q and q' are prime.

83. A method according to claim 78 wherein said order n is a prime of the form $rqq'+1$ and r is small, and q and q' are prime.

84. A method according to claim 78 wherein said order n is a prime of the form $2qq'+1$ and q is prime and q' is the product of a plurality of large primes.

85. A method according to claim 78 wherein said order n is a prime of the form $rqq'+1$ where r is small, q is prime, and q' is the product of a plurality of large primes.

86. A method of establishing a session key for encryption of data between a pair of correspondents comprising the steps of selecting an elliptic curve group of order n over a finite field, establishing a subgroup S having an order q of the elliptic curve group, determining an element α of the subgroup S to generate greater than a predetermined number of the q elements of the subgroup S and utilizing said element α to generate a session key at each correspondent.

87. A method according to claim 86 wherein said order q of said subgroup S is a prime.

88. A method according to claim 86 wherein said finite field is a finite field F_p .

89. A method according to claim 88 wherein said order q of said subgroup S is a prime.

90. A method according to claim 86 wherein said finite field is a finite field F_{2^n} .

91. A method according to claim 90 wherein said order q of said subgroup S is a prime.

92. A method of establishing a session key for encryption of data between a pair of correspondents comprising the

steps of selecting a group of order n over a finite field, establishing a subgroup S having an order q of said group, determining an element α of the subgroup S to generate greater than a predetermined number of the q elements of the subgroup S and utilising said element α to generate a session key at each correspondent.

93. A method according to claim 51 wherein said order q of said subgroup S is a prime.

94. A method of establishing by way of a discrete log key agreement scheme a session key for encryption of data between a pair of correspondents comprising the steps of selecting a finite field of order n , establishing a subgroup S having an order q of the group G , determining an element α of the subgroup S to generate greater than a predetermined number of the q elements of the subgroup S and utilising said element α to generate a session key at each correspondent.

95. A method according to claim 94 wherein said order q of said subgroup S is a prime.

96. A method according to claim 94 wherein said order q of said subgroup S is a prime.

97. A method according to claim 94 wherein said order n is a prime of the form $2q+1$ and q is prime.

98. A method according to claim 94 wherein said order n is a prime of the form $rq+1$ and r is small and q is prime.

99. A method according to claim 94 wherein said order n is a prime of the form $2qq'+1$ and q and q' are prime.

100. A method according to claim 94 wherein said order n is a prime of the form $rqq'+1$ and r is small, and q and q' are prime.

101. A method according to claim 94 wherein said order n is a prime of the form $2qq'+1$ and q is prime and q' is the product of a plurality of large primes.

102. A method according to claim 94 wherein said order n is a prime of the form $rqq'+1$ where r is small, q is prime, and q' is the product of a plurality of large primes.

103. A method of establishing by way of a discrete log key agreement scheme a session key for encryption of data between a pair of correspondents comprising the steps of selecting an elliptic curve group of order n over a finite field, establishing a subgroup S having an order q of the elliptic curve group, determining an element α of the subgroup S to generate greater than a predetermined number of the q elements of the subgroup S and utilising said element α to generate a session key at each correspondent.

104. A method according to claim 103 wherein said order q of said subgroup S is a prime.

105. A method according to claim 103 wherein said finite field is a finite field F_p .

106. A method according to claim 105 wherein said order q of said subgroup S is a prime.

107. A method according to claim 103 wherein said finite field is a finite field F_{2^m} .

108. A method according to claim 107 wherein said order q of said subgroup S is a prime.

109. A method of establishing a session key of the form α^x for encryption of data between a pair of correspondents having respective private keys x and y comprising the steps of selecting an elliptic curve group of order n over a finite field, establishing a subgroup S having an order q of the elliptic curve group, determining an element α of the group G to generate the q elements of the group G and utilising said element α to generate a session key of the form α^x at each correspondent where x is an integer selected by one of said correspondents and y is an integer selected by another of said correspondents.

110. A method according to claim 109 wherein said finite field is a finite field F_p .

111. A method according to claim 110 wherein said order q of said subgroup S is a prime.

112. A method according to claim 109 wherein said finite field is a finite field F_{2^m} .

113. A method according to claim 112 wherein said order q of said subgroup S is a prime.

114. A method of establishing by way of a discrete log key agreement scheme a session key for encryption of data between a pair of correspondents comprising the steps of selecting an elliptic curve over a field of prime order p having p elements, said elliptic curve having a prime order q to provide q points on the curve greater than a predetermined number of points sufficient to avoid vulnerability in a cryptographic system, determining an element α of the group G to generate the q elements of the group G , and utilising said element α to generate a session key at each correspondent.

115. A method according to claim 114 including the step of checking that said order q is prime.

116. A method according to claim 114 wherein said order q is greater than 10^{10} .

117. A method of establishing by way of a discrete log key agreement scheme a session key for encryption of data between a pair of correspondents comprising the steps of selecting a group G of prime order q over a finite field, determining an element α of the group G to generate the q elements of the group G , and utilising said element α to generate a session key at each correspondent.

118. A method according to claim 117 including the step of checking that said order q is prime.

119. A method of establishing a session key of the form α^x for encryption of data between a pair of correspondents having respective private keys x and y comprising the steps of selecting a group G of prime order q over a finite field, determining an element α of the group G to generate the q elements of the group G and utilising said element α to generate a session key of the form α^x at each correspondent where x is an integer selected by one of said correspondents and y is an integer selected by another of said correspondents.

120. A method according to claim 119 including the step of checking that said order q is prime.

121. A method according to claim 119 wherein said order q is greater than 10^{10} .

122. A discrete log based key agreement system to permit a message to be exchanged between a pair of correspondents in a data communication system, said system utilising a group G of order n and having a generator and wherein said message is secured by embodying said message in a function of x where x is an integer, said system having a predefined parameter of a finite group S of order q , which is a subgroup of the group G and itself has no sub groups with less than a predetermined number of elements sufficient to avoid vulnerability in a cryptographic system.

123. A system according to claim 122 wherein at least one of said correspondents includes a monitor to determine whether said message corresponds to a group identity.

124. A cryptographic unit for use in a data communication system established between a pair of correspondents exchanging public information across a communication channel by way of a public key encryption scheme operating in a finite group G , said unit including a monitor to receive public information from one of said correspondents and examine said public information to determine whether it lies within a subgroup S of group G having less than a predetermined number of elements.

125. A method according to claim 32 wherein said determination is made by operating on said message by an operator n/p where p ranges over all prime divisors of n .

126. A method according to claim 125 wherein said operation includes exponentiation of said message and said determination is made by examination for a group identity.

127. A method according to claim 32 wherein said message is examined by operating upon said public information by a value t where t is a divisor of n and determining whether the resultant value corresponds to the group identity.

128. A method according to claim 32 wherein said message is a component of a session key α^y where y is an integer selected by said one correspondent.

129. A method according to claim 128 wherein said message is examined by operating upon said public information by a value t where t is a divisor of q and determining whether the resultant value corresponds to the group identity.

130. A method according to claim 129 wherein said message is examined by operating upon said public information by a value t where t is a divisor of q and determining whether the resultant value corresponds to the group identity.

131. A method according to claim 32 wherein said message is a component of a session key α^y where y is an integer selected by said one correspondent.

132. A method according to claim 131 wherein said message is examined by operating upon said public information by a value t where t is a divisor of n and determining whether the resultant value corresponds to the group identity.

133. A method according to claim 132 wherein said message is examined by operating upon said public information by a value t where t is a divisor of n and determining whether the resultant value corresponds to the group identity.

134. A method according to claim 32 wherein said group G is a multiplicative group of a finite field.

135. A method according to claim 32 wherein said group G is a multiplicative group Z_p of integers mod p where p is a prime.

136. A method according to claim 135 wherein said message is examined by operating upon said public information by a value t where t is a divisor of n and determining whether the resultant value corresponds to the group identity.

137. A method according to claim 135 wherein said message is a component of a session key α^y where y is an integer selected by said one correspondent.

138. A method according to claim 137 wherein said message is examined by operating upon said public information by a value t where t is a divisor of n and determining whether the resultant value corresponds to the group identity.

139. A method according to claim 135 wherein said modulus p is of the form $2r+1$ and r is a prime.

140. A method according to claim 32 wherein said group G is an elliptical curve group over a finite field.

141. A method according to claim 140 wherein said message is examined by operating upon said public information by a value t where t is a divisor of n and determining whether the resultant value corresponds to the group identity.

142. A method according to claim 140 wherein said message is a component of a session key α^y where y is an integer selected by said one correspondent.

143. A method according to claim 11 wherein said message is examined by operating upon said public information by a value t where t is a divisor of n and determining whether the resultant value corresponds to the group identity.

144. A method according to claim 32 wherein said group is over a finite field.

145. A method according to claim 17 wherein said message is examined by operating upon said public information by a value t where t is a divisor of q and determining whether the resultant value corresponds to the group identity.

* * * * *

EXHIBIT B

(12) **United States Patent**
Vanstone et al.

(10) **Patent No.:** **US 6,704,870 B2**
(45) **Date of Patent:** **Mar. 9, 2004**

(54) **DIGITAL SIGNATURES ON A SMARTCARD**

(75) **Inventors:** Scott A. Vanstone, Campbellville (CA);
 Alfred J. Menezes, Toronto (CA)

(73) **Assignee:** Certicom Corp., Mississauga (CA)

(*) **Notice:** Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 290 days.

(21) **Appl. No.:** 09/942,492

(22) **Filed:** Aug. 29, 2001

(65) **Prior Publication Data**
 US 2002/0095583 A1 Jul. 18, 2002

Related U.S. Application Data

(63) Continuation of application No. 09/434,247, filed on Nov. 5, 1999, which is a continuation-in-part of application No. 08/632,845, filed on Apr. 16, 1996, new Pat. No. 5,999,626.

(51) **Int. Cl.⁷** G06F 1/24

(52) **U.S. Cl.** 713/180; 713/200; 713/201;
 380/285; 380/30; 380/44

(58) **Field of Search** 713/180, 200,
 713/201; 380/285, 44, 30

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,146,500 A	9/1992	Mawer
5,159,632 A	10/1992	Crandall
5,271,061 A	12/1993	Crandall
5,272,755 A	12/1993	Miyaji et al.
5,351,297 A	9/1994	Miyaji et al.
5,442,707 A	8/1995	Miyaji et al.
5,463,690 A	10/1995	Crandall
5,497,423 A	3/1996	Miyaji

OTHER PUBLICATIONS

Kranakis, Evangelos, "Primality and Cryptography"; (John Wiley & Sons; New York; 1986); pp. 98-99.

Kranakis, Evangelos, "Theoretical Aspects of the Security of Public Key Cryptography"; (Yale University; New Haven; Sep. 1984); p. 105.

Luby, Michael, "Pseudorandomness and Cryptographic Applications"; (Princeton University Press; Princeton; 1996); p. 51.

Nissan, Noam, "Using Hard Problems to Create Pseudorandom Generators"; (published as "An ACM Distinguished Dissertation (1990)" in 1992); pp. 3-4.

Schneier, Bruce, "Applied Cryptography"; (John Wiley & Sons; New York; 1994); pp. 39-41.

Menezes, Alfred, "Elliptic Curve Public Key Cryptosystems"; (Kluwer Academic Publishers; Boston; 1993); pp. 10-13.

Menezes, Alfred, et al., "Journal of Cryptography"; (vol. 6, No. 4, Autumn 1993); pp. 209-223.

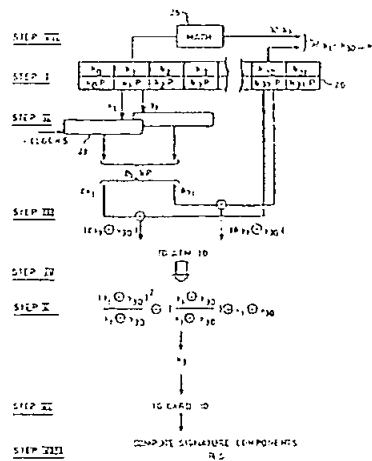
"Communications of the ACM"; (vol. 35, No. 7, Jul. 1992); pp. 33-34, 36-54.

Primary Examiner—Thomas R. Peeso
(74) Attorney, Agent, or Firm—The Maxham Firm

(57) **ABSTRACT**

A digital signature scheme for a "smart" card utilizes a set of prestored signing elements and combines pairs of the elements to produce a new session pair. The combination of the elements is performed partly on the card and partly on the associated transaction device so that the exchange of information between card and device does not disclose the identity of the signing elements. The signing elements are selected in a deterministic but unpredictable manner so that each pair of elements is used once. Further signing pairs are generated by implementing the signing over an anomalous elliptic curve encryption scheme and applying a Frobenius Operator to the normal basis representation of one of the elements.

25 Claims, 7 Drawing Sheets



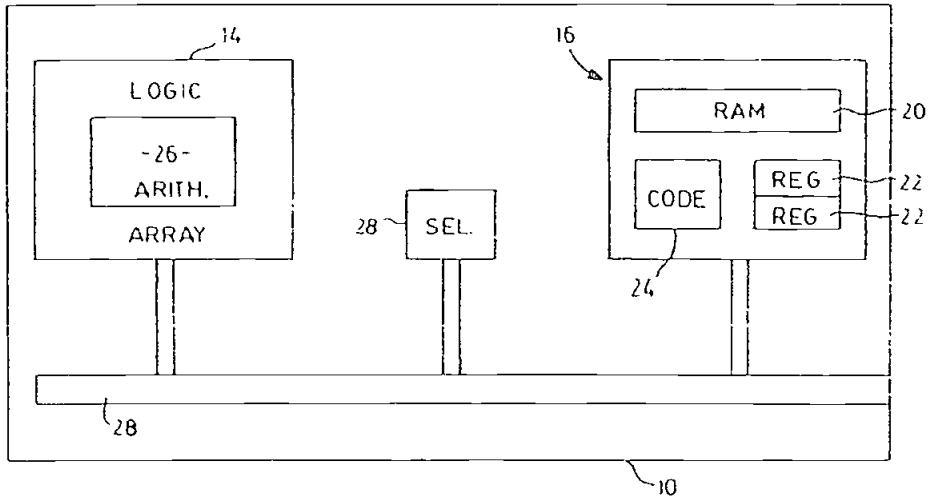


FIG. 1

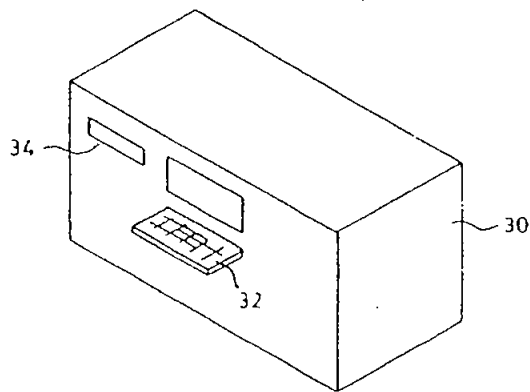


FIG. 2

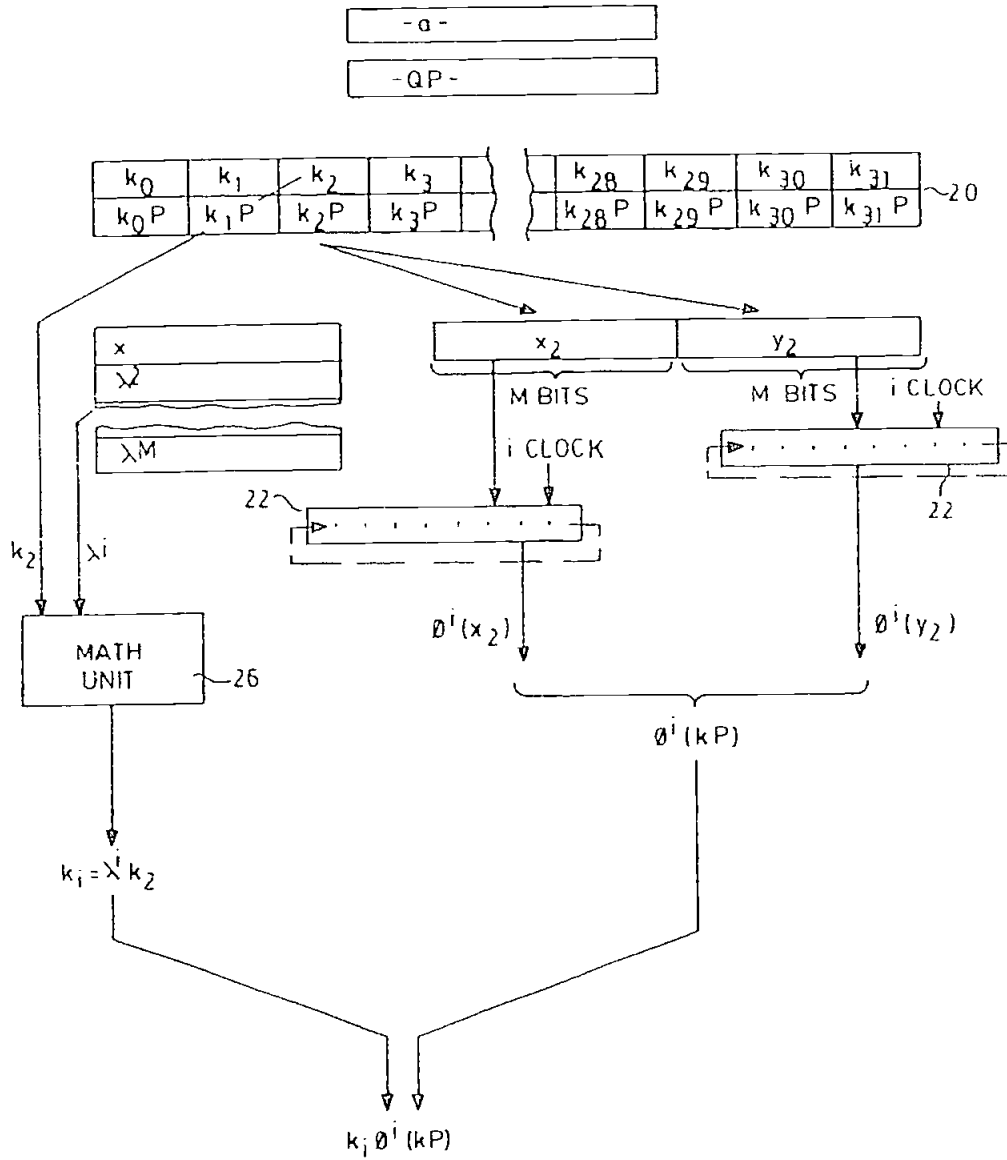


FIG. 3

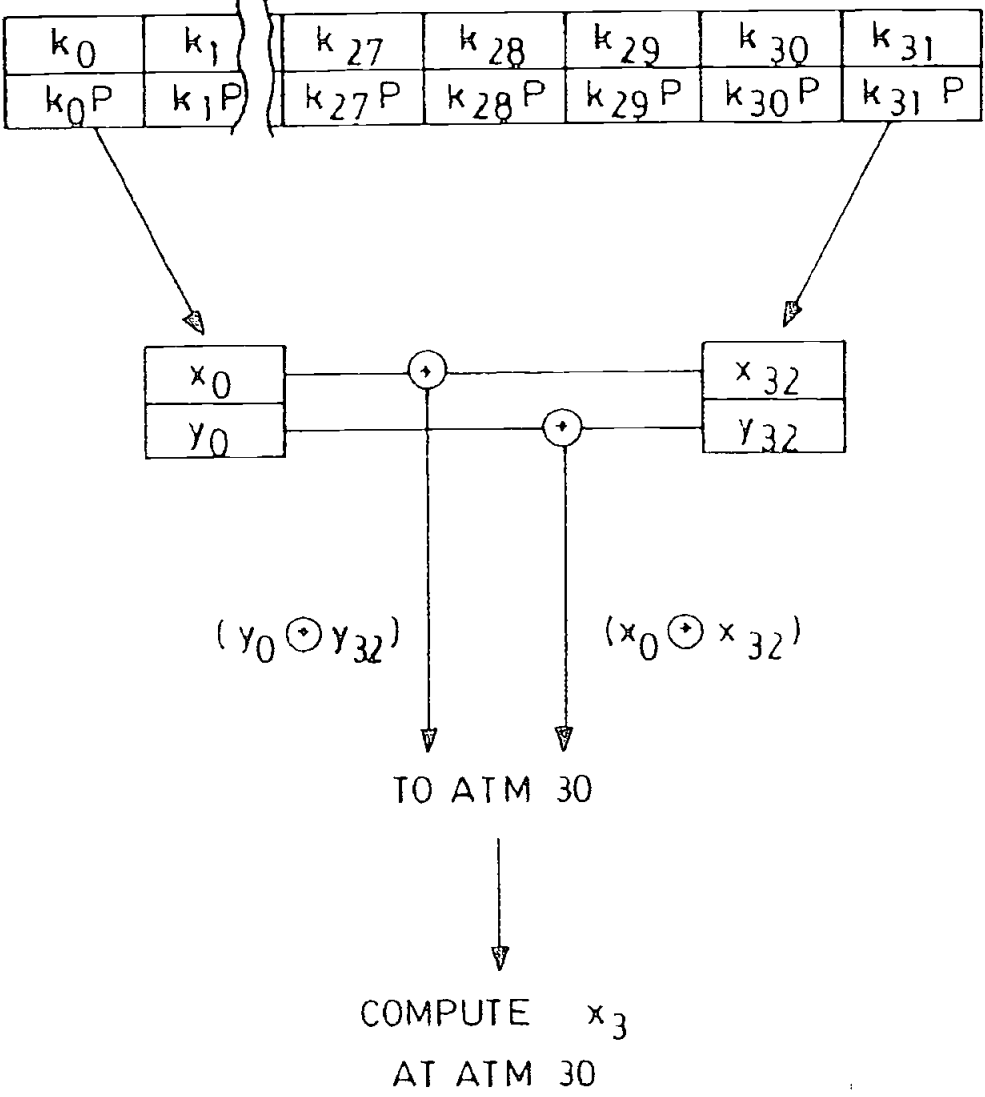


FIG. 4

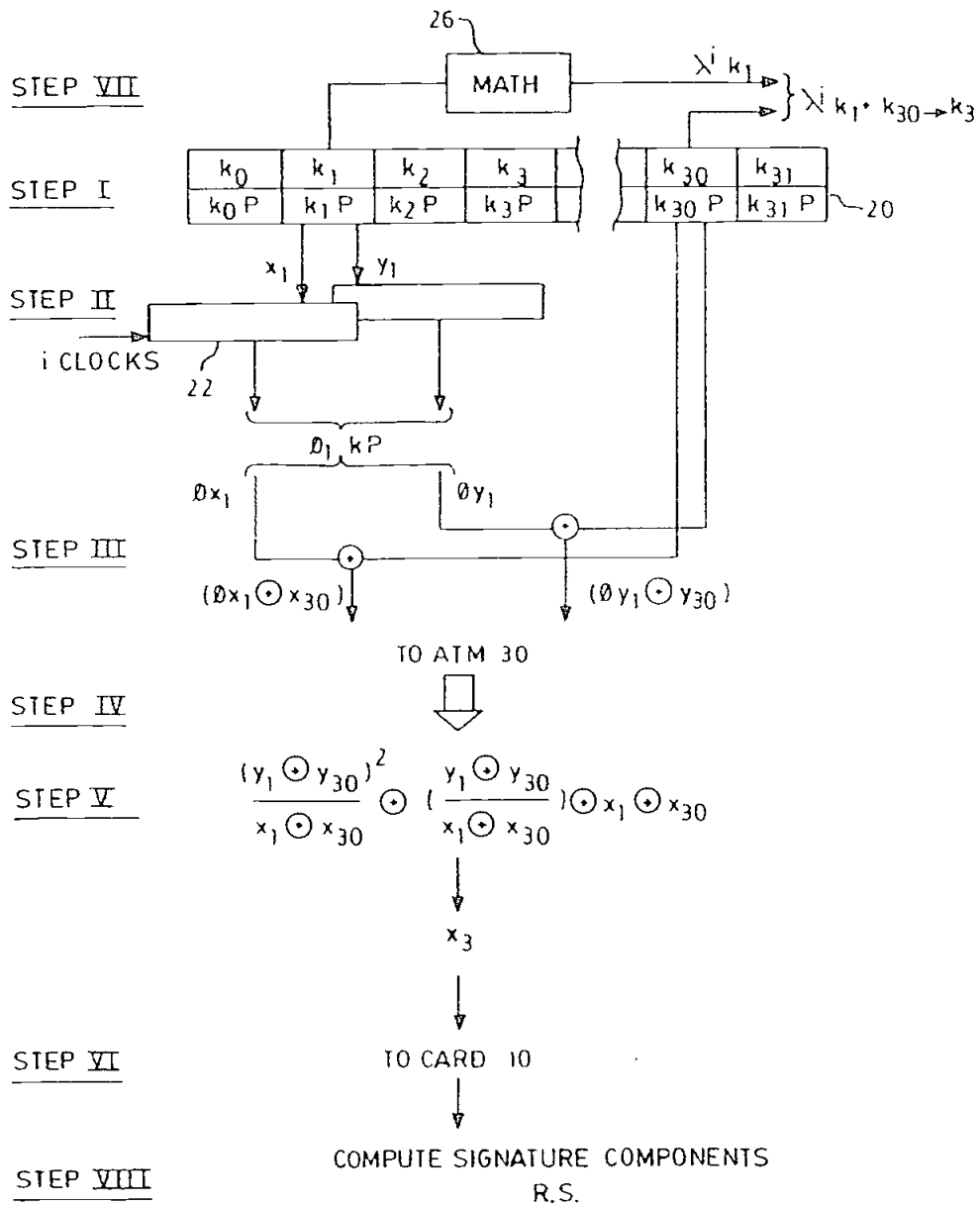


FIG. 5

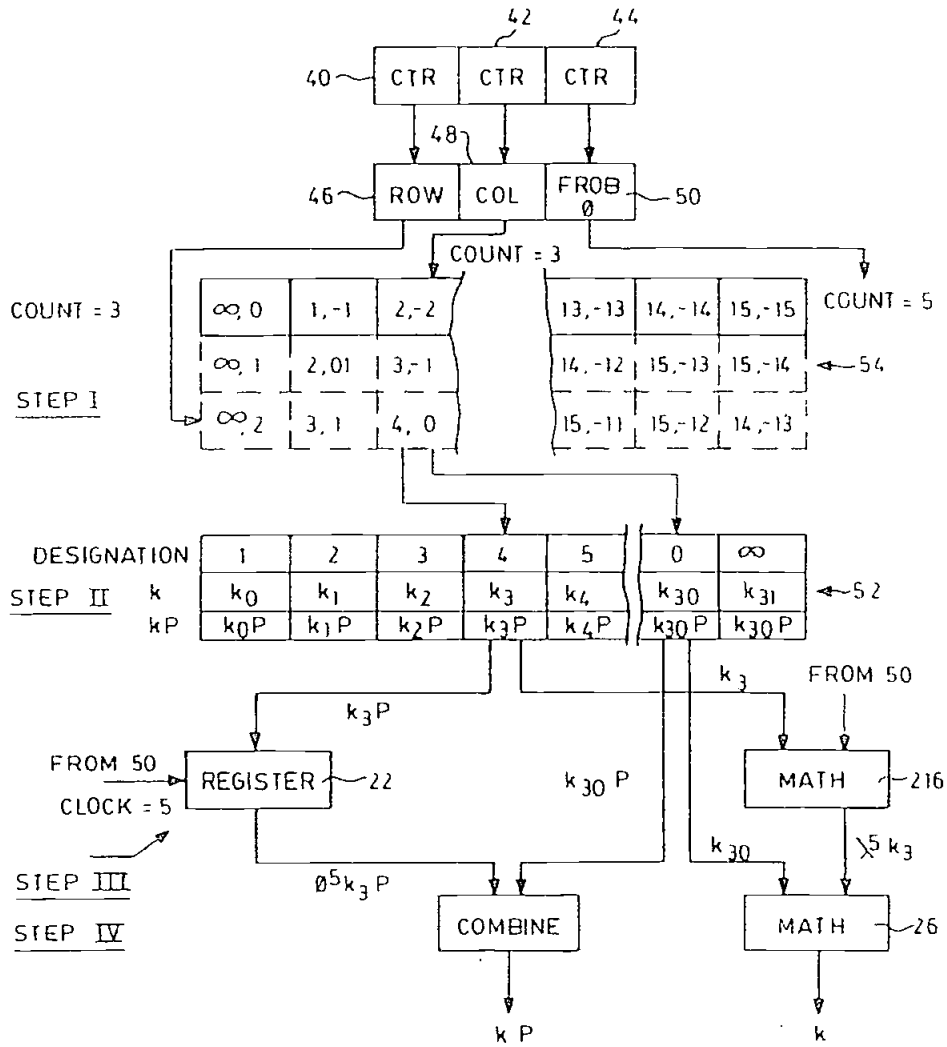
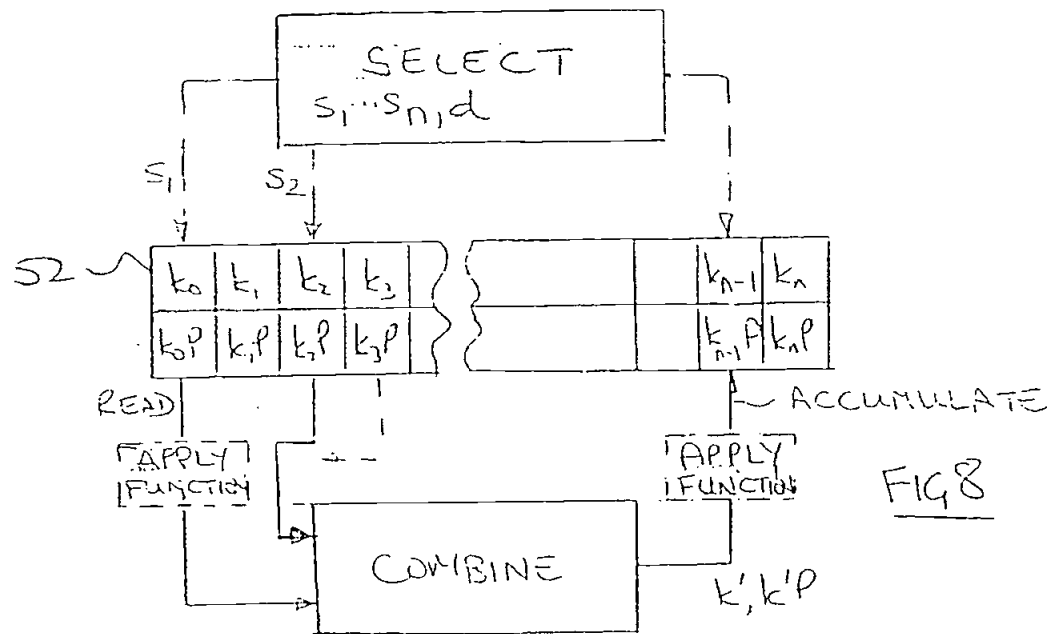
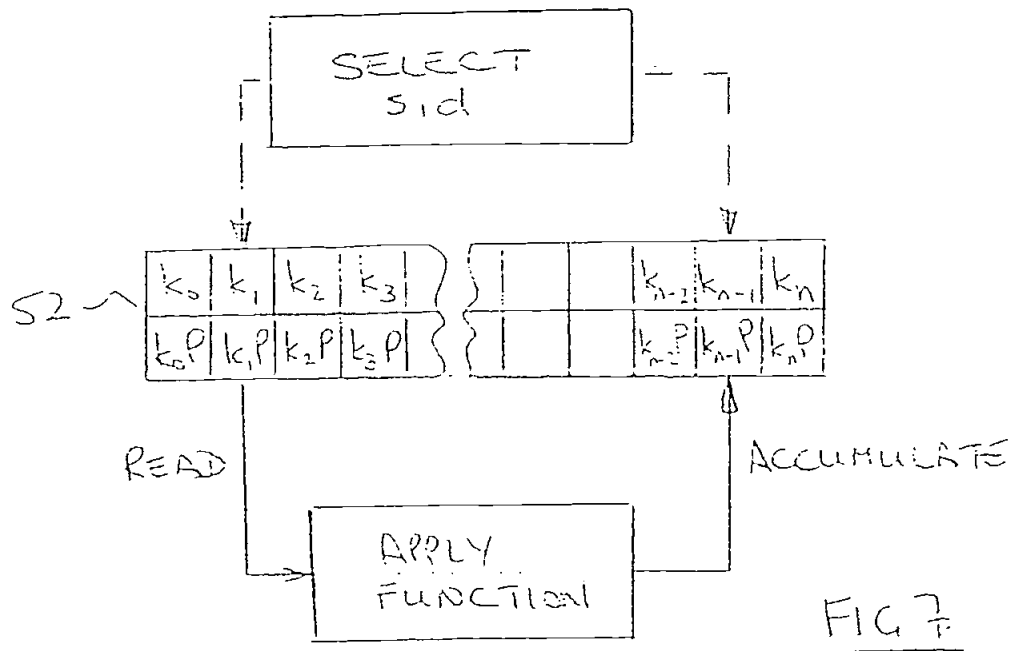


FIG. 6



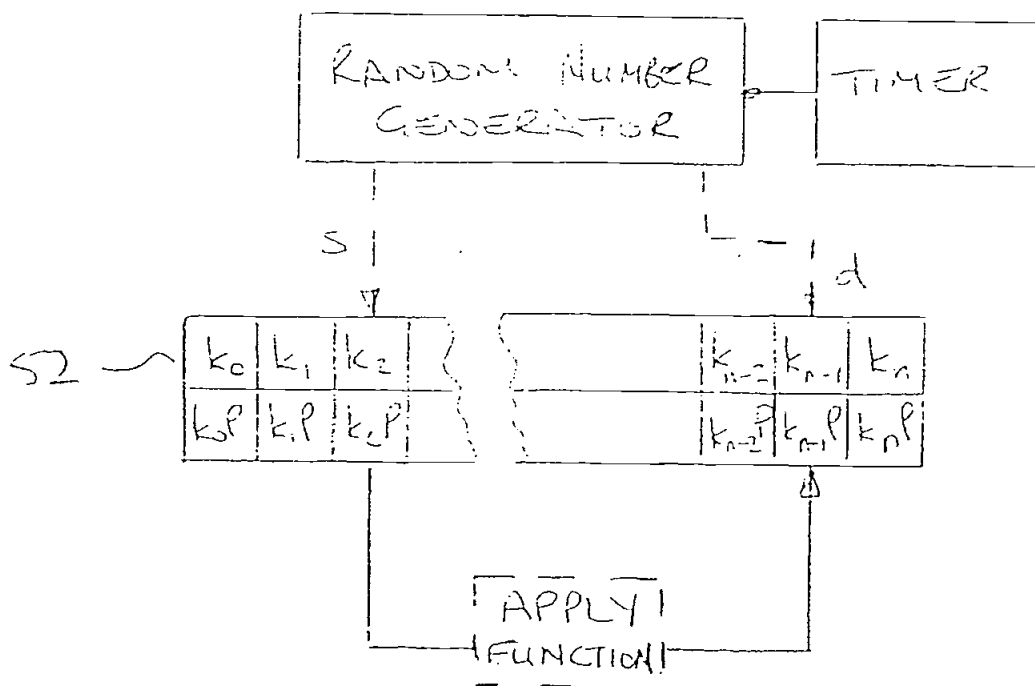


FIG 9

DIGITAL SIGNATURES ON A SMARTCARD

This application is a continuation of U.S. continuation-in-part application Ser. No. 09/434,247 and claims priority from U.S. application Ser. No. 08/632,845, now U.S. Pat. No. 5,999,626.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to methods and apparatus for generating digital signatures.

2. Discussion of Related Art

It has become widely accepted to conduct transactions, such as financial transactions or exchange of documents, electronically. In order to verify the transaction, it is also well known to "sign" the transaction digitally so that the authenticity of the transaction can be verified. The signature is performed according to a protocol that utilizes the message, i.e. the transaction, and a secret key associated with the party. The recipient can verify the signature using a public key of the signing party to recover the message and compare it with the transmitted message. Any attempt to tamper with the message or to use a key other than that of the signing party will result in an incompatibility between the sent message and that recovered from the signature or will fail to identify the party correctly and thereby lead to rejection of the transaction.

The signature must be performed such that the signing party's secret key cannot be determined. To avoid the complexity of distributing secret keys, it is convenient to utilize a public key encryption scheme in the generation of the signature. Such capabilities are available where the transaction is conducted between parties having access to relatively large computing resources but it is equally important to facilitate such transactions at an individual level where more limited computing resources are available.

Automated teller machines (ATMs) and credit cards are widely used for personal transactions and as their use expands, so the need to verify such transactions increases. Transaction cards, i.e. credit/debit cards or pass cards are now available with limited computing capacity (so-called "Smart Cards") but these do not have sufficient computing capacity to implement existing digital signature protocols in a commercially viable manner.

As noted above, in order to generate a digital signature, it is necessary to utilize a public key encryption scheme. Most public key schemes are based on the Diffie Helman Public key protocol and a particularly popular implementation is that known as DSS. The DSS scheme utilizes the set of integers Z_p where p is a large prime. For adequate security, p must be in the order of 512 bits although the resultant signature may be reduced mod q , where q divides $p-1$, and may be in the order of 160 bits.

The DSS protocol provides a signature composed of two components r, s . The protocol requires the selection of a secret random integer k referred to as the session key from the set of integers $\{0, 1, 2, \dots, q-1\}$, i.e.

$$k \in \{0, 1, 2, \dots, q-1\}.$$

The component r is then computed such that

$$r = \{g^k \bmod p\} \bmod q$$

where β is a generator of q .
The component s is computed as

$$s = \{k^{-1} (h(m) + ar)\} \bmod q$$

where m is the message to be transmitted,
 $h(m)$ is a hash of that message, and
 a is the private key of the user.

The signature associated with the message is then s, r which may be used to verify the origin of the message from the public key of the user.

The value β^k is computationally difficult for the DSS implementation as the exponentiation requires multiple multiplications mod p . This is beyond the capabilities of a "Smart Card" in a commercially acceptable time. Although the computation could be completed on the associated ATM, this would require the disclosure of the session key k to the ATM and therefore render the private key, a , vulnerable.

It has been proposed to precompute β^k and store sets of values of r and k on the card. The generation of the signature then only requires two 160 bit multiplications and signing can be completed within $\frac{1}{2}$ second for typical applications. However, the number of sets of values stored limits the number of uses of the card before either reloading or replacement is required. A problem that exists therefore is how to generate sufficient sets of values within the storage and/or computing capacity of the card.

One possibility is to use a smaller value of p but with the DSS scheme this will jeopardize the security of the transaction.

An alternative encryption scheme that provides enhanced security at relatively small modulus is that utilizing elliptic curves in the finite field 2^m . A value of m in the order of 155 provides security comparable to a 512 bit modulus for DSS and therefore offers significant benefits in implementation.

Diffie Helman Public Key encryption utilizes the properties of discrete logs so that even if a generator β and the exponentiation β^k is known, the value of k cannot be determined. A similar property exists with elliptic curves where the addition of two points on a curve produces a third point on the curve. Similarly, multiplying any point on the curve by an integer k produces a further point on the curve. However, knowing the starting point and the end point does not reveal the value of the integer 'k' which may then be used as a session key for encryption. The value kP , where P is an initial known point, is therefore equivalent to the exponentiation β^k .

In order to perform a digital signature on an elliptic curve, it is necessary to have available the session key k and a value of kP referred to as a "session pair". Each signature utilizes a different session pair k and kP and although the representation of k and kP is relatively small compared with DSS implementations, the practical limits for "Smart Cards" are in the order of 32 signatures. This is not sufficient for commercial purposes.

One solution for both DSS and elliptic curve implementations is to store pairs of signing elements k, kP and combine stored pairs to produce a new session pair. For an elliptic curve application, this would yield a possible 500 session pairs from an initial group of 32 stored signing elements. The possibilities would be more limited when using DSS because of the smaller group of signing elements that could be stored.

In order to compute a new session pair, k and kP , from a pair of stored signing elements, it is necessary to add the values of k , e.g. $k_1 + k_2 \rightarrow k$ and the values of k_1P and k_2P to give a new value kP . In an elliptic curve, the addition of two

points to provide a third point is performed according to set formula such that the addition of a point k_2P having coordinates (x_2, y_2) and a point k_1P having coordinates (x_1, y_1) provides a point k_3P whose x coordinate x_3 is given by:

$$x_3 = \frac{y_1 \oplus y_2 \oplus (y_1 \oplus y_2) \oplus (x_1 \oplus x_2)}{x_1 \oplus x_2} \oplus x_1 \oplus x_2$$

This computation may be significantly simplified using the normal basis representation in a field $F2^m$, as set out more fully in our PCT Application Serial No.

PCT/CA/9500452, the contents of which are incorporated herein by reference. However, even using such advantageous techniques, it is still necessary to utilize a finite field multiplier and provide sufficient space for code to perform the computation. This is not feasible within the practical limits of available "Smart" cards.

As noted above, the ATM used in association with the card has sufficient computing power to perform the computation but the transfer of the coordinates of k_1P and k_2P from the card to the terminal would jeopardize the integrity of subsequent digital signatures as two of the stored signing elements would be known.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to obviate or mitigate the above disadvantages and facilitate the preparation of additional pairs of values from a previously stored set.

In general terms, one aspect of the present invention proposes to compute on one computing device an initial step in the computation of a coordinate of a point derived from a pair of points to inhibit recognition of the individual components, transfer such information to another computing device remote from said one device, perform at least such additional steps in said derivation at such other device to permit the completion of the derivation at said one device and transfer the result thereof to said one computing device.

Preferably, the initial step involves a simple field operation on the two sets of coordinates which provides information required in the subsequent steps of the derivation.

Preferably also the additional steps performed at the other device complete the derivation.

In a preferred embodiment, the initial step involves the addition of the x coordinates and the addition y coordinates to provide the terms $(x_1 \oplus x_2)$ and $(y_1 \oplus y_2)$.

The addition of the coordinates is an XOR operation that can readily be performed on the card and the results provided to the terminal.

In this manner, the coordinates (x, y) representing kP in a stored signing element are not disclosed as insufficient information is provided even with subsequent uses of the card. Accordingly, the x coordinate of up to 500 signatures can be generated from an initial set of 32 stored signing elements.

The new value of k can be computed on the card and to avoid computing the inverse k^{-1} , alternative known masking techniques can be utilized.

A further aspect of the present invention provides a method of generating additional sets of points from the initial set that may be used individually as a new value of kP or in combination to generate still further values of kP .

According to this aspect of the invention, the curve is an anomalous curve and the Frobenius Operator is applied to at

least one of the coordinates representing a point in the initial set to provide a coordinate of a further point on the elliptic curve. The Frobenius Operator \emptyset provides that for a point (x_1, y_1) on an anomalous curve, then $\emptyset(x_1, y_1)$ is a point (x_1^2, y_1^2) that also lies on the curve. In general, $\emptyset^i(x_1, y_1)$ is a point $x_1^{2^i}, y_1^{2^i}$ that also lies on the curve. For a curve over the field $F2^m$, there are m Frobenius Operators so for each value of kP stored in the initial set, m values of kP may be generated, referred to as "derived" values. The new value of k associated with each point can be derived from the initial relationship between P and $\emptyset P$ and the initial value of k .

For a practical implementation where 32 pairs of signing elements are initially retained on the card and the curve is over the field $F2^{155}$, utilizing the Frobenius Operator provides in the order of 4960 possible derived values and by combining pairs of such derived values as above in the order of 10^7 values of kP can be obtained from the initial 32 stored signing elements and the corresponding values of k obtained to provide 10^7 session pairs.

Preferably, the stored values of kP are in a normal basis representation. The application Frobenius Operator then simply requires an "i" fold cyclic shift to obtain the value for an \emptyset^i operation.

According to a further aspect of the invention, there is provided a method of generating signature components for use in a digital signature scheme, said signature components including private information and a public key derived from said private information, said method comprising the steps of storing private information and related public key as an element in a set of such information, cycling in a deterministic but unpredictable fashion through said set to select at least one element of said set without repetition and utilizing said one element to derive a signature component in said digital signature scheme.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other object and advantages of the present invention will become apparent from the following description when read in conjunction with the accompanying drawings wherein:

FIG. 1 is a schematic representation of a programmable credit card;

FIG. 2 is a schematic representation of a transaction performed between the card and network;

FIG. 3 is a schematic representation of the derivation of a session pair from a pair of stored signing elements;

FIG. 4 is a schematic representation of one step in the transmission of information shown in FIG. 2;

FIG. 5 is a schematic representation of a preferred implementation of the derivation of a session pair from two pairs of stored values;

FIG. 6 is a schematic representation of a selection unit shown in FIG. 1;

FIG. 7 is a schematic representation of a further embodiment of the derivation of session pairs from stored values;

FIG. 8 is an alternative schematic to the embodiment of FIG. 7; and

FIG. 9 is yet another alternative schematic to the embodiment of FIG. 7.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The System

Referring therefore to FIG. 1, a programmable credit card 10 (referred to as a "SMART" card) has an integrated circuit 12 embedded within the body of card 10.

The integrated circuit includes a logic array 14, an addressable memory 16 and a communication bus 18. The memory 16 includes a RAM section 20 to store information, a pair of cyclic shift registers 22 for temporary storage of information and programming code 24 for control of the logic array 14 and communication bus 18. The array 14 includes an arithmetic unit 26 to provide modular arithmetic operation, e.g. additional and multiplication, and a selection unit 28 controlled by the programming code 24. It will be appreciated that the description of the card 10 is a schematic and restricted to that necessary for explanation of the preferred embodiment of the invention.

The card 10 is used in conjunction with a terminal 30, for example an automated teller machine (ATM), that is connected to a network to allow financial transactions to be conducted. The terminal 30 includes a keypad 32 to select options and tasks and has computing capabilities to perform the necessary functions in conjunction with the card 10.

Access to the terminal 30 is obtained by inserting card 10 into a reader 34 and entering a pass code in a conventional manner. The pass code is verified with the card 10 through communication bus 18 and the terminal 30 activated. The keypad 32 is used to select a transaction, for example a transfer of funds, between accounts and generate a message through the network to give effect to the transactions, and card 10 is used to sign that transaction to indicate its authenticity. The signature and message are transmitted over the network to the intended recipient and upon receipt and verification, the transaction is completed.

The Card

The RAM section 20 of memory 16 includes digital data string representing a private key, a , which remains secret with the owner of the card and a corresponding public key $Q=aP$ where P is the publicly known initial point on the selected curve. The RAM section 20 also includes a predetermined set of coordinates of points, kP , on an elliptic curve that has been preselected for use in a public key encryption scheme. It is preferred that the curve is over a finite field 2^m , conveniently, and by way of example only, 2^{155} , and that the points kP are represented in normal basis representation. The selected curve should be an anomalous curve, e.g. a curve that satisfies $y^2+xy=x^3+1$, and has an order, e . Each point kP has an x coordinate and a y coordinate and is thus represented as two 155 digital data strings that are stored in the RAM 20. By way of example, it will be assumed that the RAM 20 contains 32 such points identified generically as kP and individually as $k_0P, k_1P, \dots, k_{31}P$. Similarly, their coordinates (x, y) will be individually designated $x_0y_0, \dots, x_{31}y_{31}$.

The points kP are precomputed from the chosen parameters of the curve and the coordinates of an originating point P . The k -fold addition of point P will provide a further point kP on the curve, represented by its coordinates (x, y) and the value of k cannot be determined even if the coordinates of points P and kP are known.

RAM 20 therefore contains the values of k associated with the respective points kP so that a set of stored signing elements k, kP is available for use in the signing of the transaction.

Signing

To sign a message m generated by the transaction, one session pair k, kP is required and may be obtained from RAM 20 as set out more fully below. Assuming that values k, kP have been obtained, the signing protocol requires a signature (r, s) where

r is the data string representing the x -coordinate, x_i reduced mod q (q is a preselected publicly known divisor of e , the order of the curve, i.e. $q|e$); and $s=[k^{-1}(h(m))+ar] \bmod q$ where $h(m)$ is a q -bit hash of the message m generated by the transaction.

In this signature, even though r is known, s contains the secret k and the private key, a , and so inhibits the extraction of either.

The generation of s requires the inversion of the value k and since k is itself to be derived from the stored set of values of k , it is impractical to store corresponding inverted values of possible k 's. Accordingly, a known masking technique is used to generate components r, s' and u of a signature. This is done by selecting an integer, c , and computing a value $u=ck$. The value $s^{-1}=c(h(m)+ar) \bmod q$.

The signature value s can then be obtained by the recipient computing $s'u^{-1}=k^{-1}[h(m)+ar]$.

The signature (r, s', u) can be computed on the card 10 and forwarded by bus 18 to the terminal 30 for attachment to the message m .

Generation of Session Pair

As noted above, in order to generate the signature (r, s) , it is necessary to have for session pair k and kP . Security dictates that each session pair is only used once and it is assumed that the number of signing elements stored in RAM 20 is insufficient for commercial application.

In the preferred embodiment, two techniques are used to generate additional session pairs to the stored signing elements. It will be appreciated that each technique may be used individually although the combination of the two is preferred.

(i) Frobenius Operator

The first technique involves the use of the Frobenius Operator to derive additional session pairs from the stored signing elements and is shown in FIG. 3. The Frobenius Operator denoted \mathcal{O} operates on a point P having coordinates (x, y) on an anomalous elliptic curve in the finite field 2^m such that $\mathcal{O}^i P = (x^{2^i}, y^{2^i})$. Moreover, the point $\mathcal{O}^i P$ is also on the curve. In the field 2^{155} , there are 155 Frobenius Operators so each point kP stored in memory 20 may generate 155 points on the curve by application of the Frobenius Operators. Thus, for the 32 values of kP stored, there are 4960 possible values of kP available by application of the Frobenius Operator.

To derive the value of $\mathcal{O}^i P$, it is simply necessary to load the x and y coordinates of a point kP into respective shift registers 22 and perform an i -fold cyclic shift. Because the coordinates (x, y) have a normal basis representation, a cyclic shift in the register 22 will perform a squaring operation, and an i -fold cyclic shift will raise the value to the power 2^i . Therefore, after the application of i clock cycles, the registers 22 contain the coordinates of $\mathcal{O}^i(kP)$ which is a point on the curve and may be used in the signing protocol. The 155 possible values of the coordinates (x, y) of $\mathcal{O}^i(kP)$ may be obtained by simple cyclic shifting. The representations in the registers 22 may then be used to obtain r .

Where the use of Frobenius Operator provides sufficient values for commercial use, only one coordinate is needed to compute the value of r and so only a single shift register is needed. However, as will be described below, further session pairs can be derived if both the coordinates are known and so a pair of registers is provided.

For each value of $\mathcal{O}^i(kP)$, it is necessary to obtain the corresponding value of k $\mathcal{O}^i(P)=\lambda P$. λ is a constant that may be evaluated ahead of time and the values of its first m powers, λ^i computed. The m values are stored in RAM 20.

In general, $\Phi^i(kP) \rightarrow \lambda^i kP$ so the value of k associated with $\Phi^i(kP)$ is $\lambda^i k$. Since k is stored for each value of kP in RAM 20 and λ^i is also stored, the new value of k , i.e. $\lambda^i k$, can be computed using the arithmetic unit 26.

As an alternative, to facilitate efficient computation of λ^i and avoid excessive storage, it is possible to precompute specific powers of λ and store them in RAM 20. Because m is 155 in the specific example, the possible values of i can be represented as an 8-bit binary word. The values of $\lambda^2 \rightarrow \lambda^7$ are thus stored in RAM 20 and the value of λ represented in binary. The prestored values of λ^2 are then retrieved as necessary and multiplied mode by arithmetic unit 26 to provide the value of λ^i . This is then multiplied by k to obtain the new value associated with $\Phi^i(kP)$.

It will be seen therefore that new session pairs k, kP may be derived simply and efficiently from the stored signing elements of the initial set. These session pairs may be computed in real time, thereby obviating the need to increase storage capacity and their computation utilizes simple arithmetic operations that may be implemented in arithmetic unit 26.

(ii) Combining Pairs

A further technique, illustrated schematically in FIG. 4, to increase the number of session pairs of k and kP available, and thereby increase the number of signatures available from a card, is to combine pairs of stored signing elements to produce a new derived value. The addition of two points k_1P and k_2P will produce a third point k_3P that also lies on the curve and may therefore be used for signatures.

The addition of two points having coordinates (x_1, y_1) (x_2, y_2) respectively on a curve produces a new point having an x coordinate x_3 where

$$x_3 = \frac{y_1 \oplus y_2^2 \oplus y_1 \oplus x_2 \oplus x_1 \oplus x_2}{x_1 \oplus x_2 \quad x_1 \oplus x_2}$$

In the finite field $2m$, $y_1 \oplus y_2$ and $x_1 \oplus x_2$ is an XOR field operation that may be performed simply in logic array 16. Thus the respective values of x_1, x_2 and y_1, y_2 are placed in respective ones of registers 22 and XOR'd. The resultant data string is then passed over communication bus 16 to the terminal 30. The terminal 30 has sufficient computing capacity to perform the inversion, multiplication and summation to produce the value of x_3 . This is then returned to register 22 for signature. The potential disclosure of x_3 does not jeopardize the security of the signature as the relevant portion is disclosed in the transmission of r .

The value of k_1+k_2 is obtained from the arithmetic unit 26 within logic array 16 to provide a value of k_3 and hence a new session pair k_3, k_3P is available for signature.

It will be appreciated that the value for y_3 has not been computed as the signing value r is derived from x_3 rather than both coordinates.

It will be noted that the values of x_1 and x_2 or y_1 and y_2 are not transmitted to terminal 30 and provided a different pair of points is used for each signature, then the values of the coordinates remains undisclosed.

At the same time, the arithmetic functions performed on the card are relatively simple and those computationally more difficult are performed on the terminal 30.

Preferred Implementation of Generating Session Pairs

The above technique may of course be used with pairs selected directly from the stored signing elements or with the derived values obtained using the Frobenius Operator as

described above. Alternatively, the Frobenius Operator could be applied to the value of kP obtained from combining pairs of the stored signing elements to provide m possible values of each derived value.

To ensure security and avoid duplication of session pairs, it is preferred that only one of the stored signing elements should have the Frobenius Operator applied, as in the preferred embodiment illustrated in FIG. 5.

In this arrangement, the coordinates x_1, y_1 of one of the stored signing elements is applied to the registers 22 and cyclically shifted i times to provide $\Phi^i k_1P$.

The respective coordinates, x_{Φ}, y_{Φ} , are XOR'd with the coordinates from another of the stored values k_2P and the summed coordinates transmitted to ATM 30 for computation of the coordinate x_3 . This is retransmitted to the card 10 for computation of the value r .

The value of k_1 is processed by arithmetic unit 26 to provide $\lambda^i k$ and added to k_2 to provide the new value k_3 for generation of signature component s . In this embodiment, from an original set of 32 stored signing elements stored on card 10, it is possible to generate in the order of 10^7 session pairs. In practice, a limit of 10^6 is realistic.

Selection of Pairs Stored Signing Elements

The above procedure requires a pair of stored signing elements to be used to generate each session pair. In order to preserve the integrity of the system, the same set cannot be used more than once and the pairs of stored values constituting the set must not be selected in a predictable manner.

This selection function is performed by the selection unit 28 whose operation is shown schematically in FIG. 6.

Selection unit 28 includes a set of counters 40,42,44 whose outputs address respective look up tables 46,48,50. The look up tables 46,48,50 map the successive outputs of the counters to pseudo random output values to provide unpredictability for the selection stored signing elements.

The 32 stored values of k and kP are assigned nominal designations as elements in a set 52 ranging from -15 to +15 with one designated ∞ . To ensure that all available combinations of stored values are used without repetition, the nominal designations are grouped in 16 pairs in an ordered array 54 such that the difference (mod 31) in the assigned values of a pair uses all the numbers from 1 to 30. ∞ is grouped with 0. This array provides a first row of a notional matrix.

Successive rows 54a,b,c, etc. of the notional matrix are developed by adding 1 to each assigned designation of the preceding row until 15 rows are developed. In this way a matrix is developed without repetition of the designations in each cell. By convention $\infty+1=\infty$.

Counter 42 will have a full count after 15 increments and counter 40 will have a full count after 14 increments. Provided the full count values of counters 40,42 are relatively prime and the possible values of the counter 50 to select Frobenius Operator are relatively large, the output of counters 40,42,44 are mapped through the tables 46,48,50 respectively to provide values for row and column of the notional matrix and the order i of the Frobenius Operator to be applied.

The output of counter 48 selects a column of the array 54 from which a designation associated with a starting pair can be ascertained. In the example of FIG. 6, the output of counter 42 is mapped by table 48 to provide an output of 3, indicating that column 3 of array 54 should be selected.

Similarly, the output of counter 40 is mapped through table 46 to provide a count of 3 indicating that values in row 3 of the matrix should be used.

The assigned designations for a particular row are then obtained by adding the row value to the values of the starting pair. This gives a new pair of assigned designations that indicate the locations of elements in set 52. The signing elements are then retrieved from the set 52.

One of those pairs of signing elements is then output to a shift register 22 and operated upon by the designated Frobenius Operator ϕ . The value of the Frobenius Operation is obtained from the output of table 50 which maps counter 44. The value obtained from table 5 sets the shift clock associated with register 22 so that the contents of the register 22 are cyclically shifted to the Frobenius value ϕ indicated by the output of table 50.

Accordingly, a new value for kP is obtained. The associated value of k can be computed as described above with the arithmetic unit utilizing the output of table 50 to determine the new value of λ . Accordingly, a derived value is obtained.

The derived value and signing element are then combined as described at (ii) above to provide a new session pair k, kP for use in the signing process.

The use of the counters 40,42 provides input values for the respective tables so that the array 54 is accessed in a deterministic but unpredictable fashion. The grouping of the pairs in the array 54 ensures there is no repetition in the selected elements to maintain the integrity of the signature scheme.

Counter 44 operates upon one of the selected pairs to modify it so that a different pair of values is presented for combination on each use, even though multiple access may be made to the array 54.

The counters 40,42,44 may also be utilized to limit the use of the Smart Card if desired so that a forced expiry will occur after a certain number of uses. Given the large number of possible signatures, this facility may be desirable.

Alternative structures to the look up tables 46,48,50 may be utilized, such as a linear feedback shift register, to achieve a mapped output if preferred.

Further selection of the session pairs can be obtained by preprocessing of the contents of register 52 using one or more of the techniques shown in FIGS. 7, 8 or 9.

In its simplest form, as shown in FIG. 7, a source row 's' is selected and the session pair $k_s, k_s P$ read from the register. A function is applied to the session pair, which for example is the Frobenius operation as set out in FIG. 3 to provide a new session pair $\lambda^i k_s, \phi^i(k_s P)$. A destination row, d, is then selected in the table 52 and the new session pair combined with the contents of that row to generate a new pair of values. The contents of the table 52 are thus updated and a selection of pairs may be made for the generation of a new session pair as described above.

The preprocessing may be repeated a number of times with different source rows s, and destinations, d, so that a thorough mixing is obtained. The selection of source rows, s, and destinations, d, may be selected deterministically using the counters 40,42.

Alternatively, where the card 10 does not have adequate computing power or a curve other than an anomalous curve is used, an alternative function may be applied to the selected row. For example, a sign may be applied to the selected row prior to accumulation of a destination.

An alternative embodiment is shown in FIG. 8 where multiple source rows s_1, \dots, s_n , are used and the selected

session pairs combined. Typically two source rows are used but more than two can be combined if preferred. In this case the combining may proceed as shown in FIG. 5 and the new value accumulated at the destination row, d, of the register. As the x coordinate of the combined point will identify one of the coordinates in the register 52, it is preferred to perform the computation on the card where feasible.

The selected session pairs may be modified prior to or subsequent to their addition by application of a second function, e.g. signing, (as shown in ghosted outline) to provide further security in the updating of the register 52.

Where a random number generator is incorporated on the card 10, the above preprocessing may be used effectively in the production of the cards. Referring to FIG. 9, an initial set of session pairs is injected into the register 52 of each card 10. A random number generator 60 is run for an initial period and its output used to select the source and destination rows of the register 52. The source row is accumulated with the destination row so that the session pair of the set are changed with each iteration. If preferred, a function such as a sign or a Frobenius operation may be applied to the selected session pair before accumulation. The mixing continues for a further period with the output of generator 60 being used periodically to select each row. Once the register is considered thoroughly mixed, the session pairs may be selected and combined as described above for FIG. 6. As the output of each generator 60 will vary from device to device, the sets of session pairs in each register 52 will also vary from device to device. Therefore the same initial table may be used but different session pairs will be generated.

In summary, therefore, pairs of signing elements from an initial set of stored values can be selected in a deterministic and unpredictable manner and one of those elements operated upon by the Frobenius Operator to provide additional values for the elements. The elements may then be combined to obtain a new session pair with a portion of the computation being performed off card but without disclosing the value of the elements. Accordingly, an extended group of session pairs is available for signing from a relatively small group of stored values.

While the present invention has been illustrated and described by means of a specific embodiment, it is to be understood that numerous changes and modifications can be made therein without departing from the spirit and scope of the invention.

What is claimed is:

1. A method of generating a signature on a message m in an elliptic curve cryptographic system having a seed point P on an elliptic curve of order e over a finite field, said method comprising the steps of:

- i) selecting as a session key an integer k and computing representation of a corresponding point kP ;
- ii) deriving from said representation a first signature component, r, independent of said message, m;
- iii) combining said first signature component, r, with a private key, a, a value derived from said message, m, and said session key, k, to obtain a second signature component, s, containing said private key, a, and said session key, k, such that extraction of either is inhibited even when said signature components, r,s, are made public; and
- iv) utilizing said signature components r,s, in the signature of the message, m.

2. A method according to claim 1 wherein said value derived from said message, m, is obtained by applying a hash function to said message.

11

3. A method according to claim 2 wherein said second signature component, s , is of the form $s=k^{-1}\{h(m)+ar\}$ mod q , where q is a divisor of the order, e , of said elliptic curve and $h(m)$ is said value derived by applying a hash function to said message.

4. A method according to claim 1 wherein said first signature component r is obtained by utilizing one coordinate of said point kP .

5. A method according to claim 4 wherein said one coordinate is the x coordinate of said point kP .

6. A method according to claim 5 wherein said x -coordinate is reduced mod q .

7. A method according to claim 6 wherein said signature consists of said first and second signature components.

8. A method according to claim 7 wherein said elliptic curve is an anomalous elliptic curve.

9. A method according to claim 8 wherein said anomalous curve is of the form $y^2=xy=x^2+1$.

10. A method according to claim 1 wherein an integer is derived from said representation of said point kP .

11. A method according to claim 10 wherein said integer is obtained by selecting one of said coordinates of said point kP , and reducing said coordinate mod q where q is a divisor of the order, e , of the elliptic curve.

12. A method according to claim 11 wherein said one coordinate is the x coordinate of said point kP .

13. A method according to claim 12 wherein said divisor q is preselected and publically known.

14. A method according to claim 12 wherein said value derived from said message, m , is obtained by applying a hash function to said message.

15. A method according to claim 14 wherein said value derived from said message is a q bit hash of said message.

16. A method according to claim 15 wherein said elliptic curve is an anomalous elliptic curve.

17. A method according to claim 16 wherein said elliptic curve is of the form $y^2+xy=x^2+1$.

18. A method according to claim 1 wherein said second signature component s has a value corresponding to $k^{-1}\{h(m)+ar\}$ mod q .

19. A method according to claim 18 wherein a value corresponding to said second signature component s is obtained by selecting an integer, c , and computing a value, u , which equals the product of c and k and computing $s=c\{h(m)+ar\}$, said signature components on said message m including r , s , and u .

20. A method according to claim 19 wherein a value corresponding to $k^{-1}\{h(m)+ar\}$ mod q is obtained by a recipient of said signature by computing the product of said second signature component, s , and an inverse of said value, u .

12

21. A method of generating a digital signature r, s , of a message m using an elliptic curve cryptosystem employing an elliptic curve of order e , said method comprising the steps of:

i) selecting an integer k and determining a corresponding point kP where P is point on the curve;

ii) selecting a coordinate (x) of the point kP ;

iii) reducing the coordinate mod q where q is a known divisor of e , to obtain a first component r ; and

iv) combining said first component, r , with a long-term private key a and said integer k to obtain a second signature component s , such that extraction of either said long term private key a or said integer k is inhibited even when said signature r, s , are made public.

22. A method according to claim 21 wherein said second signature component s has the form $s=k^{-1}\{h(m)+ar\}$ mod q , where $h(m)$ is a hash of the message m .

23. A method according to claim 22 wherein said elliptic curve is an anomalous elliptic curve of the form $y^2+xy=x^2+1$.

24. A method of generating a signature r, s , of a message m performed on an elliptic curve cryptosystem implemented over an anomalous elliptic curve of the form said $y^2+xy=x^2+1$, method comprising the steps of:

i) performing a Frobenius operation θ upon at least one coordinate, x , of a point kP , where k is an integer and kP is a point on the curve obtained from a k fold composition of a point P on the curve, to obtain a corresponding coordinate x' of a point $k'P$ corresponding to $\theta'(kP)$;

ii) operating upon the integer k upon by a constant λ , where $\theta'(kP)=\lambda^k P$ to obtain a value k' ;

iii) utilizing the coordinate x' to obtain a first signature component r ; and

iv) combining said first signature component r with the value k' to obtain said second signature component s .

25. A method of generating a session key pair from an initial key pair k, kP for use in a public key encryption elliptic scheme implemented over an anomalous curve of the form $y^2+xy=x^2+1$ where k is an integer and kP is a point on the curve obtained from a k fold composition of a point P on the curve, said method comprising the steps of:

i) performing a Frobenius operation θ' upon the point kP to obtain a point $k'P$ corresponding to $\theta'(kP)$;

ii) operating upon the integer k by a constant λ , where $\theta'(kP)=\lambda^k P$ to obtain a value k' corresponding to $\lambda^k k$; and utilizing the values k' and $k'P$ as a session key pair in a cryptographic operation.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 6,704,870 B2
DATED : March 9, 2004
INVENTOR(S) : Vanstone et al.

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 10.

Line 58, delete the number "10" after the word "second."

Column 11.

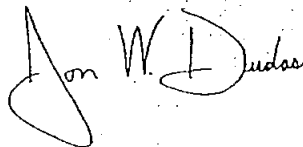
Lines 40 and 48, change the equation after the word "to" to read as
-- $k^{-1}\{h(m)+ar\} \bmod q$ --.

Column 12.

Line 11, delete the number "10" after the word "and."
Line 16, change the equation after the word "form" to read as
-- $s=k^{-1}\{h(m)+ar\} \bmod q$ --.

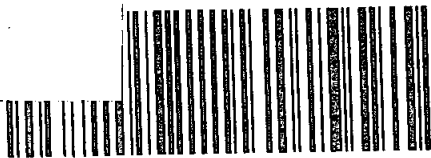
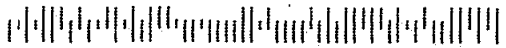
Signed and Sealed this

Twenty-fifth Day of October, 2005

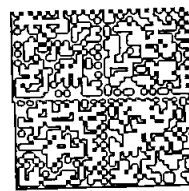


JON W. DUDAS
Director of the United States Patent and Trademark Office

CERTIFIED MAIL™



7005 1820 0002 7118 0897



015H14122029
\$6.79
05/31/07
Mailed From 75670

US POSTAGE

THE ROTH LAW FIRM
P.O. BOX 876
MARSHALL, TEXAS 75671

TO:

Sony DADC US, Inc.
Corporation Service Company
2711 Centerville Rd., Suite 400
Wilmington, DE 19808