(19) Deutsches Patent- und Markenamt

(10) **DE 10 2015 200 486 A1** 2016.07.14

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2015 200 486.4**
(22) Anmeldetag: **14.01.2015**
(43) Offenlegungstag: **14.07.2016**

(51) Int Cl.: ***H04L 9/00*** (2006.01)

(71) Anmelder:
Universität Rostock, 18055 Rostock, DE

(74) Vertreter:
Gulde & Partner Patent- und Rechtsanwaltskanzlei mbB, 10179 Berlin, DE

(72) Erfinder:
Salomon, Ralf, Prof., 18119 Rostock, DE

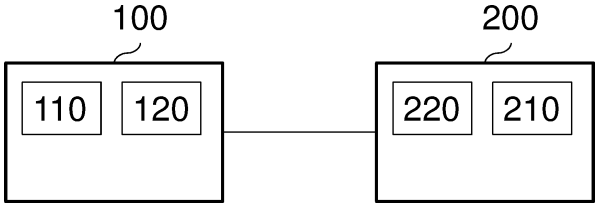
(56) Ermittelter Stand der Technik:
DE 196 40 526 A1

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren zur Bestimmung eines nachrichtabhängigen Kontrollwerts, Verfahren zur Zertifizierung der Echtheit einer Nachricht, Verfahren zur Überprüfung der Echtheit einer Nachricht, Vorrichtung zum Versenden einer Nachricht, Vorrichtung zum Empfangen einer Nachricht und Datenträger**

(57) Zusammenfassung: Die vorliegende Erfindung betrifft ein Verfahren zur Bestimmung eines nachrichtabhängigen Kontrollwerts, ein Verfahren zur Zertifizierung der Echtheit einer Nachricht, ein Verfahren zur Überprüfung der Echtheit einer Nachricht, eine Vorrichtung zum Versenden einer Nachricht, eine Vorrichtung zum Empfangen einer Nachricht und einen Datenträger.
Das Verfahren zur Bestimmung des Kontrollwerts ist dadurch gekennzeichnet, dass der Kontrollwert unter Verwendung der Nachricht und eines vorbestimmten Hilfskontrollwerts bestimmt wird.
Es ist möglich, den Hilfskontrollwert als Ergebnis einer Hashfunktion für eine Basisnachricht vorab zu berechnen. Trifft dann eine Nachricht ein, oder soll eine Nachricht versendet werden, so kann der nachrichtabhängige Kontrollwert durch Auswahl des Hilfskontrollwertes aus dem vorbestimmten Kontrollwertarray unter Verwendung der Nachricht und Bestimmung des nachrichtabhängigen Kontrollwerts unter Verwendung des ausgewählten Hilfskontrollwertes schneller algorithmisch berechnet werden, als die Hashfunktion für die Nachricht, da die Funktion, die den nachrichtabhängigen Kontrollwert in Abhängigkeit von dem ausgewählten Hilfskontrollwert bestimmt, vergleichsweise einfach sein kann.



Beschreibung

TECHNISCHES GEBIET

[0001] Die vorliegende Erfindung betrifft ein Verfahren zur Bestimmung eines nachrichtabhängigen Kontrollwerts, ein Verfahren zur Zertifizierung der Echtheit einer Nachricht, ein Verfahren zur Überprüfung der Echtheit einer Nachricht, eine Vorrichtung zum Versenden einer Nachricht, eine Vorrichtung zum Empfangen einer Nachricht und einen Datenträger.

STAND DER TECHNIK

[0002] Echtheit von Nachrichten, die versandt oder empfangen werden, kann anhand von nachrichtabhängig ermittelten Kontrollwerten zertifiziert oder überprüft werden. Ein Beispiel für Kontrollwerte sind Prüfsummen und Hashwerte. Hashwerte können anhand der Nachricht M mittels einer Hashfunktion H (M) ermittelt werden. Die Hashfunktion kann dabei von einem weiteren, beispielsweise zufällig gewählten Parameter abhängen. Alternativ oder zusätzlich kann die Hashfunktion von einem geheimen Schlüssel abhängen.

[0003] Die Kontrollwerte werden dabei auf Senderseite nachrichtabhängig berechnet und an die Nachricht angehängt. Ein Empfänger, der den geheimen Schlüssel und/oder einen weiteren Parameter kennt, kann nun anhand der Nachricht selbst die Hashwerte bestimmen und mit den an die Nachricht angehängten Hashwerten vergleichen.

[0004] Wurde nämlich die Nachricht bzw. die angehängten Kontrollwerte verändert, so sind die empfängerseitig bestimmten Kontrollwerte unterschiedlich zu den angehängten Kontrollwerten. Es ist aufgrund der Komplexität der Hashfunktion zudem praktisch unmöglich, wie die angehängten Hashwerte zusammen mit der Nachricht M so zu ändern, dass die empfängerseitig bestimmten Kontrollwerte zur veränderten Nachricht gleich den an die veränderte Nachricht angehängten veränderten Kontrollwerten sind.

[0005] Die Komplexität der Hashfunktion bewirkt jedoch auch, dass die algorithmische Berechnung zeitaufwändig ist und/oder entsprechende Rechenkapazität erfordert. Da der Hashwert zudem anhand der Nachricht bestimmt wird, kann eine Berechnung der Hashfunktion erst nach Erhalt der Nachricht erfolgen. Die Latenz zwischen dem vollständigen Empfang und der Verifizierung der Nachricht ist also groß.

OFFENBARUNG DER ERFINDUNG

[0006] Die vorliegende Erfindung befasst sich mit einer Verringerung der Latenz zwischen dem vollständigen Empfang und der Verifizierung der Nachricht sowie der hierfür benötigten Rechenkapazität.

[0007] Erfindungsgemäß wird daher ein Verfahren nach Anspruch 1 zur Bestimmung von mindestens einem nachrichtabhängigen Kontrollwert zu einer Nachricht unter Verwendung der Nachricht vorgeschlagen. Das Verfahren ist dadurch gekennzeichnet, dass der nachrichtabhängige Kontrollwert weiterhin unter Verwendung eines vorbestimmten Hilfskontrollwerts bestimmt wird.

[0008] Es ist also möglich, den Hilfskontrollwert vorab zu berechnen. Trifft dann eine Nachricht ein, oder soll eine Nachricht versendet werden, so kann der nachrichtabhängige Kontrollwert schneller berechnet werden.

[0009] In einer bevorzugten Ausführungsform wird der Hilfskontrollwert unter Verwendung der Nachricht aus einem vorbestimmten Kontrollwerte-Array ausgewählt.

[0010] Dann kann der nachrichtabhängige Kontrollwert zum Beispiel durch eine bitweise XOR-Verknüpfung des ausgewählten Hilfskontrollwertes mit mindestens einem weiteren Hilfskontrollwert bestimmt werden.

[0011] Dabei kann der oder die weiteren Hilfskontrollwerte ebenfalls unter Verwendung der Nachricht aus dem Kontrollwerte-Array ausgewählt werden.

[0012] Unterscheidet sich eine weitere Nachricht lediglich in einem Bit von der Nachricht, so kann sich ein zugehöriger, weiterer nachrichtabhängig bestimmter Kontrollwert von dem nachrichtabhängigen Kontrollwert in mindestens einem Bit unterscheiden. Dabei kann durch ein, mehrere oder alle verbleibenden Bits der Nachricht M bestimmt sein, in welchem Bit sich der weitere nachrichtabhängige Kontrollwert von dem nachrichtabhängigen Kontrollwert unterscheidet.

[0013] Erfindungsgemäß wird weiterhin ein Verfahren nach Anspruch 6 zur Zertifizierung der Echtheit einer Nachricht anhand von nachrichtabhängigen Kontrollwerten, umfassend Bestimmung von nachrichtabhängigen Kontrollwerten nach dem erfindungsgemäß vorgeschlagenen Verfahren und Anhängen der bestimmten Kontrollwerte an die Nachricht.

[0014] Erfindungsgemäß wird auch ein Verfahren nach Anspruch 7 zur Überprüfung der Echtheit einer Nachricht anhand von nachrichtabhängigen Kontrollwerten, umfassend Bestimmung von nachrichtabhängigen Kontrollwerten nach dem erfindungsgemäß vorgeschlagenen Verfahren und Vergleichen der bestimmten Kontrollwerte mit an die Nachricht angehängten Kontrollwerten.

[0015] Erfindungsgemäß wird darüber hinaus eine Vorrichtung gemäß Anspruch 8 zum Empfangen von Nachrichten vorgeschlagen, wobei die Vorrichtung konfiguriert ist, das erfindungsgemäße Verfahren zur Überprüfung der Echtheit einer Nachricht auszuführen, um die Nachrichten auf Echtheit zu überprüfen.

[0016] Erfindungsgemäß wird darüber hinaus eine Vorrichtung gemäß Anspruch 9 zum Versenden von Nachrichten vorgeschlagen, wobei die Vorrichtung konfiguriert ist, das erfindungsgemäße Verfahren zur Zertifizierung der Echtheit einer Nachricht auszuführen, um die Nachrichten auf Echtheit zu zertifizieren.

[0017] Erfindungsgemäß wird schließlich ein Datenträger gemäß Anspruch 10 vorgeschlagen. Der Datenträger umfasst auf dem Datenträger gespeicherte prozessorausführbare Anweisungen, wobei bei Ausführung der Anweisungen durch einen Prozessor eines der erfindungsgemäßen Verfahren ausgeführt wird.

ZEICHNUNGEN

[0018] Ausführungsbeispiele der Erfindung werden anhand der Zeichnungen und der nachfolgenden Beschreibung näher erläutert. Es zeigen, schematisch:

[0019] Fig. 1 Ausführungsbeispiele der erfindungsgemäßen Vorrichtungen zum Senden bzw. Empfangen von Nachrichten,

[0020] Fig. 2 ein Ausführungsbeispiel eines erfindungsgemäßen Verfahrens und

[0021] Fig. 3 ein Ausführungsbeispiel eines erfindungsgemäßen Datenträgers.

AUSFÜRUNGSFORMEN DER ERFINDUNG

[0022] Fig. 1 zeigt beispielhaft und schematisch eine Vorrichtung **100** zum Senden von Nachrichten, die mit einer Vorrichtung **200** zum Empfangen von Nachrichten verbunden ist. Die Vorrichtung **100** umfasst eine auch als Mittel zum Senden bezeichnete Sendeeinheit **120**, die konfiguriert ist, Nachrichten zur Vorrichtung **200** zu übertragen. Die Vorrichtung **200** umfasst eine auch als Mittel zum Empfang bezeichnete Empfangseinheit **220**, die konfiguriert ist, Nachrichten von der Vorrichtung **100** zu empfangen.

[0023] Eine Zertifizierungseinheit **110**, die ebenfalls von der Vorrichtung **100** umfasst ist, ist dabei konfiguriert, mindestens einen von einer zu sendenden Nachricht abhängigen Kontrollwert unter Verwendung der zu sendenden Nachricht zu bestimmen und an die zu sendende Nachricht anzuhängen.

[0024] Die Vorrichtung **200** umfasst dabei eine zugehörige Überprüfungs- oder Verifizierungseinheit **210**. Die Verifizierungseinheit **210** ist konfiguriert, einen oder mehrere von einer empfangenen Nachricht umfasste Kontrollwerte von einem Rest der Nachricht abzutrennen, eine entsprechende Anzahl weiterer Kontrollwerte unter Verwendung des Rest der Nachricht zu bestimmen und die abgetrennten Kontrollwerte mit den weiteren Kontrollwerten zu vergleichen.

[0025] Dabei sind die Verifizierungseinheit **210** und die Zertifizierungseinheit **110** so aufeinander abgestimmt, dass die weiteren Kontrollwerte, die von der Verifizierungseinheit **210** unter Verwendung des Rest der empfangenen Nachricht bestimmt werden, identisch zu den Kontrollwerten sind, die von der Zertifizierungseinheit **110** unter Verwendung der zu sendenden Nachricht bestimmt werden, sofern der Rest der empfangenen Nachricht identisch mit der zu sendenden Nachricht ist.

[0026] Insbesondere sind die Verifizierungseinheit **210** und die Zertifizierungseinheit **110** in einer beispielhaften Ausführungsform konfiguriert, mindestens einen nachrichtabhängigen Kontrollwert durch eine bitweise XOR-Verknüpfung eines Hilfskontrollwertes mit mindestens einem weiteren Hilfskontrollwert zu bestimmen. Dabei kann die Nachricht dazu verwendet werden, den Hilfskontrollwert aus einem vorbestimmten Kontrollwerte-Array auszuwählen. Zusätzlich oder alternativ kann die Nachricht dazu verwendet werden, den weiteren Hilfskontrollwert aus einem vorbestimmten Kontrollwerte-Array auszuwählen.

[0027] Die Hilfskontrollwerte im Kontrollwerte-Array können beispielsweise Bytes eines Hashwerts sein, der anhand einer Hashfunktion bestimmt ist. Die Hashfunktion kann in einem Ausführungsbeispiel mittels mindestens eines der folgenden Elemente initialisiert sein: ein Schlüssel, eine Zufallszahl und eine vorbestimmte Nachricht. Ein Beispiel einer vorbestimmten Nachricht ist die Nachricht M0, in der alle Bits den Wert ‚0' haben; natürlich kann die Nachricht auch jede andere vorher zwischen den beiden Einheiten **110** und **210** vereinbarte Bitkombination sein. Das oder die initialisierenden Elemente werden zwischen der Sendeeinheit und der Empfangseinheit im Vorfeld der Nachrichtenübertragung ausgetauscht oder vereinbart.

[0028] Die Nachricht kann beispielsweise so zur Auswahl verwendet werden, dass ihr Bitstring oder ein Teilbitstring als ein Ganzzahlwert ausgewertet und der Ganzzahlwert MODULO einer Anzahl Lh von Hilfskontrollwerten im Kontrollwertarray (Lh Bytes im Hashwert) auf den Wertebereich [0; Lh[beschränkt wird, sofern der größte in dem Bitstring/Teilbitstring darstellbare Ganzzahlenwert größer als Lh ist. Der gegebenenfalls beschränkte Ganzzahlwert VAL kann dann als ein Index zur Auswahl des Hilfskontrollwerts aus dem Kontrollwertarray verwendet werden.

[0029] Dabei gilt: X Modulo Y = X – Y·[X/Y], wobei [X/Y] der ganzzahlige Anteil von X/Y ist.

[0030] Lh kann auch so gewählt werden, dass Lh = 2^n. Dann lässt sich mit einem Teilbitstring mit n Bits ein Hilfskontrollwert im Array adressieren.

[0031] Insbesondere bei Verwenden eines Teilbitstrings können weitere Teilbitstrings zu einer entsprechenden Auswahl eines oder mehrerer weiterer Hilfskontrollwerte aus dem Kontrollwertearray verwendet werden.

[0032] Zu einer Nachricht können mehrere von der Nachricht abhängige Kontrollwerte bestimmt werden, beispielsweise kann die Anzahl der bestimmten nachrichtabhängigen Kontrollwerte der Anzahl Lh oder einer Anzahl Lm von Bits in der Nachricht entsprechen.

[0033] Dabei kann jeder der nachrichtabhängigen Kontrollwerte durch eine XOR-Verknüpfung eines zugehörigen Hilfskontrollwerts mit einem oder mehreren zugehörigen weiteren Hilfskontrollwert(en) bestimmt werden.

[0034] Fig. 2 zeigt beispielhaft und schematisch ein Verfahren zur Bestimmung nachrichtabhängiger Kontrollwerte.

[0035] Das gezeigte Verfahren umfasst einen Initiierungsschritt S1, einen Verknüpfungsschritt S2, einen Variablenschaltschritt S3 und einen Entscheidungsschritt S4.

[0036] Im Schritt S1 werden eine Zählervariable i und mindestens zwei Indexvariablen initialisiert. Mindestens eine der Indexvariablen wird dabei unter Verwendung eines Ganzzahlwertes initialisiert, der aus einem (Teil-)Bitstring der Nachricht gewonnen wurde.

[0037] In Schritt S2 werden Hilfskontrollwerte miteinander verknüpft, beispielsweise bitweise XOR-verknüpft. Dabei werden die Hilfskontrollwerte aus einem Kontrollwertarray anhand der Indexvariablen ausgewählt. Das Ergebnis ist ein nachrichtabhängiger Kontrollwert.

[0038] In Schritt S3 werden die Zählervariable i und die Indexvariablen weitergeschaltet. Mindestens eine der Indexvariablen wird dabei um Eins erhöht, sofern durch das Erhöhen die eine Indexvariable nicht gleich der Anzahl Lh der Hilfskontrollwerte im Kontrollwertarray wird, in welchem Fall die eine Indexvariable auf Null gesetzt wird, und mindestens eine andere der Indexvariablen wird dabei um Eins erniedrigt, sofern durch das Erniedrigen die Indexvariable nicht kleiner Null wird, in welchem Fall die eine andere Indexvariable auf Lh – 1 gesetzt wird. Die Zählervariable wird um Eins erhöht. Die Reihenfolge der Schritte S2 und S3 ist frei wählbar, muss jedoch bei der Initialisierung und/oder im folgenden Schritt S4 berücksichtigt werden.

[0039] In Schritt S4 wird geprüft, ob die Zählervariable kleiner als ein Looplängenwert ist. Der Looplängenwert kann etwa der Anzahl Lh der Hilfskontrollwerte im Kontrollwertarray oder der Anzahl Mh der Bits in der Nachricht entsprechen. Er kann insbesondere der größeren der beiden Anzahlen Lh, Mh entsprechen. Ist die Zählervariable kleiner als der Looplängenwert, so kehrt das Verfahren zu Schritt S2 zurück. Andernfalls endet das Verfahren.

[0040] In einer ersten beispielhaften Ausführungsform wird zur Bestimmung des i-ten Kontrollwertes der i-te Hilfskontrollwert aus dem Kontrollwertarray mit dem k-ten Hilfskontrollwert aus dem Kontrollwertarray bitweise XOR verknüpft, wobei die Indexvariable k unter Verwendung von VAL2 und Lh bestimmt wird. Beispielsweise wird k = (VAL – i) Modulo Lh gesetzt.

[0041] Die erste beispielhafte Ausführungsform ist besonders vorteilhaft, wenn die Nachricht, deren Echtheit zertifiziert/verifiziert werden soll, aus maximal so vielen Bits besteht, wie für das Adressieren eines der Hilfskontrollwerte aus einem Kontrollwertarray benötigt werden.

[0042] In einer zweiten beispielhaften Ausführungsform wird die Nachricht in zwei disjunkte Teilbitstrings zerlegt, die als Ganzzahlwerte VAL1, VAL2 ausgewertet und gegebenenfalls auf den auf den Wertebereich [0; Lh[beschränkt werden.

[0043] Dann wird zur Bestimmung des i-ten Kontrollwertes der j-te Hilfskontrollwert aus dem Kontrollwertarray mit dem k-ten Hilfskontrollwert aus dem Kontrollwertarray bitweise XOR verknüpft, wobei die Indexvariable k unter Verwendung von i, VAL2 und Lh und die weitere Indexvariable j unter Verwendung von i, VAL1 und Lh bestimmt wird. Beispielsweise wird j = (VAL1 + i) Modulo Lh und k = (VAL2 – i) Modulo Lh gesetzt.

[0044] Die zweite beispielhafte Ausführungsform ist besonders vorteilhaft, wenn die Nachricht, deren Echtheit zertifiziert/verifiziert werden soll, aus maximal doppelt so vielen Bits besteht, wie für das Adressieren eines der Hilfskontrollwerte aus einem Kontrollwertarray benötigt werden.

[0045] In einer dritten beispielhaften Ausführungsform wird die Nachricht in drei disjunkte Teilbitstrings zerlegt, die als Ganzzahlwerte VAL1, VAL2, VAL3 ausgewertet und gegebenenfalls auf den auf den Wertebereich [0; Lh[beschränkt werden.

[0046] Dann wird zur Bestimmung des i-ten Kontrollwertes der j-te Hilfskontrollwert aus dem Kontrollwertarray mit dem k-ten Hilfskontrollwert aus dem Kontrollwertarray und mit dem mit dem l-ten Hilfskontrollwert aus dem Kontrollwertarray bitweise XOR verknüpft, wobei die Indexvariable k unter Verwendung von i, VAL2 und Lh, die weitere Indexvariable j unter Verwendung von i, VAL1 und Lh und die noch weitere Indexvariable l unter Verwendung von i, VAL3 und Lh bestimmt werden. Beispielsweise wird j = (VAL1 + i) Modulo Lh, k = ((VAL2 – HK0 – i) Modulo Lh und l = (VAL3 – i) Modulo Lh gesetzt, wobei HK0 der Hilfskontrollwert im Kontrollwertarray zum Index Null ist.

[0047] Die dritte beispielhafte Ausführungsform ist besonders vorteilhaft, wenn die Nachricht, deren Echtheit zertifiziert/verifiziert werden soll, aus maximal dreimal so vielen Bits besteht, wie für das Adressieren eines der Hilfskontrollwerte aus einem Kontrollwertarray benötigt werden.

[0048] Ein besonderer Vorzug der ersten bis dritten beispielhaften Ausführungsform ist, dass die nachrichtabhängigen Kontrollwerte empfängerseitig in der Reihenfolge des Eintreffens der Nachrichtenteile mittels einfacher XOR-Operation auf Korrektheit überprüft werden können.

[0049] In einer vierten beispielhaften Ausführungsform wird die Nachricht in m Teilbitstrings mit je n Bits zerlegt, wobei $2^{(n-1)} < Lh \leq 2^n$ bevorzugt $Lh = 2^n$ ist. Zu jedem Teilbitstring wird ein Kontrollwert ermittelt. Dazu werden zuerst die nachrichtabhängigen Kontrollwerte initialisiert, indem der i-te nachrichtabhängige Kontrollwert gleich dem (i Modulo Lh)-ten Hilfskontrollwert gesetzt wird.

[0050] Dann wird unter Verwendung einer Zählervariable $0 \leq i < m$ ein Hilfskontrollwert aus dem Kontrollwertarray ausgewählt und unter Verwendung des ausgewählten Hilfskontrollwert und des i-ten Teilstrings eine Indexvariable j bestimmt.

[0051] Schließlich wird der j-te nachrichtabhängige Kontrollwert mit dem ausgewählten Hilfskontrollwert verknüpft, beispielsweise bitweise XOR-verknüpft. Mit dem Ergebnis wird dann der j-te Kontrollwert aktualisiert.

[0052] Die vierte beispielhafte Ausführungsform ist besonders vorteilhaft, wenn die Nachricht, deren Echtheit zertifiziert/verifiziert werden soll, aus mehr als dreimal so vielen Bits besteht, wie für das Adressieren eines der Hilfskontrollwerte aus einem Kontrollwertarray benötigt werden.

[0053] In der vierten beispielhaften Ausführungsform werden die einzelnen Kontrollwerte anhand der Hilfskontrollwerte im Kontrollwertarray initialisiert und anschließend in einer Reihenfolge verändert, die sich aus den Nachrichtenwerten sowie den Werten des Kontrollwertarray ergibt. Bei einem nachrichtabhängigen Kontrollwert mit 1024 Bits liegt die Sicherheit gegenüber einer Ein-Bit Manipulation bei $1:2^{30}$

[0054] **Fig.** 3 zeigt einen exemplarischen Datenträger **300** in Form einer optischen Disk, zum Beispiel eine CD, DVD oder eine Blu-ray-Disk. Auf dem Datenträger sind prozessorausführbare Anweisungen gespeichert. Bei Ausführung der Anweisungen durch einen Prozessor wird eines der Ausführungsbeispiele des erfindungsgemäßen Verfahrens ausgeführt.

[0055] Die prozessorausführbaren Anweisungen, bei deren Ausführung durch einen Prozessor eines der Ausführungsbeispiele des erfindungsgemäßen Verfahrens ausgeführt wird, können auf anderen Datenträgern, beispielsweise auf einer lokal oder remote gehosteten Festplatte oder auf einem USB-Stick gespeichert sein.

[0056] Ein Vorteil der vorliegenden Erfindung ist, dass die Kontrollwerte vorausberechnet werden können und die eigentliche Prüfung einfach ist. Dies gewährt gegenüber dem nachrichtabhängigen Berechnen von Hash-Werten einen Geschwindigkeits- und/oder Speicherplatzvorteil. Ein weiterer Vorteil ist, dass sich die Erfindung auf bekannte Hash-Funktionen wie SHA-1, SHA-256 etc. aufbauen lässt.

[0057] Beispielhafte Ausführungsformen des Verfahrens können, müssen jedoch nicht, auf folgenden Verfahren aufbauen:
Vor dem eigentlichen Senden der Nachricht schickt eine Empfänger E eine Zufallszahl r1 an den späteren Sender S der Machricht M. Hierzu verwenden beide Kommunikationspartner einen vorher festgelegten Hash-Algorithmus, beispielsweise SHA-1 oder SHA-256, sowie einen geheimen Schlüssel, den beide Partner in einer initialen Konfigurationsphase ausgetauscht haben. Diese Form der Hash-Anwendung ist auch als Salted-Hashes bekannt.

[0058] Dann können Sender S und Empfänger E zu einer symbolischen Nachricht M0 und Unter Verwendung der zuvor ausgetauschten Zufallszahl r1 einen Hash-Wert h0 errechnen. Die symbolische Nachricht M0 kann beispielsweise die leere Nachricht (alle Nachrichtenbits haben den Wert 0) oder jede beliebige andere Nachricht sein, auf die sich beide Kommunikationspartner verständigt haben.

[0059] Für die Berechnung dieses (ersten) Hash-Wertes muss noch nicht einmal die Nachricht M0 verwendet werden. Es reicht aus, die zuvor ausgetauschte Zufallszahl zu verwenden. Die Berechnung kann im vor dem Ausstauch der eigentlichen Nachricht M erfolgen.

[0060] Wird nun eine Nachricht ausgetauscht, können die Kommunikationspartner eine im Vergleich zur Hash-Funktion einfach berechenbare Funktion f(M, h) verwenden, die aus dem ersten Hash-Wert h und der eigentlichen Nachricht einen modifizierten Hash-Wert hm berechnet. Diese Funktion f() kann dabei auf weitere Geheimnisse bzw. Hash-Werte zurückkreifen, die beide Kommunikationspartner im Voraus (also vor dem Versenden der eigentlichen Nachricht) berechnen können.

[0061] Es ist vorteilhaft aber nicht notwendig, wenn die Funktion F so gewählt ist, dass Änderung eines Bits der Nachricht M zu mehreren Änderungen des modifizierten Hash-Wertes hm führt, um so besonders gute Fälschungssicherheit zu erreichen.

[0062] Weiterhin ist es vorteilhaft aber nicht notwendig, wenn die Funktion F so gewählt ist, dass in die Bestimmung des modifizierten Hash-Wertes hm möglichst viele oder alle Bits der eigentlichen Nachricht einfließen, da so das Erstellen einer gefälschten Nachricht mit passendem modifizierten Hash-Wert besonders schwer wird.

[0063] Weiterhin ist es vorteilhaft aber nicht notwendig, wenn die Funktion F so gewählt ist, dass ein externer Zuhörer nicht wissen kann, an welchen Stellen sich der modifizierte Hash-Wert hm ändert, wenn sich ein bestimmtes Bit der eigentlichen Nachricht ändert, da so das Erstellen einer gefälschten Nachricht mit passendem modifizierten Hash-Wert besonders schwer wird.

Patentansprüche

1. Verfahren zur Bestimmung von mindestens einem nachrichtabhängigen Kontrollwert zu einer Nachricht unter Verwendung der Nachricht, **dadurch gekennzeichnet,** dass der nachrichtabhängige Kontrollwert weiterhin unter Verwendung eines Hilfskontrollwerts bestimmt wird.

2. Verfahren nach Anspruch 1, wobei der Hilfskontrollwert unter Verwendung der Nachricht aus einem vorbestimmten Kontrollwerte-Array ausgewählt wird.

3. Verfahren nach Anspruch 2, wobei der nachrichtabhängige Kontrollwert durch eine bitweise XOR-Verknüpfung des ausgewählten Hilfskontrollwertes mit mindestens einem weiteren Hilfskontrollwert bestimmt wird

4. Verfahren nach Anspruch 3, wobei der oder die weiteren Hilfskontrollwerte ebenfalls unter Verwendung der Nachricht aus dem Kontrollwerte Array ausgewählt werden.

5. Verfahren nach einem der Ansprüche 1–4, wobei ein weiterer, zu einer weiteren Nachricht, die sich lediglich in einem Bit von der Nachricht unterscheidet, nachrichtabhängig bestimmter Kontrollwert sich von dem nachrichtabhängigen Kontrollwert in mindestens einem Bit unterscheidet, wobei das mindestens eine Bit, in welchem sich der weitere nachrichtabhängige Kontrollwert von dem nachrichtabhängigen Kontrollwert unterscheidet, durch ein, mehrere oder alle verbleibenden Bits der Nachricht M bestimmt ist.

6. Verfahren zur Zertifizierung der Echtheit einer Nachricht anhand von nachrichtabhängigen Kontrollwerten, umfassend Bestimmen von nachrichtabhängigen Kontrollwerten nach einem der vorangehenden Ansprüche und Anhängen der bestimmten Kontrollwerte an die Nachricht

7. Verfahren zur Überprüfung der Echtheit einer Nachricht anhand von nachrichtabhängigen Kontrollwerten, umfassend Bestimmen von Kontrollwerten nach einem der Ansprüche 1–5 und Vergleichen der bestimmten Kontrollwerte mit an die Nachricht angehängten Kontrollwerten.

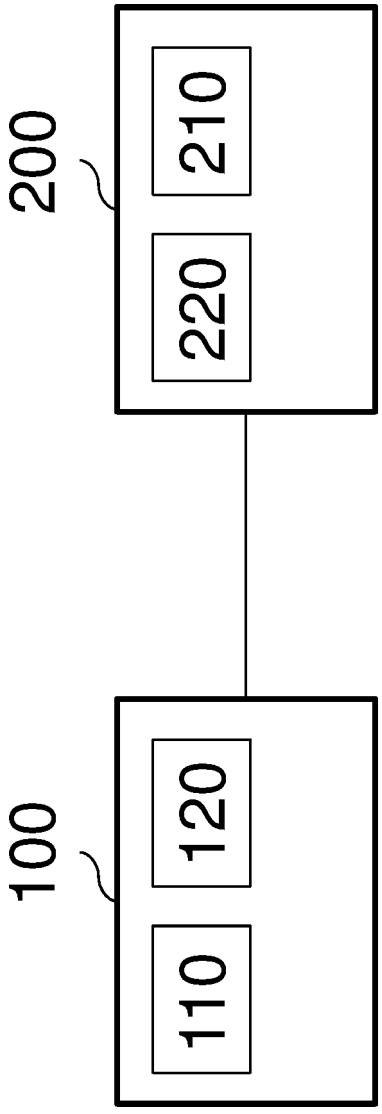
8. Vorrichtung zum Empfangen von Nachrichten, wobei die Vorrichtung konfiguriert ist, dass Verfahren gemäß Anspruch 7 auszuführen, um die Nachrichten auf Echtheit zu überprüfen.

9. Vorrichtung zum Versenden von Nachrichten, wobei die Vorrichtung konfiguriert ist, das Verfahren gemäß Anspruch 6 auszuführen, um die Nachrichten auf Echtheit zu zertifizieren.

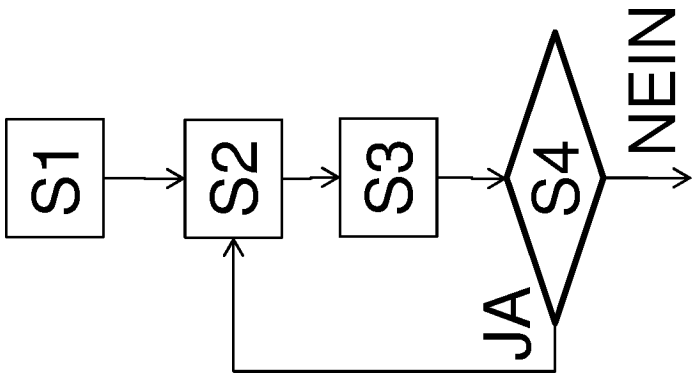
10. Datenträger umfassend auf dem Datenträger gespeicherte prozessorausführbare Anweisungen, wobei bei Ausführung der Anweisungen durch einen Prozessor ein Verfahren ausgeführt wird, **dadurch gekennzeichnet,** dass das Verfahren nach einem der Ansprüche 1 bis 7 ausgeführt wird.

Es folgen 3 Seiten Zeichnungen

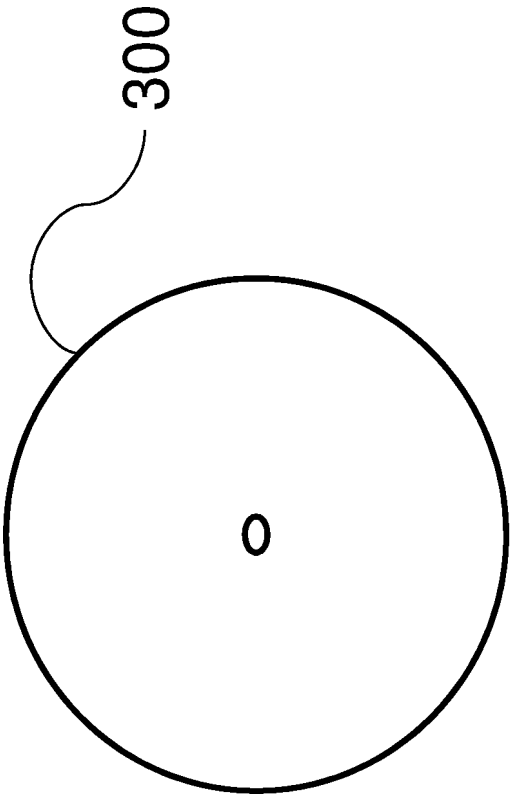
Anhängende Zeichnungen



Figur 1



Figur 2



Figur 3