(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 698 31 792 T2** 2006.06.22

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 963 638 B1**
(21) Deutsches Aktenzeichen: **698 31 792.0**
(86) PCT-Aktenzeichen: **PCT/FR98/02680**
(96) Europäisches Aktenzeichen: **98 959 943.6**
(87) PCT-Veröffentlichungs-Nr.: **WO 99/033220**
(86) PCT-Anmeldetag: **10.12.1998**
(87) Veröffentlichungstag der PCT-Anmeldung: **01.07.1999**
(97) Erstveröffentlichung durch das EPA: **15.12.1999**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **05.10.2005**
(47) Veröffentlichungstag im Patentblatt: **22.06.2006**

(51) Int Cl.[8]: ***H04L 9/32*** (2006.01)

(30) Unionspriorität:
9716061 **18.12.1997** **FR**

(73) Patentinhaber:
Etat-Français representé par le Délégué Général pour l'Armement, Armees, FR

(74) Vertreter:
Prinz und Partner GbR, 80335 München

(84) Benannte Vertragsstaaten:
BE, CH, DE, DK, ES, GB, GR, IT, LI, LU, NL, PT, SE

(72) Erfinder:
JOUX, Antoine, F-35235 Thorigne-Fouillard, FR

(54) Bezeichnung: **VERFAHREN ZUR DIGITALEN UNTERSCHRIFT**

Beschreibung

[0001] Die vorliegende Erfindung hat insbesondere ein Verfahren für die Erzeugung einer digitalen Signatur (c, d) einer Nachricht M sowie ein Verfahren zur Authentisierung einer solchen Signatur zum Gegenstand.

[0002] Digitale Signaturverfahren richten sich auf das Beglaubigen des Ursprungs eines elektronischen Dokuments. In einer zu einer handschriftlichen Signatur ähnlichen Weise wird eine digitale Signatur an eine elektronische Nachricht angefügt, um ihre Authentizität zu garantieren. Es sei der praktische Fall betrachtet, in dem eine Entität A eines Kommunikationssystems eine Nachricht M an eine Entität B schicken will. In einer ersten Phase der Erzeugung der Signatur führt der Sender A, nachdem er seine Nachricht geschrieben hat, in Abhängigkeit von der zu signierenden Nachricht M und von Operanden, die sowohl geheim als auch öffentlich sein können, eine Gesamtheit von mathematischen Operationen aus. Diese Berechnungen ermöglichen das Erzeugen einer digitalen Entität, die als Signatur bezeichnet wird. Die Nachricht M sowie ihre Signatur werden anschließend elektronisch übertragen. In einer zweiten Phase, nach dem Empfang der Nachricht und der Signatur, führt der Empfänger B seinerseits mathematische Operationen aus, Das Ergebnis dieser letzten Berechnungen ermöglicht das Überprüfen der Gültigkeit der empfangenen Signatur. Es ist anzumerken, dass das Ziel der Signaturfunktion das Sicherstellen der Authentisierung einer Nachricht N und nicht das Sicherstellen der Vertraulichkeit ihres Inhalts ist. Diese Nachricht kann folglich entweder unverschlüsselt oder durch eine von dem Signaturmechanismus völlig unabhängige Chiffrierfunktion chiffriert übertragen werden.

[0003] Global ermöglicht ein digitales Signaturverfahren in einem modernen Kommunikationssystem:

(a) das Authentifizieren in zuverlässiger Weise der Identität des Senders der Nachricht,

(b) das Sicherstellen der Unversehrtheit des Inhalts einer Nachricht (es wird geprüft, ob die Nachricht während ihrer Übertragung nicht verändert worden ist).

[0004] Bei den digitalen Signaturverfahren basiert die Sicherheit auf der extremen Schwierigkeit, bestimmte mathematische Funktionen umzukehren. Tatsächlich ist es heutzutage bei der heutigen Rechenleistung der Rechner unmöglich, bestimmte dieser Gleichungen zu lösen, ohne die geheimen Elemente des Algorithmus zu kennen.

[0005] Gegenwärtig gibt es mehrere Typen von digitalen Signaturverfahren.

[0006] Ein erster Typ, der von Rivest-Shamir-Adelman entwickelt worden ist, stützt sich auf die Schwierigkeit, große ganze Zahlen in Faktoren zu zerlegen (siehe "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, Februar 1978, Bd. 21, Nr. 2, S. 120–126, und das sich darauf beziehende US-Patent 4.405.829).

[0007] Ein zweiter Typ, der von Taher El-Gamal entwickelt worden ist, schlägt Signaturalgorithmen vor, die auf dem Problem des diskreten Logarithmus, das eine diskrete Potenzierung einsetzt, basiert (siehe "A Public Key Cryptosystem and a signature scheme based on discrete logarithms", IEEE Trans. on Inform Theory, Bd. IT-31, S. 469–472, Juli 1985).

[0008] Die diskrete Potenzierung umfasst drei Argument, die Basis der Potenzierung g, den Exponenten x und das Modulo N Das Problem des diskreten Logarithmus besteht darin, bei gegebener mathematischer Beziehung: $Y = g^x$ modulo N (was bedeutet: Y ist der Rest der Division von g^x durch N) x zu finden, wenn N, g und Y bekannt sind.

[0009] Ein Verfahren desselben, jedoch einfacheren Typs ist durch Schnorr offenbart worden und bildet den Gegenstand des US-Patents 4.995.082. Es unterscheidet sich von jenem von El-Gamal dadurch, dass es darin besteht, die Größe der Exponenten der diskreten Potenzierungen zu verkleinern, um die Berechnungen zu beschleunigen. Dazu erzeugt ein Element g eine Untergruppe der Größenordnung q, wobei q beispielsweise 160 bit breit ist. Zudem wird bei der Berechnung der Signatur eine Hashfunktion verwendet.

[0010] Die so erzeugte digitale Signatur besitzt eine kleine Größe.

[0011] Allgemein kann die diskrete Potenzierung je nach Fall eine modulare Potenzierung sein, bei der dann mit ganzen Zahlen und einer gut gewählten Zahl als Modulo, gearbeitet wird, oder eine Multiplikation mit einer ganzen Zahl auf einer elliptischen Kurve sein, was eine zu einer modularen Potenzierung ähnliche Operation ist, jedoch über eine Gruppe, die als additiv anstatt multiplikativ vermerkt ist, definiert ist.

[0012] Bei zahlreichen Anwendungen müssen die digitale Signatur sowie ihre Verifizierung in Echtzeit ausgeführt werden. Bestimmte Verfahren wie etwa jenes von El-Gamal benötigen eine große Investition an Hardware, da die Algorithmen sehr leistungsstarke Maschinen erfordern. Um diesen Hardwarezwängen zu entgehen, ermöglicht die Optimierung der Algorithmen das Verringern des Umfangs an Berechnungen und dabei das Bewahren einer vergleichbaren Sicherheit.

[0013] Die Lösung der diskreten Potenzierung ist heutzutage die am meisten bei den kryptographi-

schen Systemen angewandte Lösung, wobei an den Algorithmen bestimmte Verbesserungen vorgenommen worden sind, um die Rechengeschwindigkeit zu erhöhen und dennoch eine maximale Sicherheit zu bewahren.

[0014] Unter dieser Perspektive ist das Verkleinern der Größe (der Anzahl von Bits) des Exponenten sehr wichtig, da die Rechenzeit der modularen Potenzierung zu dieser Größe proportional ist.

[0015] Zum anderen muss bei den bis heute bekannten Algorithmen die Kardinalzahl der Gruppe, in der gearbeitet wird, bekannt sein. Die Kardinalzahl dieser Gruppe hängt von der Wahl des Modulo N ab. Da die Sicherheit des Algorithmus auf der diskreten Potenzierung beruht, muss ihre Auflösung unmöglich gemacht werden. Diese Sicherheit impliziert bestimmte Zwänge bezüglich der Wahl des Modulo N.

[0016] Im Fall einer modularen Potenzierung bietet die Sicherheit der diskreten Potenzierung gemäß dem Stand der Technik nur zwei Möglichkeiten der Wahl des Modulo N.

[0017] Im Rahmen der ersten Möglichkeit ist N ein Produkt aus zwei Primzahlen. El-Gamal schlägt vor, N so zu wählen, dass (N – 1)/2 teilerfremd ist und der behaltene Divisor (N – 1) ist.

[0018] Die zweite Möglichkeit betrifft die Basisalgorithmen der diskreten Potenzierung, bei der eine Untergruppe sowie ihre Kardinalzahl bekannt sein müssen, wobei die Kardinalzahl dieser Untergruppe ein Teiler von N – 1 ist, wenn N teilerfremd ist, oder im Fall einer elliptischen Kurve ein Teiler mit der Anzahl von Punkten auf der Kurve ist. Schnorr schlägt vor, q als Kardinalzahl der Untergruppe zu wählen, wobei q derart ist, dass es N – 1 teilt.

[0019] Die Erfindung beseitigt diese Nachteile, indem sie ein Verfahren vorschlägt, das geeignet ist, den Umfang der Berechnungen zu verringern und das Arbeiten in Echtzeit mit einem Rechner des Typs PC zu ermöglichen.

[0020] Sie hebt ferner die oben genannten Beschränkungen auf, wobei die Wahl des Modulo N nicht mehr auf die zwei anführten Möglichkeiten begrenzt ist oder die Berechnung der Anzahl von Punkten auf der elliptischen Kurve nicht mehr erforderlich ist.

[0021] Dazu besteht ein Verfahren für die Erzeugung einer digitalen Signatur (c, d) einer Nachricht m darin:

– ein Modulo N und eine Basis g, einen öffentlichen Schlüssel Y und einen privaten Schlüssel x zu definieren, wobei diese Parameter N, g, Y und x durch die folgende Beziehung miteinander verbunden sind:

$$Y = g^x (\mathrm{mod}\ N)$$

– eine Hashfunktion H zu definieren, bei der die Größe des Ergebnisses S Bits enthält;
– eine Zahl r aus T Bits mit T ≥ 25 zu wählen;
– u gemäß der folgenden Beziehung zu berechnen:

$$u = g_r \cdot Y_Z,$$

wobei $Z = 2^S$
– die Verkettung von M und u durch die Funktion H zu hashen, wobei die auf diese Weise erhaltene Zahl der Wert c der Signatur ist,
– den Wert d der Signatur durch die Beziehung d = r + c·x zu berechnen.

[0022] Gemäß einem zusätzlichen Merkmal, das ein noch ein weiteres Verringern der Rechenzeit ermöglicht, wird die Nachricht M durch eine Funktion h_1 gehashed und danach mit u verkettet, wobei die Funktionen h_1 und H eventuell identisch sein können.

[0023] Gemäß einem besonderen Merkmal wird der private Schlüssel x vor dem öffentlichen Schlüssel Y definiert, wobei dieser letztere Schlüssel dann durch die Beziehung:

$$Y = g^x (\mathrm{mod}\ N)$$

berechnet wird.

[0024] Gemäß einem weiteren Merkmal wird der öffentliche Schlüssel Y vor dem privaten Schlüssel x definiert und wird für das Modulo N keine Primzahl gewählt.

[0025] Gemäß einem weiteren Merkmal ist die Zahl r eine Zufallszahl.

[0026] Die Erfindung betrifft ferner ein Verfahren zur Authentisierung der digitalen Signatur (c, d) einer Nachricht M, die gemäß der Erfindung erzeugt wird, wobei das Verfahren dadurch gekennzeichnet ist, dass es bei Kenntnis des öffentlichen Schlüssels Y, des Modulos N und der Basis g sowie der Hashfunktion H und daher des Wertes S darin besteht:

– u durch die Beziehung

$$u = g^d \cdot Y^{(Z-c)}$$

zu berechnen, wobei $Z = 2^S$
– die Verkettung von M und u durch die Funktion H zu hashen,
– zu verifizieren, dass der auf diese Weise erhaltene Wert gleich c ist, falls die Signatur authentisch ist.

[0027] Gemäß einem zusätzlichen Merkmal dieses Verfahrens wird die Nachricht M durch die Funktion h1 gehashed, bevor sie durch die Funktion H gehashed und dann mit u verkettet wird.

[0028] Weitere Vorteile und Merkmale der vorliegenden Erfindung werden deutlich in der Beschreibung einer besonderen Ausführungsform der Erfindung in Gegenüberstellung der beigefügten Figuren, unter denen:

[0029] Fig. 1 ein Schema eines Verfahrens für die Erzeugung einer digitalen Signatur zeigt,

[0030] Fig. 2 ein Schema eines Verfahrens zur Authentisierung einer digitalen Signatur, die nach dem in Fig. 1 gezeigten Verfahren erzeugt worden ist, zeigt.

[0031] Das erfindungsgemäße Verfahren wird unter anderem verwendet, um die Signatur einer Nachricht M zu erzeugen und zu prüfen. Unabhängig von den Phasen der Signatur und der Prüfung oder Verifizierung der Signatur legt eine Behörde, Garant für die Sicherheit innerhalb der Kommunikationssysteme, die folgenden allgemeinen Parameter fest:

a) Das Modulo N. Die Größe dieses Modulos ist durch Überlegungen festgelegt, die mit der Sicherheit des Algorithmus verbunden sind (gegenwärtig sind 1024 Bits eine gute Wahl). Dieses Modulo kenn mehreren Benutzern (eventuell einer großen Anzahl von Benutzern) innerhalb des Verschlüsselungssystems gemeinsam sein. Dieses Modulo kann gemäß Varianten eine Primzahl sein oder nicht, eine elliptische Kurve sein oder allgemeiner eine Gruppe sein, für die die diskrete Potenzierung schwierig umzukehren ist.

b) Die Basis g. Diese ist ein Generator der Untergruppe der durch das Modulo N bestimmten Gruppe (Modulozahl, Punkt auf der elliptischen Kurve, Element der gewählten Gruppe). Die erzeugte Untergruppe muss eine große Kardinalität besitzen ($> 2^S$, wobei S die Größe des Ergebnisses von H, der Hashfunktion, die im Folgenden erläutert wird, ist), jedoch ist diese nicht zwangsläufig die gesamte Modulo-N-Gruppe. Wie N kann auch g mehreren Benutzern gemeinsam sein.

[0032] Die Kardinalität muss sehr groß sein, jedoch ist deren Kenntnis für die Signaturalgorithmen und ihre Verifizierung nicht notwendig. Es ist dann möglich, mit der Potenzierung als Basisoperation zu arbeiten und gleichzeitig N als Produkt von Primzahlen zu wählen.

[0033] Die Parameter N und g sind Hauptparameter, die ein für allemal festgelegt werden und den Benutzergruppen gemeinsam sind. Sie sind nicht geheim, da ihre bloße Kenntnis kein Durchkreuzen der Sicherheit des Algorithmus ermöglicht.

[0034] Der Verantwortliche für das Verschlüsselungssystem ordnet jedem Benutzer ein Paar von Schlüsseln zu, die ihm gehören. Der Schlüssel x wird privater Schlüssel genannt, während Y öffentlicher Schlüssel genannt wird. Der Schlüssel x darf nur seinem Benutzer bekannt sein. Er allein verwendet diesen in der Phase der Erzeugung der Signatur. Der Schlüssel Y ist öffentlich. Er gehört zum Sender A der Nachricht. Jeder Benutzer wird, wenn er eine Nachricht von A empfängt, über die Identität des Senders informiert. Mit Hilfe eines Verzeichnisses der Schlüssel lässt sich der Schlüssel Y, der dem Sender der Nachricht und dem Benutzer zugeordnet ist, in der Phase der Verifizierung der Signatur wieder finden. Der Schlüssel Y, der der Entität A zueigen ist, wird folglich gleichzeitig von der Entität A und von der Entität B verwendet. Die zwei Schlüssel sind dadurch verknüpft, dass Y das Ergebnis der diskreten Potenzierung ist, mit g als Basis, x als Exponenten und N als Modulo. Sie sind durch die folgende Beziehung verknüpft:

$$Y = g^x (\mathrm{mod}\ N)$$

[0035] Bei den beiden Optionen, die nachstehend beschrieben werden und sich auf die Wahl von x und Y beziehen, ist der private Schlüssel allein dem Benutzer des Schlüssels bekannt. Wenn der private Schlüssel bekannt gemacht ist, geht das Problem des diskreten Logarithmus verloren, so dass das System nicht mehr sicher ist.

[0036] Gemäß der ersten Option werden der private und der öffentliche Schlüssel gewählt, indem x mit der Größe von S Bits festgelegt wird (beispielsweise S = 160, falls für H der Standard SHA gewählt wird) und danach Y anhand der obigen Beziehung berechnet wird. Diese Variante ermöglicht das Verwenden von privaten Schlüsseln kleiner Größe (beispielsweise 160 bit) und das Arbeiten auf einer elliptischen Kurve, ohne zuvor die Kardinalzahl dieser Kurve berechnen zu müssen.

[0037] Gemäß der zweiten Option wird mit dem Festlegen von Y begonnen, indem Y beispielsweise aus dem Namen des Benutzers abgeleitet wird (siehe Maurer und Yacobi, "Non-interactive public-key cryptography" EUROCRYPT'91, Lecture Notes in Computet Science, Springer-Verlag, Bd. 547, Seiten 498–507, 1991) und danach x durch eine Berechnung des diskretem Logarithmus, Modulo N, hergeleitet wird. Dieses Verfahren impliziert das Verwenden einer Zahl für N, die keine Primzahl ist, N = pq, damit die Berechnung des Logarithmus durchführbar ist. Es verlangt außerdem, die Zerlegung N = pq nicht zu verbreiten, damit die Berechnung nicht durch jedermann ausgeführt werden kann. Das hier dargestellte Signaturverfahren ermöglicht es im Gegensatz zu bekannten Verfahren, p und q nicht preiszugeben. Tatsächlich muss bei den Letzteren jeder die Kardi-

nalzahl der multiplikativen Modulo-N-Gruppe, d. h. (p – 1) (q – 1), kennen; nun aber ermöglicht die Kenntnis von (p – 1) (q – 1) das Wiederfinden von p und q.

[0038] Die für das Verschlüsselungssystem verantwortliche Autorität verlangt eine Hashfunktion, die allen Benutzern gemeinsam ist. Diese wird verwendet, um jede Zahl beliebiger Größe in eine Anzahl S von Bits umzuwandeln. Die Wahl von H und S ist von dem Algorithmus unabhängig, weshalb unterschiedslos jede bis heute bekannte Hashfunktion übernommen werden kann.

[0039] Wenn diese Vorphase abgeschlossen ist, werden fortan zwei Entitäten A und B betrachtet, die eine gesicherte Verbindung in dem Informationssystem herstellen wollen. Im ersten, anhand von Fig. 1 beschriebenen Schritt berechnet die Entität A eine digitale Signatur, die durch das Paar (c, d) repräsentiert ist, anhand der Nachricht M, die sie an die Entität B zu übertragen wünscht. Dieser Signaturschritt wird insgesamt von der Entität A ausgeführt.

[0040] Die Nachricht M, die möglicherweise sehr lang ist, wird eventuell durch eine beliebige Hashfunktion h_1 transformiert, um das Resultat m zu ergeben.

[0041] Es wird dann $Z = 2^S$ gesetzt, wobei S durch die Wahl der Hashfunktion festgelegt ist.

[0042] Es wird eine Zufallszahl r mit T Bits gewählt (wobei T fest ist und $T \geq 25$).

[0043] Mit der folgenden Beziehung wird die Zahl u berechnet:

$$u = g^r Y^Z (\text{mod } N)$$

[0044] Die Zahlen m und u werden durch ein einfaches Nebeneinanderlegen verkettet.

[0045] Das Ergebnis der Verkettung von m und u wird mit Hilfe der Hashfunktion H gehashed. Die aus den S Bits des Ergebnisses gebildete Zahl wird mit c bezeichnet.

[0046] Durch die folgende Beziehung wird die Zahl d berechnet:

$$d = r + cx$$

[0047] Das Paar (c, d) repräsentiert die Signatur der Nachricht. Diese Signatur wird zusätzlich zur Nachricht M an die Entität B gesendet. Hier beginnt der zweite Schritt, der Schritt der Authentisierung der Signatur, die in Gegenüberstellung von Fig. 2 beschrieben wird.

[0048] Nach dem Empfang der Signatur (c, d) und der Nachricht M, die ihr entspricht, kann die Nachricht M durch die Hashfunktion h_1 gehashed werden.

[0049] Es wird dann $Z = 2^S$ gesetzt, wobei S durch die Wahl der Hashfunktion festgelegt ist.

[0050] Durch die folgende Formel wird die Zahl v berechnet:

$$v = Z – c$$

[0051] Durch die Folgende Formel wird die Zahl u berechnet:

$$u = g^d Y^v (\text{mod } N)$$

[0052] Die Zahlen m und u werden verkettet.

[0053] Das Ergebnis der Verkettung wird durch die Hashfunktion H über S Bits gehashed. Das erhaltene Ergebnis wird mit c' bezeichnet.

[0054] Dann wird die durch die Entität A geschickte Signatur geprüft. Wenn c = c', dann kann der Sender der Nachricht M unter dem Vorbehalt, dass der geheime Schlüssel x der Entität A niemals preisgegeben worden ist, nur die Entität A sein. Im gegenteiligen Fall, wenn c und c' verschieden sind, ist die Nachricht verfälscht worden.

Patentansprüche

1. Verfahren für die Erzeugung einer digitalen Signatur (c, d) einer Nachricht M, das darin besteht:
– ein Modulo N und eine Basis g, einen öffentlichen Schlüssel Y und einen privaten Schlüssel x zu definieren, wobei diese Parameter N, g, Y und x durch die folgende Beziehung miteinander verbunden sind:

$$Y = g^x (\text{mod } N)$$

– eine Hashfunktion H zu definieren, bei der die Größe des Ergebnisses S Bits enthält,
– eine Zahl r aus T Bits mit $T \geq 25$ zu wählen;
wobei das Verfahren **dadurch gekennzeichnet** ist, dass es außerdem darin besteht:
– u gemäß der folgenden Beziehung zu berechnen:

$$u = g^r \cdot Y^Z,$$

wobei $Z = 2^S$
– die Verkettung von M und u durch die Funktion H zu hashen, wobei die auf diese Weise erhaltene Zahl der Wert c der Signatur ist,
– den Wert d der Signatur durch die Beziehung: $d = r + c \cdot x$ zu berechnen.

2. Verfahren für die Erzeugung einer digitalen Signatur (c, d) einer Nachricht M nach Anspruch 1, dadurch gekennzeichnet, dass die Nachricht M durch

eine Funktion h1 gehashed wird, bevor sie durch die Funktion H gehashed und dann mit u verkettet wird.

3. Verfahren für die Erzeugung einer digitalen Signatur (c, d) einer Nachricht M nach Anspruch 2, dadurch gekennzeichnet, dass die Funktionen H und h1 identisch sind.

4. Verfahren für die Erzeugung einer digitalen Signatur (c, d) einer Nachricht M nach einem der Ansprüche 1 und 3, dadurch gekennzeichnet, dass der private Schlüssel x vor dem öffentlichen Schlüssel Y definiert wird, wobei dieser letztere Schlüssel dann durch die Beziehung:

$Y = g^x (\mathrm{mod}\ N)$

berechnet wird.

5. Verfahren für die Erzeugung einer digitalen Signatur (c, d) einer Nachricht M nach einem der Ansprüche 1 und 3, dadurch gekennzeichnet, dass der öffentliche Schlüssel Y vor dem privaten Schlüssel x definiert wird und dass für das Modulo N keine Primzahl gewählt wird.

6. Verfahren für die Erzeugung einer digitalen Signatur (c, d) einer Nachricht M nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Zahl r eine Zufallszahl ist.

7. Verfahren zur Authentisierung der digitalen Signatur (c, d) einer Nachricht M, die gemäß dem Verfahren nach einem der Ansprüche 1 bis 6 erzeugt wird, dadurch gekennzeichnet, dass es bei Kenntnis des öffentlichen Schlüssels Y, des Modulos N und der Basis g sowie der Hashfunktion H und daher des Wertes S darin besteht:
– u durch die Beziehung

$u = g^d \cdot Y^{(Z-c)}$

zu berechnen, wobei $Z = 2^S$
– die Verkettung von M und u durch die Funktion H zu hashen,
– zu verifizieren, dass der auf diese Weise erhaltene Wert gleich c ist, falls die Signatur authentisch ist.

8. Verfahren zur Authentisierung der digitalen Signatur (c, d) einer Nachricht M nach Anspruch 7, dadurch gekennzeichnet, dass die Nachricht M durch die Funktion h1 gehashed wird, bevor sie durch die Funktion H gehashed und dann mit u verkettet wird.

9. Verfahren zur Authentisierung der digitalen Signatur (c, d) einer Nachricht M nach Anspruch 8, dadurch gekennzeichnet, dass die Funktionen H und h1 identisch sind.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

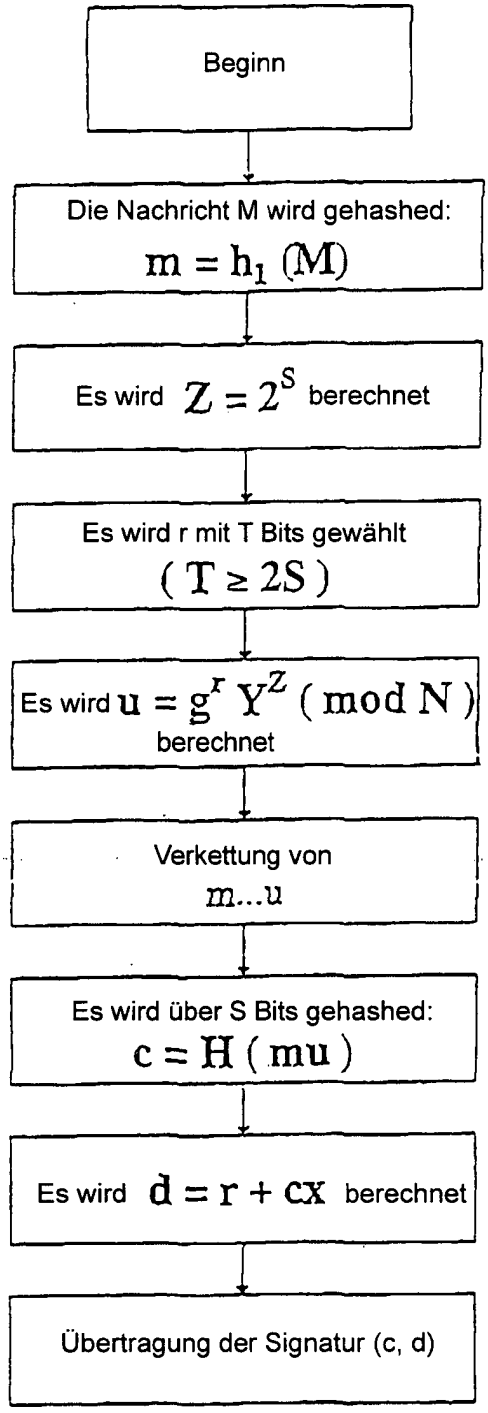

Fig. 1

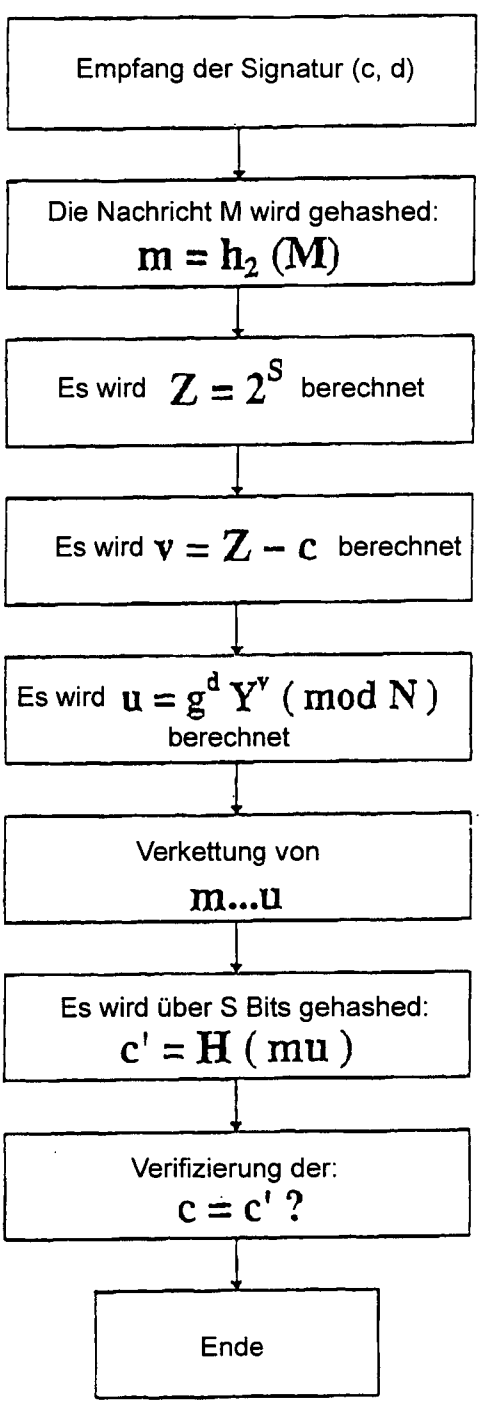
Empfang der Signatur (c, d)
50
Die Nachricht M wird gehashed:
$m = h_2 (M)$
55
Es wird $Z = 2^S$ berechnet
60
Es wird $v = Z - c$ berechnet
65
Es wird $u = g^d Y^v \pmod N$ berechnet
70
Verkettung von
m...u
75
Es wird über S Bits gehashed:
$c' = H (mu)$
80
Verifizierung der:
$c = c'$?
85
Ende

Fig. 2