(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
25. November 2010 (25.11.2010)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2010/133266 A1

(51) Internationale Patentklassifikation:
G06F 21/00 (2006.01) *H04L 9/32* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2010/001356

(22) Internationales Anmeldedatum:
4. März 2010 (04.03.2010)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2009 022 233.2 20. Mai 2009 (20.05.2009) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **FEUSTEL, Dietmar** [DE/DE]; Parksiedlung 8, 04451 Panitzsch (DE). **TOPF, Birgit** [DE/DE]; Zum Herrnholz 33, 04435 Schkeuditz (DE).

(72) Erfinder; und
(71) Anmelder : **JENTZSCH, Rolf** [DE/DE]; Falladastrasse 31, 04159 Leipzig (DE).

(74) Anwälte: **BOCKHORNI, Josef** et al.; Bockhorni und Kollegen, Zimmerstrasse 3, 04109 Leipzig (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

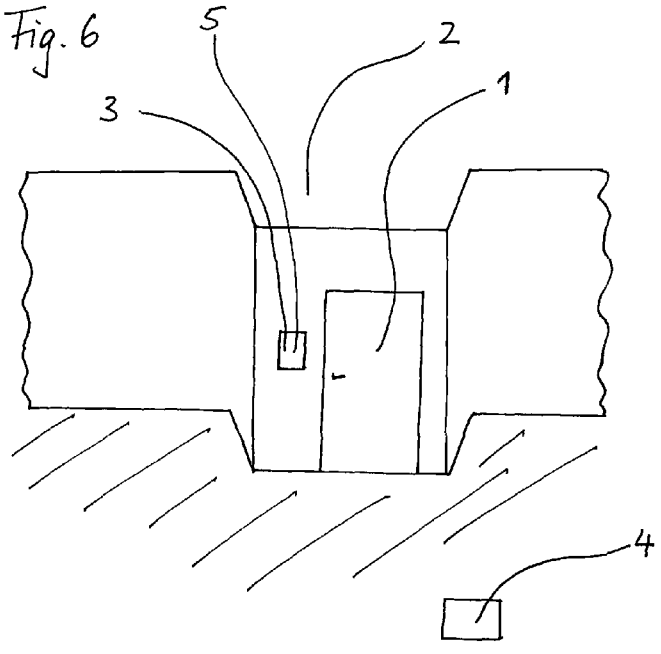
(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

(54) Title: UNIQUE IDENTIFIER, METHOD FOR PROVIDING SAID UNIQUE IDENTIFIER AND USE OF SAID UNIQUE IDENTIFIER

(54) Bezeichnung : ORIGINALKENNUNG, VERFAHREN ZUR BEREITSTELLUNG DER ORIGINALKENNUNG SOWIE VERWENDUNG DER ORIGINALKENNUNG



(57) Abstract: The invention relates to a unique identifier (OK) which substantially prevents product forgery, the unique identifier (OK) being very cost-effective to produce. The unique identifier (OK) is suitable not only for use as a product identifier but also for purposes of authorization, for example for securing physical or electronic accesses, such as doors (1), computer programs or the like.

(57) Zusammenfassung: Mit der vorliegenden Erfindung wird eine Originalkennung (OK) bereitgestellt, die Produktfälschungen weitgehend verhindert, wobei die Originalkennung (OK) in ihrer Herstellung sehr kostengünstig ist. Die Originalkennung (OK) eignet sich nicht nur zur Verwendung als Produktkennzeichnung, sondern auch zum Autorisierungsnachweis, beispielsweise bei der Sicherung von räumlichen oder elektronischen Zugängen, wie Türen (1), Computerprogrammen und dgl.

WO 2010/133266 A1

Originalkennung, Verfahren zur Bereitstellung der Originalkennung sowie Verwendung der Originalkennung

Die vorliegende Erfindung betrifft eine Verfahren zur Herstellung einer Originalkennung, Verwendungen dieser Originalkennung, die Originalkennung selbst, sowie eine Einrichtung und ein Computerprogrammprodukt zur Durchführung des Verfahrens.

Produktpiraterie hat im Wirtschaftsverkehr einen bedeutenden Stellenwert eingenommen. Nach aktuellen Angaben entfallen durch Produktpiraterie, illegale Überproduktion, Parallel- und Re-Importe mittlerweile bereits 10 % des Welthandels auf Plagiate oder Fälschungen, was einem internationalen Schaden von über 300 Milliarden Euro gleichgesetzt wird. In Deutschland sind nach dem Verband deutscher Maschinen- und Anlagenbau rund zwei Drittel der Hersteller von Investitionsgütern von Produktpiraterie betroffen.

Diese Produktpiraterie hat natürlich auch bedeutende Auswirkungen auf den Arbeitsmarkt, wobei allein in Deutschland nach Schätzungen des Justizministeriums jährlich ca. 50.000 Arbeitsplätze auf Grund von Produktpiraterie verloren gehen. Im gesamteuropäischen Raum sollen insgesamt sogar 300.000 Arbeitsplätze betroffen sein.

Dabei sind die Hersteller von Investitionsgütern vor allem dadurch durch Produktpiraterie bedroht, dass sie erhebliche Investitionsvorleistungen erbringen mussten, um ihre Qualitätsprodukte zu entwickeln, zu testen, herzustellen und zu bewerben. Diese Investitionen hat ein Plagiateur nicht, so dass er sich an den Erfolg des Originals anhängend erhebliche Kosten spart und damit wesentlich höhere Gewinnspannen hat – zumal wenn die Plagiate minderwertiger Qualität sind – oder zu erheblich günstigeren Preisen anbieten kann.

Eine weitere Bedrohung liegt darin, dass diese Hersteller ihren guten Ruf verlieren, wenn Plagiate minderwertiger Qualität und Sicherheit auf den Markt gelangen, aber nicht gleich als Plagiate erkennbar sind, sondern den Original-Herstellern zugeordnet werden.

Ein weiteres großes Problem neben den wirtschaftlichen Schäden der Produktpiraterie besteht darin, dass unter Umständen mit Plagiaten auch Unfall- und Gesundheitsgefahren verbunden sind. Dies ist insbesondere dann der Fall,

BESTÄTIGUNGSKOPIE

wenn Plagiate nicht nach den gleichen Standards gefertigt werden wie die Originale. Zu nennen ist hier besonders die Arzneimittelbranche, aber auch in anderen sicherheitsrelevanten Branchen, wie dem Maschinenbau, können minderwertige Plagiate gravierende Folgen haben.

Das Ziel der Hersteller von Investitionsgütern besteht somit darin, Produktpiraterie weitestgehend zu verhindern. Hierzu wurden verschiedene Schutztechnologien bzw. technische Sicherungsmittel entwickelt, wie z. B. Hologramme, Sicherheitsetiketten, Mikrofarbcodes, digitale Wasserzeichen und dgl. mehr, wobei das gegenwärtige Hauptaugenmerk darauf liegt, Produktkennzeichnungen zu entwickeln, deren Merkmale technisch nicht fälschbar sind.

Beispielsweise werden für modernes Papiergeld eine Vielzahl von Sicherheitsmerkmalen verwendet, die die Fälschung unmöglich machen sollen. Dazu gehören am Beispiel von Euro-Banknoten, die Verwendung von Spezialpapier, optischen Sicherheitsmerkmalen, wie Wasserzeichen, Anti-Kopierraster, Melierfasern, Sicherheitsfaden, Sonderfarben, Irisdruck, Folienelementen, Hologrammen, Mikro-Perforation, Mikro-Schrift, fluoreszierende Farben, optisch veränderliche Tinte, Glanzeffekte, Durchsichtfenster und Durchsichtregister, haptische Sicherheitsmerkmale wie Papiergefühl und Prägung sowie akustische Sicherheitsmerkmale hinsichtlich des Klangs der Banknoten beim Knüllen oder Reiben. Zusätzlich werden noch von Automaten erkennbare Merkmale eingesetzt, wie Infrarotfarbe, magnetische Elemente, elektrische Leitfähigkeit und dgl. mehr.

Nachteilig an diesen Produktkennzeichnungen ist es aber, dass ihre Fälschungssicherheit immer nur solange besteht, solang bezüglich der Produktkennzeichnung ein Technologievorsprung gegenüber den Produktpiraten gegeben ist, der jedoch erfahrungsgemäß nur von kurzer Dauer ist. Außerdem sind solche vielschichtigen Produktkennzeichnungen relativ kostenintensiv und somit nur bei hochpreisigen Produkten sinnvoll einsetzbar. Schließlich lässt sich auch eine Fälschung von besonders sicheren Produktkennzeichnungen nicht vollständig verhindern, zumal es bei sehr komplexen Produktkennzeichnungen sowohl für Verbraucher als auch für Verkäufer sehr schwierig ist, zu erkennen, ob es sich um eine originale Produktkennzeichnung handelt oder um eine Fälschung.

Die Aufgabe der vorliegenden Erfindung besteht daher darin, Originalkennungen bereitzustellen, die Produktfälschungen weitgehend verhindern, wobei die Originalkennung in ihrer Herstellung sehr kostengünstig sein soll. Insbe-

sondere soll sich die Originalkennung nicht nur zur Verwendung als Produktkennzeichnung eignen, sondern auch zum Autorisierungsnachweis, beispielsweise bei der Sicherung von räumlichen oder elektronischen Zugängen, wie Türen, Computerprogrammen und dgl.

Diese Aufgabe wird gelöst mit dem Verfahren zur Bereitstellung einer Originalkennung nach Anspruch 1 der Verwendung der Originalkennung zur Produktkennzeichnung nach Anspruch 9, der Verwendung der Produktkennzeichnung zur Autorisierung nach Anspruch 12, der Originalkennung nach Anspruch 14 und einem Computerprogrammprodukt nach Anspruch 15. Vorteilhafte Weiterbildungen sind in den abhängigen Unteransprüchen angegeben.

Die Erfinder haben erkannt, dass der Weg, das Fälschen an sich zu erschweren, ein kostenintensiver und auf Grund des technischen Fortschritts auch aussichtsloser Weg ist, um Produktfälschungen zu verhindern bzw. Autorisierungen abzusichern. Deshalb wird erfindungsgemäß ein anderer Weg gegangen, der darin besteht, bei der Motivation des Fälschers anzusetzen, nämlich seinen Gewinn soweit zu minimieren, dass kein Anlass mehr für eine Fälschung gegeben ist. Im Einzelfall könnte also weiterhin eine Produkt-Fälschung möglich sein, jedoch sind die Kosten für diese Fälschungen im großen Stil so hoch, dass hierfür kein Anlass mehr besteht. Das Erschleichen einer Autorisierung ist dagegen ganz unmöglich gemacht.

Das erfindungsgemäße Verfahren zur Bereitstellung einer Originalkennung für einen Gegenstand, wie ein Produkt, eine Autorisierung für einen Zugang oder dgl., zeichnet sich dadurch aus, dass es zumindest die folgenden Schritte umfasst: (a) zur Verfügung stellen eines Hauptschlüssels, (b) Erzeugung eines ersten zufälligen Sitzungsschlüssels und (c) Mischen des Hauptschlüssels mit dem ersten zufälligen Sitzungsschlüssel.

Dieses Ziel wird also dadurch erreicht, dass die Originalkennung im Wege einer Verschlüsselung erzeugt wurde, wobei ein Hauptschlüssel zur Verfügung gestellt wird und nach Erzeugung eines ersten zufälligen Sitzungsschlüssels der Hauptschlüssel mit diesem ersten zufälligen Sitzungsschlüssel gemischt wird. Dadurch kann beispielsweise der Hersteller von Investitionsgütern basierend auf einem einzigen Hauptschlüssel, beispielsweise einer physikalischen Zufallszeichenfolge, mit Hilfe von ersten zufälligen Sitzungsschlüsseln zahlreiche Originalkennungen für die zu verkaufenden Produkte bereitstellen. Der Hersteller muss nun nur noch diese ersten zufälligen Sitzungsschlüssel abspeichern und kann dabei gegebe-

nenfalls auch noch registrieren, welchen Vertriebsweg das mit dem entsprechenden Sitzungsschlüssel und der daraus hergestellten Originalkennung versehene Produkt genommen hat. Ein Wiederverkäufer oder Verbraucher des Produkts kann dann beispielsweise durch Anruf bei einer Hotline des Herstellers leicht herausfinden, ob es sich um ein Originalprodukt handelt, wozu er die Originalkennung an den Hersteller übermittelt, und dieser überprüft, ob diese Originalkennung sich mit dem vorgegebenen Hauptschlüssel und den gespeicherten Sitzungsschlüsseln erzeugen lässt und ob gegebenenfalls dem verwendeten Sitzungsschlüssel ein Vertriebsweg zugeordnet ist, der dem Vertriebsweg entspricht, den der Zwischenhändler bzw. Endverbraucher angibt.

Somit lässt sich zwar die einzelne Produkt-Fälschung nicht verhindern, da eine solche Originalkennung natürlich einfach kopiert werden könnte, jedoch würde eine Fälschung im großen Stil schnell auffliegen, da jede Originalkennung nur einmal vergeben wird.

Insbesondere für die Verwendung der Originalkennung zur Autorisierung kann in Schritt (b) vorteilhaft vorgesehen sein, dass der erste zufällige Sitzungsschlüssel dem Verwender verschlüsselt zur Verfügung gestellt wird. Dabei kann es sich bei dem Verwender um eine natürliche Person handeln aber auch um eine Vorrichtung oder Einrichtung. Zur Verschlüsselung des ersten zufälligen Sitzungsschlüssels wird ein erster Verwenderschlüssel bereitgestellt, und der erste zufällige Sitzungsschlüssel wird mit dem ersten Verwenderschlüssel gemischt. Der erste Verwenderschlüssel ist dabei auf den vorgesehenen Verwender abgestimmt und nur dieser Verwender oder eine Gruppe von berechtigten Verwendern hat Kenntnis von diesem ersten Verwenderschlüssel. Der Verwender nimmt dann den ihm zugeteilten Verwenderschlüssel und bestimmt den ersten zufälligen Sitzungsschlüssel durch Entmischen mit seinem zugeteilten Verwenderschlüssel. Wenn sein Verwenderschlüssel mit dem ersten Verwenderschlüssel übereinstimmt, dann kann der Verwender den ersten zufälligen Sitzungsschlüssel bestimmen und daraus die Originalkennung erzeugen.

In einer bevorzugten Ausgestaltung ist vorgesehen, dass weiterhin folgende Schritte vorgenommen werden: d) zur Verfügung stellen eines Gegenstandsschlüssels und e) Mischen des Gegenstandsschlüssels mit dem Ergebnis von Schritt c), wobei bevorzugt weiterhin das Ergebnis von Schritt c) oder Schritt d) auf eine dem Gegenstandsschlüssel entsprechende Länge mit einem vorgegebenen Reduktionsalgorithmus reduziert wird. Es

ist dabei also vorgesehen, dass ein Gegenstandsschlüssel zur Verfügung gestellt wird und das Ergebnis der Mischung von ersten zufälligem Sitzungsschlüssel und Hauptschlüssel mit dem Gegenstandsschlüssel gemischt wird. Auf diese Weise kann jeder Originalkennung eine Information über das Produkt beigefügt werden, wobei diese Informationen insbesondere Informationen über die Art, die Menge, den Vertriebsweg und dgl. sind. In einer vorteilhaften Weiterbildung ist vorgesehen, dass die Länge der Originalkennung auf eine den Gegenstandsschlüssel entsprechende Länge mit Hilfe eines vorgegebenen Reduktionsalgorithmus reduziert wird. Unabhängig von dem Gegenstandsschlüssel kann natürlich auch das Ergebnis des Mischens des Hauptschlüssels mit dem ersten zufälligen Sitzungsschlüssel schon auf eine bestimmte Länge reduziert werden mit Hilfe eines vorgegebenen Reduktionsalgorithmus.

In einer weiteren bevorzugten Ausgestaltung ist vorgesehen, dass weiterhin folgende Schritte vorgenommen werden: f) zur Verfügung stellen eines zweiten Verwenderschlüssel, der bevorzugt identisch dem ersten Verwenderschlüssel ist und der charakteristisch ist für die Benutzung der Originalkennung, insbesondere dessen Verwender, g) Erzeugung einer Kennung durch Mischung des ersten zufälligen Sitzungsschlüssels und des zweiten Verwenderschlüssel und h) Verbindung der Ergebnisse von Schritt c) oder Schritt e) und der Kennung zur Originalkennung, wobei bevorzugt die Kennung dem Ergebnis voran- oder nachgestellt wird. Es ist dabei also vorgesehen, dass ein zweiter Verwenderschlüssel zur Verfügung gestellt wird, der charakteristisch ist für die Benutzung der Originalkennung, insbesondere dessen Verwender, beispielsweise also für den Hersteller des Produkts. Mit Hilfe dieses zweiten Verwenderschlüssels, der bevorzugt identisch mit dem ersten Verwenderschlüssels ist, wird eine Kennung durch Mischen des ersten zufälligen Sitzungsschlüssels und des zweiten Verwenderschlüssels erzeugt. Diese Kennung wird dann mit dem Ergebnis der Mischung von Hauptschlüssel und ersten zufälligen Sitzungsschlüssel bzw. der Mischung von Hauptschlüssel, ersten zufälligen Sitzungsschlüssel und Gegenstandsschlüssel verbunden, um die Originalkennung zu bilden. Bevorzugt wird dabei die Kennung voran- oder nachgestellt, wobei allerdings auch vorgegebene Mischalgorithmen verwendet werden können. Auf diese Weise muss der Hersteller nicht mehr die einzelnen ersten zufälligen Sitzungsschlüssel speichern, sondern der verwendete erste zufällige Sitzungsschlüssel kann mit Hilfe des zweiten Verwenderschlüssels, der dem Hersteller bekannt ist, jeder Originalkennung zugeordnet werden, wodurch leicht ermittelt werden kann, ob die Originalkennung echt und in Bezug auf das Produkt, den Autorisierungsversuch oder dgl. zulässig ist.

Besonders bevorzugt ist vorgesehen, dass weiterhin folgende Schritte vorgenommen werden: i) das Ergebnis aus Schritt c) oder e) in zwei Teillängen aufgeteilt wird, wobei eine Teillänge mit der anderen Teillänge gemischt wird und j) das Ergebnis aus Schritt c) oder e) wird mit dem Ergebnis von Schritt i) gemischt. Natürlich können auch die anderen Schlüssel und/oder Mischergebnisse zu modifiziert werden. Es werden also Hauptschlüssel, erster Verwenderschlüssel, zweiter Verwenderschlüssel und/oder Gegenstandsschlüssel und/oder die vorgenannten Ergebnisse von Mischungen weiter modifiziert. Dies erfolgt bevorzugt dadurch, dass der entsprechende Schlüssel bzw. das entsprechende Mischergebnis in zwei Teillängen aufgeteilt wird und die eine Teillänge mit der anderen Teillänge gemischt wird. Dieses Mischergebnis kann dann wieder mit der Ausgangsgröße gemischt werden. Dadurch wird die Sicherheit der Originalkennung weiter erhöht.

In einer besonders bevorzugten Weiterbildung erfolgt die Aufteilung in zwei Teillängen dadurch, dass eine der beiden Teillängen nur Zeichen oder Bitfolgen enthält, die in einem bereitgestellten zweiten zufälligen Sitzungsschlüssel enthalten sind, und die andere der beiden Teillängen nur Zeichen oder Bitfolgen enthält, die nicht in dem zweiten zufälligen Sitzungsschlüssel enthalten sind. Besonders vorteilhaft ist es dann, wenn der zweite zufällige Sitzungsschlüssel identisch ist mit dem ersten zufälligen Sitzungsschlüssel. Dann kann bei Verwendung eines Verwenderschlüssels eine Abspeicherung der Sitzungsschlüssel unterbleiben.

In einer vorteilhaften Ausgestaltung ist vorgesehen, dass zumindest bei einem Mischvorgang das Mischen als logische XOR-Codierung oder bevorzugt als logisch erweiterte XOR-Codierung erfolgt.

Zweckmäßig sind der erste zufällige Sitzungsschlüssel, der erste Verwenderschlüssel, der zweite Verwenderschlüssel und/oder der Gegenstandsschlüssel > 1 Bit, bevorzugt ≥ 24 Byte und insbesondere ≥ 32 Byte groß.

Weiterhin ist es zweckmäßig, wenn der Hauptschlüssel > 100 Byte, bevorzugt ≥ 1 MByte und insbesondere ≥ 100 MByte ist. Dadurch ist der Mischungsraum sehr groß, so dass zufällige Übereinstimmungen von gefälschten Originalkennungen ausgeschlossen werden können.

In Bezug vor allem auf die Verfahrensschritte bei der Bereitstellung einer Originalkennung, die Durchführung der Teilung, das Mischen mit logischer XOR-Codierung oder logisch erweiterter XOR-Codierung wird auf die DE 10 2009 022 233.2 Bezug genommen, deren Inhalt vollumfänglich in die vorliegende Erfin-

dungsoffenbarung aufgenommen wird. Diese DE 10 2009 022 233.2 beschreibt dabei ein Verfahren zur Verwendung einer Zeichenkette und dieses Verfahren kann für das Verfahren zur Bereitstellung einer Originalkennung eingesetzt werden. Alle Verfahrensschritte der DE 10 2009 022 233.2 sind also auch vorliegend verwendbar und sollen ausdrücklich Bestandteil der vorliegenden Erfindung sein. Ebenso sind auch alle in der DE 10 2009 022 233.2 beschriebenen Vorteile solche, die auf die vorliegende Erfindung zutreffen.

Selbstständiger Schutz wird beansprucht für die Verwendung der erfindungsgemäß hergestellten Originalkennung für die Kennzeichnung eines Produkts oder dgl. Dabei sind der Hauptschlüssel und ggf. der Verwenderschlüssel an einer Überprüfungsvorrichtung hinterlegt und zur Überprüfung der Originalkennung auf Echtheit wird bestimmt, ob die Originalkennung unter Verwendung des hinterlegten Hauptschlüssels und ggf. des hinterlegten Verwenderschlüssels erzeugbar ist. In einer bevorzugten Ausgestaltung dieser Verwendung ist vorgesehen, dass überprüft wird, ob der in der Originalkennung verwendete Gegenstandsschlüssel mit den Angebots-, Vertriebs- und/oder Verkaufsmodalitäten und dgl. für das Produkt übereinstimmt. Dabei wird bevorzugt überprüft, ob der Gegenstandsschlüssel mit dem für das Produkt festgestellten Vertriebsweg übereinstimmt.

Besonders vorteilhaft ist das Produkt oder dgl. in einer Verpackung angeordnet, wobei zumindest eine erste Originalkennung auf dem Produkt selbst oder dgl. und zumindest eine zweiter Originalkennung auf der Verpackung vorgesehen sind, wobei sich die erste Originalkennung von der zweiten Originalkennung unterscheidet. Hierdurch wird die Fälschungssicherheit noch einmal bedeutend erhöht, da ein Fälscher nun für ein Produkt mehrere Originalkennungen fälschen müsste.

Weiterhin wird selbstständiger Schutz für die Verwendung der erfindungsgemäß hergestellten Originalkennung für die Autorisierung der Zugangsberechtigung zu einem Zugang, insbesondere zu einem Bereich, einem Fahrzeug, einem Programm oder dgl. beansprucht. Diese Verwendung zeichnet sich dadurch aus, dass der Hauptschlüssel und gegebenenfalls der erste und/oder zweite Verwenderschlüssel an einer dem Zugang zugeordneten Überprüfungsvorrichtung hinterlegt sind und die Originalkennung von dem den Zugang nachsuchenden Verwender bereitgehalten wird, wobei zur Überprüfung der Zugangsberechtigung zu dem Zugang durch die Überprüfungsvorrichtung bestimmt wird, ob die Originalkennung

unter Verwendung des hinterlegten Hauptschlüssels und gegebenenfalls des hinterlegten ersten und/oder zweiten Verwenderschlüssels erzeugbar ist.

In einer besonders bevorzugten Ausgestaltung ist vorgesehen, dass dem Verwender ein erstes elektronisches Mittel zugeordnet ist, in dem der Hauptschlüssel hinterlegt ist, und wobei dem Zugang ein zweites elektronisches Mittel zugeordnet ist, das den ersten zufälligen Sitzungsschlüssel erzeugt und diesen Sitzungsschlüssel bzw. das Ergebnis einer Mischung des ersten zufälligen Sitzungsschlüssels und des ersten Verwenderschlüssels dem dem Verwender zugeordneten ersten elektronischen Mittel übermittelt, wobei das erste elektronische Mittel aus dem ersten zufälligen Sitzungsschlüssel und dem Hauptschlüssel die Originalkennung erzeugt.

Außerdem wird unabhängiger Schutz beansprucht für die Originalkennung selbst, die nach dem erfindungsgemäßen Verfahren hergestellt wurde und die als ein Barcode insbesondere als 1- oder 2-dimensionaler Barcode, oder eine Oberflächenstrukturierung ausgebildet ist oder die in einem elektronischen Speicher, insbesondere einem RFED-Chip angeordnet ist.

Selbständiger Schutz wird beansprucht für eine Einrichtung die angepasst ist, das erfindungsgemäße Verfahren auszuführen.

Die Erfindung kann in Form einer völligen Hardware-Ausgestaltung, einer völligen Software-Ausgestaltung oder einer Ausgestaltung, die sowohl Hardware- als auch Software-Elemente enthält, verwirklicht werden. In einer bevorzugten Ausgestaltung ist die Erfindung in Software implementiert, die Firmware, systemeigene Software, Microcode und dgl. umfasst, jedoch nicht darauf beschränkt ist.

Weiterhin kann die Erfindung in Gestalt eines Computerprogrammprodukts verwirklicht werden, das von einem computernutzbaren oder computerlesbaren Medium zugänglich ist und einen Programmcode für die Benutzung durch oder für die Benutzung in Verbindung mit einem Computer oder jeden Befehlsausführungssystem bereitgestellt ist. Daher wird auch selbständiger Schutz beansprucht für ein Computerprogrammprodukt, das auf einem für einen Computer lesbaren Medium gespeichert ist und für den Computer lesbare Programmmittel umfasst, die den Computer veranlassen, das erfindungsgemäße Verfahren auszuführen, wenn die Programmmittel auf dem Computer ausgeführt werden.

Für die Zwecke dieser Beschreibung können computernutzbare oder computerlesbare Medien alle Einrichtungen oder Vorrichtungen sein, die das Programm für die Benutzung durch oder die Benutzung in Verbindung mit dem Befehlsausführungssystem, der Vorrichtung oder der Einrichtung enthalten, speichern, kommunizieren, verbreiten oder transportieren.

Das Medium kann ein elektronisches, magnetisches, optisches, elektromagnetisches, Infrarot- oder Halbleitersystem (oder Vorrichtung oder Einrichtung) sein oder ein Ausbreitungsmedium. Beispiele eines computerlesbaren Mediums umfassen einen Halbleiter oder Feststoffspeicher, Magnetband, eine entfernbare Computerdiskette, einen Random Access Memmory (RAM), einen Read-only Memmory (ROM), eine feste magnetische Disk und eine optische Disk. Gegenwärtige Beispiele von optischen Disks umfassen Compaktdisk-Read-only Memmory (CD-ROM), Compaktdisk-Read/Write (CD-R/W) und DVD.

Ein Datenverarbeitungssystem, das geeignet ist, den Programmcode zu speichern und/oder auszuführen, umfasst wenigstens einen Prozessor, der direkt oder indirekt mit zumindest einem Speicherelement durch einen Systembus verbunden ist. Das Speicherelement kann lokalen Speicher umfassen, der während der aktuellen Ausführung des Programmcodes tätig wird, Massenspeicher und Pufferspeicher, der eine temporäre Speicherung von wenigstens einigen Programmcodes bereitstellt, um die Anzahl an Abrufen des Codes vom Massenspeicher während der Ausführung zu reduzieren.

Eingabe/Ausgabe- oder I/O-Einrichtungen, die Tastaturen, Displays, Zeigeeinrichtungen etc. umfassen können, jedoch nicht darauf limitiert sind, können mit dem System entweder direkt oder durch zwischengeschaltete I/O-Controller an das System angekoppelt sein.

Netzwerkadapter können ebenfalls mit dem System verbunden sein, um zu ermöglichen, dass das Daten verarbeitende System mit anderen Datenverarbeitungssystemen oder entfernten Druckern oder Speichereinrichtungen durch zwischengeschaltete private oder öffentliche Netzwerke angekoppelt wird. Modems, Kabelmodems oder Ethernet-Karten sind in diesem Zusammenhang nur einige Beispiele der gegenwärtig verfügbaren Typen von Netzwerkadaptern.

Die Merkmale der vorliegenden Erfindung sowie weitere Vorteile werden nun anhand der Beschreibung bevorzugter Ausführungsbeispiele anhand der Figuren verdeutlicht werden. Dabei zeigen:

Fig. 1 eine erste bevorzugte Ausgestaltung zur Erzeugung des ersten Teils der Originalkennung,

Fig. 2a, 2b eine erste bevorzugte Ausgestaltung zur Erzeugung des zweiten Teils der Originalkennung,

Fig. 3 die aus dem ersten Teil gemäß Fig. 1 und dem zweiten Teil gemäß Fig. 2a, 2b erzeugte Originalkennung,

Fig. 4 den bei der Erzeugung des dritten Teils der Originalkennung nach Fig. 2 verwendeten Mischalgorithmus,

Fig. 5 den im Mischalgorithmus nach Fig. 3 verwendeten Teilungsalgorithmus,

Fig. 6 die Verwendung der erfindungsgemäßen Originalkennung zur Autorisierung eines Zugangs und

Fig. 7 die in der Verwendung nach Fig. 6 benutzte zweite bevorzugte Ausgestaltung zur Erzeugung der Originalkennung.

Die in den nachfolgend beschriebenen Figuren aufgezeigten alphanumerischen Zeichenfolgen und Barcodes sind nur beispielhaft zur grafischen Erläuterung angegeben. Sie folgen nicht den angegebenen Mischungsalgorithmen.

In Fig. 1 ist rein schematisch die Herstellung des ersten Teils OK1 der Originalkennung OK nach einer ersten bevorzugten Ausgestaltung dargestellt. Zu erkennen ist, dass der erste zufällige Sitzungsschlüssel ZZ$ mit einem Verwenderschlüssel V$ mittels einer XOR-Codierung gemischt wird, um einen Kennungsschlüssel K$ zu erzeugen. Der Kennungsschlüssel K$ wird anschließend in einen 1-dimensionalen Barcode umgewandelt, der den ersten Teil OK1 der erfindungsgemäßen Originalkennung OK bildet.

In Fig. 2a und 2b ist rein schematisch die Erzeugung des zweiten Teils OK2 der Originalkennung OK nach der ersten bevorzugten Ausgestaltung dargestellt. Zu erkennen ist, dass der Hauptschlüssel Mutter$ mit dem ersten zufälligen Sitzungsschlüssel ZZ mit Hilfe eines besonderen Mischalgorithmus MA gemischt wird, um einen One-time-Pad Schlüssel OTP$ zu bilden.

Wie aus Fig. 2b zu erkennen ist, wird dieser One-time-Pad Schlüssel OTP$ mit einem Gegenstandsschlüssel G$ mittels einer logischen XOR-Codierung gemischt wird, wodurch ein Produktschlüssel P$ entsteht. Auch dieser Produkt-

schlüssel P$ wird in einen 1-dimensionalen Barcode umgewandelt und bildet den zweiten Teil OK2 der Originalkennung OK.

In diesem bevorzugten Ausführungsbeispiel ist der Hauptschlüssel Mutter$ 100 MB groß, der Verwenderschlüssel V$ genauso wie der erste zufällige Sitzungsschlüssel ZZ$ ist 16 Byte groß.

Die Originalkennung OK selbst wird dann dadurch gebildet, dass der erste Teil OK1 der Originalkennung OK dem zweiten Teil OK2 der Originalkennung OK vorangestellt wird und sich so ein einheitlicher Barcode OK ergibt, so wie dies in Fig. 3 dargestellt ist. Die beiden Teile OK1, OK2 des Originalkennung OK können dabei, wie in Fig. 3 dargestellt räumlich abgesetzt dargestellt sein oder auch direkt ineinander übergehend, so dass keine Trennung erkennbar ist.

In Fig. 4 ist in rein schematischer Weise der in dem bevorzugten Ausführungsbeispiel nach Fig. 2a verwendete Mischalgorithmus MA dargestellt, wobei Fig. 5 den in diesem Mischalgorithmus verwendeten Teilungsalgorithmus WV rein schematisch zeigt. Der in Fig. 5 gezeigte Sitzungsschlüssel ZZ$ ist nur beispielhaft dargestellt und entspricht nicht dem in den Fig. 1, 2a und 2b verwendetem Sitzungsschlüssel ZZ$, da in Fig. 5 nur das Prinzip des Teilungsalgorithmus WV beschrieben werden soll.

In Fig. 4 ist zu erkennen, dass der Hauptschlüssel Mutter$ mit dem ersten zufälligen Sitzungsschlüssel ZZ$ logisch erweitert XOR codiert wird. Dies erfolgt dadurch, dass die ersten 16 Byte des Hauptschlüssels Mutter$ mit dem Sitzungsschlüssel ZZ$ logisch XOR codiert werden, wodurch als Ergebnis ein erster Teilstring ZK$ 1 entsteht, der ebenfalls eine Länge von 16 Byte aufweist. Dieser erste Teilstring ZK$ 1 wird dann wiederum verwendet, um einen weiteren Teil des Hauptschlüssels Mutter$ XOR zu codieren. Dazu werden die nächsten 16 Byte des Sitzungsschlüssels Mutter$ verwendet und es entsteht im Ergebnis ein zweiter Teilstring ZK$ 2, der seinerseits für die XOR Codierung der nächsten 16 Byte des Hauptschlüssels Mutter$ verwendet wird. Dieses Prozedere wird, wie in Fig. 4 angedeutet, solange wiederholt, bis die gesamten 100 MB des Hauptschlüssels Mutter$ verwertet wurden. Die Aneinanderreihung der Teilstrings ZK$ 1, ZK$ 2, ZK$ 3, ZK$ 4, ZK$ 5 und so fort, ergibt im Ergebnis eine erste Zeichenkette Work$ 1, die wie der Hauptschlüssel Mutter$ eine Länge von 100 MB aufweist.

Diese erste Zeichenkette Work$ 1 wird nun nach dem in Fig. 5 näher beschriebenen Teilungsalgorithmus WV in zwei Teillängen True$, Untrue$ aufge-

spaltet und nachfolgend werden beide Teillängen True$, Untrue$ miteinander XOR codiert. Dies erfolgt dadurch, dass die kürzere Teillänge, im vorliegenden Beispiel True$, so oft aneinandergereiht wird, dass ihre Länge zumindest der längeren Teillänge, im vorliegenden Beispiel Untrue$, entspricht. Im Ergebnis entsteht dann eine zweite Zeichenkette Work$ 2, die die Länge der längeren Teillänge Untrue$ aufweist.

Selbstverständlich könnte anstatt einer XOR Codierung der beiden Teillängen True$, Untrue$ alternativ auch eine erweiterte XOR Codierung erfolgen, um die Angreifbarkeit des Hauptschlüssels Mutter$ weiter zu senken.

Anschließend wird die erste Zeichenkette Work$ 1 mit der zweiten Zeichenkette Work$2 logisch XOR codiert, wobei wiederum die zweite Zeichenkette Work$ 2 sooft aneinandergereiht wird, dass ihre Länge der der ersten Zeichenkette Work$ 1 entspricht. Im Ergebnis entsteht ein Codeschlüssel Code$, der wiederum die Länge des Hauptschlüssels Mutter$, also 100 MB aufweist.

Aus diesem Codeschlüssel Code$ wird der One-time-Pad Schlüssel OTP$ durch Größenreduktion generiert, der 32 Byte groß ist. Diese Größenreduktion erfolgt dadurch, dass der im Mischalgorithmus erzeugte Codeschlüssel Code$ mittels eines bestimmten Reduktionsalgorithmus von 100 MB auf 32 Byte reduziert wird. Dies kann beispielsweise dadurch erfolgen, dass die ersten 32 Byte von den 100 MB herausselektiert werden. Es sind aber natürlich auch andere Reduktionsalgorithmen verwendbar, solang diese reproduzierbar festgelegt sind.

In Fig. 5 ist rein schematisch der Teilungsalgorithmus WV aus Fig. 4 in einem Blockschaltbild dargestellt. Und zwar wird im Rahmen dieses Teilungsalgorithmus WV verglichen, welche in dem Sitzungsschlüssel ZZ$ enthaltenen Zeichen auch in der ersten Zeichenkette Work$ 1 enthalten sind. Diejenigen Zeichen, die in der ersten Zeichenkette Work$ 1 enthalten sind, werden in der Reihenfolge, die in dem Sitzungsschlüssel ZZ$ vorgegeben ist, in der ersten Teillänge True$ abgelegt. Andererseits werden diejenigen Zeichen der ersten Zeichenkette Work$ 1, die nicht in dem Sitzungsschlüssel ZZ$ enthalten sind, in derjenigen Reihenfolge, die in der erste Zeichenkette Work$ 1 vorgegeben ist, in der zweiten Teillänge Untrue$ abgelegt. Dieser Mischalgorithmus verhindert zusätzlich die Rückwärtsrechnung, die sonst bei einfachen XOR Codierungen unter Umständen möglich sein könnte. Natürlich kann auch eine andere Reihenfolge beim Erstellen der Teillängen True$, Untrue$ gewählt werden.

Bei den Schlüsseln Mutter$, ZZ$, V$, G$, P$ handelt es sich um alphanumerische Zeichenketten bestehend aus Buchstaben, Zahlen und Sonderzeichen, wobei alternativ natürlich auch nur rein binäre Zeichenfolgen Verwendung finden können.

Der Verwenderschlüssel V$ steht im vorliegenden Ausführungsbeispiel für den Namen eines bestimmten Herstellers. Der in Fig. 2b verwendete Gegenstandsschlüssel G$ setzt sich aus einer Vielzahl von Informationen zusammen, wie dies in Fig. 2b näher dargestellt ist. In diesem Beispiel ist gezeigt, dass die Gegenstandsschlüssel G$ Informationen zum Herstellungsdatum, der für die Ausfuhr vorgesehenen Zollstelle, nämlich im vorliegenden Fall Frankfurt a. Main, den Zwischenhändler im Empfängerland, das Empfängerland, darüber, ob es sich um eine Ausfuhr oder Einfuhr handelt, die Produktnummer und den Produktnamen enthält. Natürlich können hier auch andere Informationen über das Produkt hinterlegt sein.

Die solchermaßen hergestellte Originalkennung OK wird nun an dem Produkt angebracht, wobei beispielsweise bei Medikamenten eine erste Originalkennung OK auf der gemeinsamen Verpackung der Medikamente vorgesehen ist und auf jedem in der Verpackung enthaltenen Blister eine weitere, dazu unterschiedliche Originalkennung OK.

Der erste Teil OK1 der Originalkennung OK identifiziert dabei den Hersteller des Medikaments und gibt Rückschlüsse über den verwendeten ersten zufälligen Sitzungsschlüssel ZZ$. Der zweite Teil OK2 wiederum enthält Produktinformationen und ermöglicht eine Rückverfolgung zum Hersteller.

Beide Teile OK1, OK2 der Originalkennung OK haben gemeinsame und unverwechselbare Eigenschaften. Ihr Auftreten als Pärchen OK1, OK2 ist in dieser Form faktisch einmalig. Außerdem hat dieses Pärchen OK1, OK2 nur für einen einzigen Hersteller seine Gültigkeit. Die in dem zweiten Teil OK2 der Originalkennung OK verschlüsselte Produktinformation ist ein One-time-Pad und damit absolut fälschungssicher. Dabei können die Pärchen OK1, OK2 in Echtzeit beim Hersteller generiert werden und zeigen keine statistischen Merkmale, die eine Entschlüsselung ermöglichen würden. Der Zufallsraum Ω bezüglich der Erzeugung der Originalkennung OK beträgt $\Omega = 2^{384}$, wodurch sichergestellt ist, dass ohne Wechseln des Hauptschlüssels Mutter$ eine Vielzahl von Produkten mit einer Originalkennung OK versehen werden kann, ohne dass es zu Wiederholungen der Originalkennung OK kommt. Ein weiterer wesentlicher Vorteil besteht darin, dass einmal

generierte Pärchen OK1, OK2 und somit die Originalkennungen OK zu keiner Zeit gespeichert werden müssen, da dem Hersteller sein eigener Verwenderschlüssel V$ bekannt ist und er so auf den ersten zufälligen Sitzungsschlüssel ZZ$ zurückrechnen kann und der Hersteller damit und mit Hilfe seines gespeicherten Hauptschlüssels Mutter$ aus dem zweiten Teil OK2 der Originalkennung OK den Gegenstandsschlüssel G$ zurückrechnen kann, um festzustellen, ob dieser Gegenstandsschlüssel G$ überhaupt sinnvoll ist und auch dem Produkt zugeordnet werden kann, nämlich beispielsweise hinsichtlich dessen Vertriebsweg.

Wie gesagt können bezüglich des Produkts mehrere Originalkennungen OK angebracht werden, nämlich beispielsweise eine erste Originalkennung OK auf der Verpackung, eine davon unterschiedliche zweite Originalkennung OK auf dem Blister und bei Bedarf auch eine dritte unterschiedliche Originalkennung OK auf dem Beipackzettel eines Medikaments. Dadurch dass es sich hier um unterschiedliche Originalkennungen OK handelt, wird die Fälschung noch aussichtsloser für den Plagiateur.

Anhand eines Beispiels soll im Folgenden verdeutlicht werden, warum die Fälschung von Originalkennungen für einen Plagiateur beispielsweise für Medikamente nicht sinnvoll ist. Dabei wird davon ausgegangen, dass eine Lieferung von Medikamenten des Namens ABC in den Kongo geliefert werden soll, wobei die Lieferung 4.000 Packungen des Medikaments aufweist. Auf jeder Verpackung sind unterschiedliche Originalkennungen OK angebracht und außerdem sind weitere unterschiedliche Originalkennungen noch auf den enthaltenen Blistern sowie auf den Beipackzetteln vorgesehen. Wenn nur ein Blister pro Verpackung enthalten ist, dann sind bezüglich der Lieferung 12.000 also unterschiedliche Originalkennungen OK vorhanden.

Ein Fälscher, der nun eine gefälschte Lieferung dieses Medikaments auf den Markt bringen will, hätte nun verschiedene Möglichkeiten. So könnte er überhaupt keine Originalkennungen OK anbringen. Dies würde man aber sofort beim Zoll erkennen. Damit könnten solche Lieferungen sofort aus dem Verkehr gezogen werden.

Weiterhin könnte er statt der Originalkennungen OK reine Phantasiekennungen anbringen. Dies würde man nach einer Entschlüsselung als Fälschung erkennen. Hierzu könnte entweder der Zoll beim Hersteller um Mithilfe bitten, wonach dann der Hersteller rückrechnet, ob die angebrachten Originalkennungen OK

sinnvoll sind. Alternativ könnten dem Zoll vom Hersteller auch spezielle Entschlüsselungsgeräte zur Verfügung gestellt werden, die den auslesegesicherten Hauptschlüssel Mutter$ und den ggf. ebenfalls auslesegesicherten Verwenderschlüssel V$ enthalten. Damit könnte dann beim Zoll direkt überprüft werden, ob die Codes Fälschungen sind.

Weiterhin könnte der Plagiateur sich einige echte Originalkennungen OK beschaffen und diese wahllos auf der Lieferung anbringen. Dies würde dazu führen, dass beim Überprüfen der Originalkennungen OK nach einigen Stichproben festgestellt werden würde, dass hier gleiche Originalkennungen OK vorliegen, was aber nicht sein kann, so dass es sich um eine Fälschung handeln muss. Andererseits wird auch der in den Originalkennungen OK enthaltene Gegenstandsschlüssel G$ beispielsweise nicht mit den Vertriebsmodalitäten des Produkts übereinstimmen.

Schließlich könnte der Plagiateur sich auch beispielsweise 3.000 echte Originalkennungen OK beschaffen und diese anbringen. In diesem Fall würde allerdings wiederum die Produktinformation in dem Gegenstandsschlüssel G$ nicht stimmen, da beispielsweise das Herstellungsdatum, das in dem Gegenstandsschlüssel G$ enthalten ist, nicht mit dem Mindesthaltbarkeitsdatum in Einklang stehen und dgl. Im Übrigen würde die Beschaffung einer solch großen Menge von Originalkennungen OK beim Plagiateur sehr hohe Kosten verursachen, so dass diese Beschaffung in Bezug auf den erzielten Gewinn wirtschaftlich nicht sinnvoll ist. Außerdem würde eine solche Fälschung auch dadurch erkannt werden, dass mehrfach das gleiche Produkt mit der gleichen Produktnummer gehandelt werden würde, was wiederum nicht möglich ist.

Noch einen weiteren Vorteil weisen die erfindungsgemäßen Originalkennungen OK auf. Sollten nämlich alle Originalkennungen OK und zudem auch noch die Produkte selbst echt sein, dann würde sofort erkannt werden, dass es sich um einen gegebenenfalls illegalen Reimport handelt, da der Gegenstandsschlüssel G$ hinsichtlich der Angabe Ausfuhr oder Einfuhr nicht korrekt ist.

Wesentlich ist, dass die erfindungsgemäße Originalkennung nicht nur für Produkte, wie Medikamente, Ersatzteile oder dgl., eingesetzt werden kann, sondern auch für Urkunden, Zertifikate, amtliche Siegel, beispielsweise TÜV-Siegel, und dgl. Die Produktinformationen sind auch nicht auf Gegenstandsschlüssel G$ von 32 Byte und die Verwenderschlüssel V$ auch nicht auf 16 Byte beschränkt, sondern können maximal der Größe des Hauptschlüssel Mutter$ entsprechen, also

im vorliegenden Beispiel 100 MB groß sein, wobei der Hauptschlüssel Mutter$ natürlich auch beliebig größer gewählt werden kann. Dies ist alles nur eine Frage der verfügbaren Rechenkapazität.

Besonders vorteilhaft bei der erfindungsgemäßen Originalkennung OK ist es, dass das Verfahren zur Herstellung der Originalkennung OK ein sehr schnelles Verfahren ist und die Originalkennung OK sehr kostengünstig vorgesehen werden kann, beispielsweise mittels eines einfachen Aufdrucks. Alternativ kann die Originalkennung natürlich auch elektronisch abgelegt werden, beispielsweise in einem RFID-Chip, einem RAM, einen ROM oder dgl.

Das Verfahren ist zudem sehr flexibel und die Originalkennungen OK können jederzeit geändert werden, indem die Produktinformation im Produktschlüssel P$ geändert wird, der Verwenderschlüssel V$ und/oder der Hauptschlüssel Mutter$. Außerdem sind die der Originalkennung OK zugrunde liegenden Informationen für Niemanden einsehbar, sondern nur die Originalkennungen OK selbst.

Die verwendeten Originalkennungen OK können jederzeit leicht direkt beim Hersteller selbst abgefragt werden oder mittels vom Hersteller autorisierter Lesegeräte, die kein Sicherheitsrisiko darstellen, da die in den Lesegeräten enthaltenen Hauptschlüssel Mutter$ und Verwenderschlüssel V$ nicht ausgelesen werden können, wozu geeignete Maßnahmen zu ergreifen sind.

Eine Abfrage der Originalkennung OK kann beispielsweise mittels Handy erfolgen, indem die Originalkennung OK fotografiert und an den Hersteller übermittelt wird. Aber auch im Internet könnte ein Hersteller eine Kontrollmöglichkeit für seine Originalkennungen OK anbieten.

Wesentlich ist außerdem, dass nicht nur das Fälschen innerhalb einer legalen Handelskette verhindert wird, sondern auch geschmuggelte Ware wird sicher als Fälschung erkannt.

In einer zweiten bevorzugten Ausgestaltung gemäß Fig. 6 und Fig. 7 wird die erfindungsgemäße Originalkennung zur Autorisierung der Zugangsberechtigung für einen Zugang 1 zu einem gesicherten Bereich 2 verwendet. Der Zugang ist in diesem Falle eine Tür 1, die nach entsprechender Autorisierung durch einen Verwender (nicht gezeigt) geöffnet werden kann, um zu dem gesicherten Bereich 2 Zutritt zu erlangen, wobei der gesicherte Bereich 2 beispielsweise ein Kassenbereich einer Bank oder dgl. ist.

Dem Zugang 1 ist eine Überprüfungsvorrichtung 3 zugeordnet, die einen Autorisierungsvorgang des Verwenders überprüft und ggf. bei erfolgreicher Autorisierung den

Zugang 1 für den Verwender freigibt. Zur Durchführung des Autorisierungsvorganges benutzt der Verwender ein erstes elektronisches Mittel 4, das so ausgebildet ist, dass es mit einem zweiten elektronischen Mittel 5, das der Überprüfungseinrichtung 3 zugeordnet ist, kommunizieren kann. Das erste und zweite elektronische Mittel 4, 5 weisen dazu beispielsweise Funk- und Empfangsmittel oder dgl. auf.

In Fig. 6 ist nun rein schematisch der Autorisierungsvorgang dargestellt. Sowohl die Überprüfungsvorrichtung 3 als auch das erste elektronische Mittel 4 beinhalten den Hauptschlüssel Mutter$, der beispielsweise in einem ROM hinterlegt und gegenüber unberechtigtem Ausleseversuch gesichert ist. Weiterhin weist die Überprüfungsvorrichtung 3 eine Zufallsquelle auf, die beispielsweise als Zufallsgenerator 7 ausgebildet ist.

Nach dem der Verwender mit Hilfe des ersten elektronischen Mittels 4 sich bei der Überprüfungsvorrichtung 3 bemerkbar gemacht hat, stellt die Überprüfungsvorrichtung 3 mit Hilfe des Zufallszahlengenerators 7 einen Sitzungsschlüssel ZZ$ bereit, den es an das erste elektronische Mittel 4 übermittelt. Das erste elektronische Mittel 4 erzeugt aus dem gespeicherten Hauptschlüssel Mutter$ und dem Sitzungsschlüssel Z$ nach dem erfindungsgemäßen Verfahren eine Originalkennung OK(V), wobei V in diesem Fall für den Verwender steht. Diese Originalkennung OK(V) wird an die Überprüfungsvorrichtung 3 kommuniziert. Die Überprüfungsvorrichtung 3 erzeugt ebenfalls aus dem hinterlegten Hauptschlüssel Mutter$ und dem übermittelten Sitzungsschlüssel ZZ$ nach dem erfindungsgemäßen Verfahren eine Originalkennung OK.

Anschließend stellt die Überprüfungsvorrichtung 3 fest, ob die eigene erzeugte Originalkennung OK identisch ist mit der von dem ersten elektronischen Mittel 4 übermittelten Originalkennung OK(V). Wenn dies der Fall ist, dann gibt die Überprüfungsvorrichtung 3 den Zugang 1 für den Verwender frei. Falls keine Identität vorliegt, dann gibt die Überprüfungsvorrichtung 3 den Zugang 1 nicht frei und es kann ggf. vorgesehen werden, dass sogleich ein Alarm ausgelöst wird und/oder der Verwender optisch registriert wird.

Falls mehrere unterschiedlich berechtigte Verwender für den Zugang 1 vorgesehen sind, kann es sinnvoll sein, nicht den Sitzungsschlüssel ZZ$ selbst an das erste elektronische Mittel 4 zu kommunizieren, sondern den Sitzungsschlüssel ZZ$ mit Hilfe eines Verwenderschlüssels V$ und/oder Gegenstandsschlüssels G$ zu verschlüsseln und dieses verschlüsselte Ergebnis an das erste elektronische Mittel 4 zu kommunizieren. Hierzu würde das erste elektronische Mittel 4 beim Beginn des Autorisierungsvorganges mit Hilfe eines vorgesehenen Codes der Überprüfungsvorrichtung 3 mitteilen, welcher Verwender Zutritt

zu dem Zugang 1 begehrt und die Überprüfungsvorrichtung 3 würde den entsprechenden Verwenderschlüssel zur Verschlüsselung des Sitzungsschlüssels ZZ$ benutzen.

Nur wenn das erste elektronische Mittel 4 den identischen Verwenderschlüssel V$ und/oder Gegenstandsschlüssels G$ aufweist, kann das erste elektronische Mittel 4 durch Entmischung den zufälligen Sitzungsschlüssel ZZ$ stimmen und damit mit Hilfe des Hauptschlüssels Mutter$(V) die erforderliche Originalkennung OK(V) erzeugen.

In allen Fällen, in denen das erste elektronische Mittel nicht den korrekten Hauptschlüssel Mutter$ (V) aufweist, der identisch mit den in der Überprüfungseinrichtung 3 abgespeicherten Hauptschlüssel Mutter$ ist und ggf. der Verwenderschlüssel V$ und/oder Gegenstandsschlüssels G$ nicht mit dem in der Überprüfungseinrichtung 3 für den Verwender hinterlegten Verwenderschlüssel V$ und/oder Gegenstandsschlüssels G$ übereinstimmt, findet keine erfolgreiche Autorisierung statt und der Zugang 1 bleibt für den Verwender verschlossen, da die erzeugten Originalkennungen OK, OK(V) nicht identisch sind.

Alternativ kann auch vorgesehen sein, dass der Sitzungsschlüssel ZZ$ dem ersten elektronischen Mittel 4 nicht verschlüsselt übermittelt wird, sondern dass in dem ersten elektronischen Mittel 4 ein Verwenderschlüssel V$ und/oder Gegenstandsschlüssel G$ abgelegt ist und damit mit dem erfindungsgemäßen Verfahren die Originalkennung OK(V) erzeugt wird. In diesem Falle würde die Überprüfungsvorrichtung 3, in der alle zugangsberechtigten Verwenderschlüssel V$ bzw. Gegenstandsschlüssel G$ hinterlegt sind, alle möglichen Originalkennungen OK durchrechnen und überprüfen, ob die übermittelte Originalkennung OK(V) mit einer dieser möglichen Originalkennungen OK identisch ist und den Zugang 1 öffnen.

Vorliegend ist die Zufallsquelle 7 der Überprüfungsvorrichtung 3 zugeordnet. Alternativ kann natürlich auch vorgesehen sein, dass die Zufallsquelle 7 dem ersten elektronischen Mittel 4 zugeordnet ist und der damit erzeugte Sitzungsschlüssel ZZ$ an die Überprüfungsvorrichtung 3 übermittelt wird, wonach dann sowohl die Überprüfungsvorrichtung 3 als auch das erste elektronische Mittel 4 jeweils die Originalkennung OK, OK(V) erzeugen und die Überprüfungsvorrichtung 3 feststellt, ob Identität vorliegt.

Im beschrieben Beispiel ist der Zugang 1 eine Tür zu einem gesicherten Bereich 2, der beispielsweise in einem Haus angeordnet ist. Alternativ kann natürlich auch vorgesehen sein, dass es sich um einen Zugang zu einem Automobil handelt, wobei dann das erste elektronische Mittel 4 in einer Funkentriegelung integriert ist.

Unabhängig von solchen rein körperlichen Zugängen 1 kann es sich auch um einen reinen Informationszugang bzw. elektronischen Zugang handeln, beispielsweise also

um den Zugang zu gesicherten Strukturen einer Datenverarbeitungsanlage oder einem gesicherten Softwarebereich auf einer solchen Datenverarbeitungsanlage.

Auch jegliche anderen Arten von Zugängen lassen sich mit Hilfe der erfindungsgemäßen Originalkennung OK und des erfindungsgemäßen Verfahrens zur Erzeugung dieser Originalkennung OK gegenüber einem unbefugten Zugriff absichern.

Bei der Beschreibung der bevorzugten Ausführungsbeispiele wurde davon ausgegangen, dass die Zufallsquelle ein Zufallszahlengenerator 7 ist. Alternativ kann natürlich auch jede andere Art von Zufallsquelle verwendet werden. Solche Quellen können beispielsweise die Oberflächenbeschaffenheit, insbesondere Rauheiten von bestimmten Oberflächen sein. Andererseits können auch bestimmte Farbwerte einer Fläche oder eines Gegenstandes zur Erzeugung einer Zufallszahl verwendet werden, oder es werden dazu Kontrastverhältnisse verwendet.

Die Originalkennung OK muss auch nicht als alphanumerische Zeichenfolge, Barcode oder dgl. abgebildet oder als Binärcode elektronisch gespeichert bzw. übertragen werden. Alternativ könnte die Originalkennung OK auch als ein- oder zweidimensionaler Farb- oder Kontrastwerte, als Hologramm und mittels besonderer Farben oder dgl. ggf. auch unsichtbar dargestellt werden.

Bezüglich der Generierung des Hauptschlüssels Mutter$ und des Sitzungsschlüssels ZZ$ zu deren Bereitstellung für das Verfahren wird auf die deutsche Patentanmeldung DE 10 2008 033 162 verwiesen und ihr Inhalt hiermit auch vollständig mit einbezogen. Diese Patentanmeldung beschreibt ausführlich, wie Zufallszahlen mit extrem hoher statistischer Qualität als physikalische Zufallszahlen erzeugt werden können. Alternativ können diese Schlüssel Mutter$, ZZ$ auch kostengünstig als Pseudozufallszahl erzeugt werden.

Wesentlich an dem erfindungsgemäßen Verfahren zur Erzeugung der Originalkennung OK und der erfindungsgemäßen Originalkennung OK sowie den Verwendungen dieser Originalkennung ist, dass dies auf einem besonders einfach und effizient erzeugbaren One-Time-Pad beruht, wodurch gewährleistet ist, dass auch beispielsweise bei einem Abfangen des Sitzungsschlüssels ZZ$ bei der Zugangsautorisierung nichtberechtigte Verwender die Autorisierung nicht vornehmen können, weil sie den Hauptschlüssel Mutter$ nicht bestimmen können.

Im Gegensatz zur erfindungsgemäßen Originalkennung OK waren bisherige Produktkennzeichnungen im großen Stil fälschbar, da sie nicht einzigartig sind. Und für den

Fall, dass die Produktkennzeichnung eine Vielzahl von Sicherheitsmerkmalen enthält, konnte eine Fälschung nur mit Hilfe von speziell ausgebildeten Fachleuten ermittelt werden.

Mit der erfindungsgemäßen Originalkennung OK kann jedem Produkt ohne weiteres eine einzigartige Originalkennung OK zugeordnet werden und eine Überprüfung auf Originalität ist nicht nur speziell ausgebildeten Fachleuten vorbehalten, sondern kann ohne weiteres beim Hersteller selbst mit Hilfe einer Hotline oder dgl. oder mit Hilfe von durch den Hersteller autorisierter Geräte beim Zoll oder ähnlichen Einrichtungen ohne weitere Ausbildung mühelos erfolgen.

Aus dem vorstehenden ist klar geworden, dass die vorliegende Erfindung eine Originalkennung bereitstellt, die Produktfälschungen weitgehend verhindert, wobei die Originalkennung in ihrer Herstellung sehr kostengünstig ist. Die erfindungsgemäße Originalkennung eignet sich dabei nicht nur zur Verwendung als Produktkennzeichnung, sondern auch zum Autorisierungsnachweis, beispielsweise bei der Sicherung von räumlichen oder elektronischen Zugängen, wie Türen, Computerprogrammen und dgl.

Patentansprüche

1. Verfahren zur Bereitstellung einer Originalkennung (OK) für einen Gegenstand, wie ein Produkt, eine Autorisierung für einen Zugang (1) oder dgl., **dadurch gekennzeichnet, dass** das Verfahren die folgenden Schritte umfasst:
   a) zur Verfügung stellen eines Hauptschlüssels (Mutter$),
   b) Erzeugung eines ersten zufälligen Sitzungsschlüssels (ZZ$) und
   c) Mischen des Hauptschlüssels (Mutter$) mit dem ersten zufälligen Sitzungsschlüssel (ZZ$).

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** in Schritt b) der erste zufällige Sitzungsschlüssel einem Verwender als Ergebnis der Mischung des ersten zufälligen Sitzungsschlüssels und einem ersten Verwenderschlüssel bereitgestellt wird, dem Verwender ein Verwenderschlüssel zugeteilt wurde und der erste zufällige Sitzungsschlüssel durch Entmischen des Ergebnisses mit dem dem Verwender vorliegenden Verwenderschlüssel bestimmt wird.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** weiterhin folgende Schritte vorgenommen werden:
   d) zur Verfügung stellen eines Gegenstandsschlüssels (G$) und
   e) Mischen des Gegenstandsschlüssels (G$) mit dem Ergebnis von Schritt c), wobei bevorzugt weiterhin das Ergebnis von Schritt c) oder Schritt d) auf eine dem Gegenstandsschlüssel (G$) entsprechende Länge mit einem vorgegebenen Reduktionsalgorithmus reduziert wird.

4. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet, dass** weiterhin folgende Schritte vorgenommen werden:
   f) zur Verfügung stellen eines zweiten Verwenderschlüssel (V$), der bevorzugt identisch dem ersten Verwenderschlüssel ist und der charakteristisch ist für die Benutzung der Originalkennung (OK), insbesondere dessen Verwender,
   g) Erzeugung einer Kennung (K$) durch Mischung des ersten zufälligen Sitzungsschlüssels (ZZ$) und des zweiten Verwenderschlüssel (V$) und

h) Verbindung der Ergebnisse (P$, OK2) von Schritt c) oder Schritt e) und der Kennung (K$, OK1) zur Originalkennung (OK), wobei bevorzugt die Kennung (OK1) dem Ergebnis (P$, OK2) voran- oder nachgestellt wird.

5. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet, dass** weiterhin folgende Schritte vorgenommen werden:

i) das Ergebnis aus Schritt c) oder e) in zwei Teillängen (True$, Untrue$) aufgeteilt wird, wobei eine Teillänge (Untrue$) mit der anderen Teillänge (True$) gemischt wird und

j) das Ergebnis aus Schritt c) oder e) wird mit dem Ergebnis von Schritt i) gemischt.

6. Verfahren nach Anspruch 5, **dadurch gekennzeichnet, dass** eine der beiden Teillängen (True$) nur Zeichen oder Bit-Folgen enthält, die in einem bereitgestellten zweiten zufälligen Sitzungsschlüssel (ZZ$) enthalten sind, und die andere der beiden Teillängen (Untrue$) nur Zeichen oder Bit-Folgen enthält, die nicht in dem zweiten zufälligen Sitzungsschlüssel (ZZ$) enthalten sind, wobei insbesondere der erste zufällige Sitzungsschlüssel und der zweite zufällige Sitzungsschlüssel als identische zufällige Sitzungsschlüssel (ZZ$) bereitgestellt werden.

7. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet, dass** das Mischen als logische XOR-Codierung, bevorzugt logisch erweiterte XOR-Codierung erfolgt.

8. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet, dass** der erste zufällige Sitzungsschlüssel, der zweite zufällige Sitzungsschlüssel (ZZ$), der erste Verwenderschlüssel, der zweite Verwenderschlüssel (V$) und/oder der Gegenstandsschlüssel (G$) größer als 1 Bit, bevorzugt $\geq$ 24 Byte und insbesondere $\geq$ 34 Byte groß gewählt werden und/oder dass der Hauptschlüssel (Mutter$) größer als 100 Byte, bevorzugt $\geq$ 1 MByte und insbesondere $\geq$ 100 MByte gewählt wird.

9. Verwendung der Originalkennung (OK) nach einem der vorherigen Ansprüche für die Kennzeichnung eines Produktes oder dgl., **dadurch gekennzeichnet, dass** der Hauptschlüssel und ggf. der erste und/oder zweite Verwenderschlüssel an einer Überprüfungsvorrichtung hinterlegt sind und zur Überprüfung der Originalkennung (OK) auf Echtheit bestimmt wird, ob die Originalkennung (OK) unter Verwendung des hinterlegten Hauptschlüssels (Mutter$) und ggf. des hinterlegten ersten und/oder zweiten Verwenderschlüssels (V$) erzeugbar ist.

10. Verwendung nach Anspruch 9, **dadurch gekennzeichnet, dass** überprüft wird, ob der in der Originalkennung (OK) verwendete Gegenstandsschlüssel (G$) mit den Angebots-, Vertriebs- und/oder Verkaufsmodalitäten und dgl. für das Produkt oder dgl., insbesondere mit dem für das Produkt oder dgl. festgestellten Vertriebsweg übereinstimmt.

11. Verwendung nach Anspruch 9 oder 10, **dadurch gekennzeichnet, dass** das Produkt oder dgl. in einer Verpackung angeordnet ist, wobei zumindest eine erste Originalkennung (OK) auf dem Produkt oder dgl. und zumindest eine zweite Originalkennung, die sich von der ersten Originalkennung unterscheidet, auf der Verpackung vorgesehen sind.

12. Verwendung der Originalkennung (OK) nach einem der Ansprüche 1 bis 8 für die Autorisierung der Zugangsberechtigung zu einem Zugang (1), insbesondere zu einem Bereich, einem Fahrzeug, einem Programm und dgl., **dadurch gekennzeichnet, dass** der Hauptschlüssel (Mutter$) und ggf. der erste und/oder zweite Verwenderschlüssel (V$) an einer dem Zugang (1) zugeordneten Überprüfungsvorrichtung (3) hinterlegt sind und die Originalkennung (OK(V)) von der den Zugang nachsuchenden Person oder nachsuchenden Vorrichtung bereitgehalten wird, wobei zur Überprüfung der Zugangsberechtigung zu dem Zugangs (1) durch die Überprüfungsvorrichtung (3) bestimmt wird, ob die Originalkennung (OK(V)) unter Verwendung des hinterlegten Hauptschlüssels (Mutter$) und ggf. des hinterlegten ersten und/oder zweiten Verwenderschlüssels (V$) erzeugbar ist.

13. Verwendung nach Anspruch 12, dadurch gekennzeichnet, dass zumindest die Schritte a) und c) in einem ersten elektronischen Mittel (4) durchgeführt werden, das der

nachsuchenden Person oder der nachsuchenden Vorrichtung zugeordnet ist, wobei bevorzugt ein dem Zugang (1) zugeordnetes zweites elektronisches Mittel (5) Schritt b) ausführt und den Sitzungsschlüssel (ZZ$) oder das Ergebnis der Mischung von erstem zufälligem Sitzungsschlüssel und ersten Verwenderschlüssel zur Durchführung von Schritt c) an das erste elektronische Mittel (4) übermittelt.

14. Originalkennung hergestellt nach dem Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass die Originalkennung ein Barcode, insbesondere 1- oder 2-dimensionaler Barcode, oder eine Oberflächenstrukturierung ist oder in einem elektronischen Speicher, insbesondere einem RFID-Chip angeordnet ist.

15. Computerprogrammprodukt, das auf einem für einen Computer lesbaren Medium gespeichert ist, umfassend für den Computer lesbare Programmmittel, die den Computer veranlassen, ein Verfahren nach einem der Ansprüche 1 bis 8, insbesondere im Rahmen einer Verwendung nach einem der Ansprüche 9 bis 13 auszuführen, wenn die Programmmittel auf dem Computer ausgeführt werden.

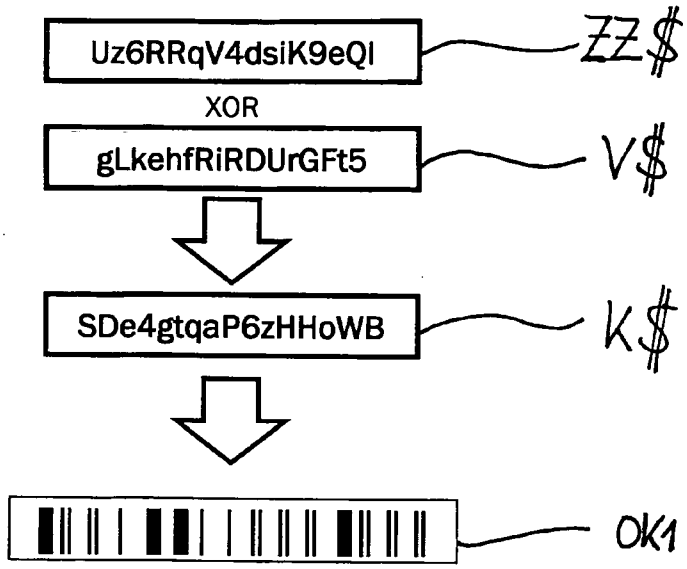

Uz6RRqV4dsiK9eQl
ZZ$
XOR
gLkehfRiRDUrGFt5
V$
SDe4gtqaP6zHHoWB
K$
OK1

Fig. 1


Datum : 130810
Zollstelle : 67 (Frankfurt)
Händler : 5677
Land : USA
Ausfuhr/Einfuhr : A
Produkt Nr.: J27031
Produkt : ABC
ABC J27031 A USA 5677 67 130810
G$
XOR
hrHU65saswFjhgREzdxztrdzdtdZ5BvC
OTP$
BvCHZGR44EwqaQQsarefdfkLJzvdSAlu
P$
OK2

Fig. 2b

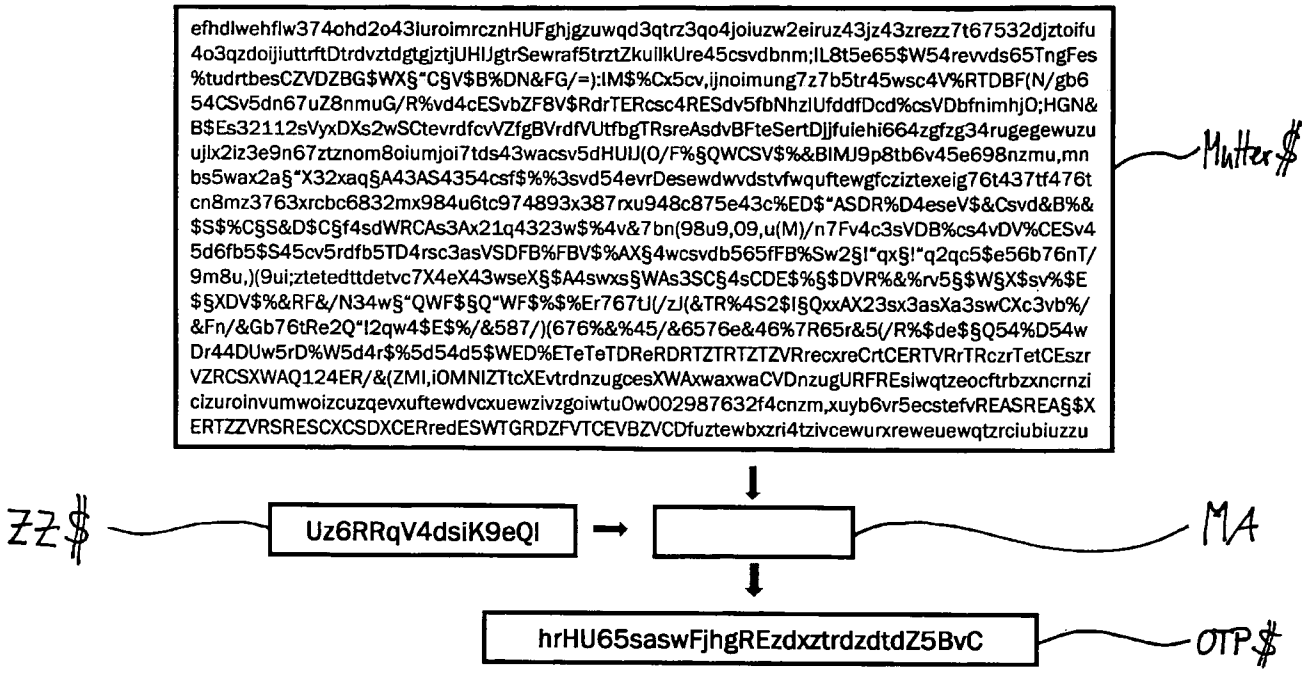

efhdlwehflw374ohd2o43luroimrcznHUFghjgzuwqd3qtrz3qo4joiuzw2eiruz43jz43zrezz7t67532djztoifu
4o3qzdoijiuttrftDtrdvztdgtgjztjUHIJgtrSewraf5trztZkullkUre45csvdbnm;IL8t5e65$W54revvds65TngFes
%tudrtbesCZVDZBG$WX§"C§V$B%DN&FG/=):IM$%Cx5cv,ijnoimung7z7b5tr45wsc4V%RTDBF(N/gb6
54CSv5dn67uZ8nmuG/R%vd4cESvbZF8V$RdrTERcsc4RESdv5fbNhzlUfddfDcd%csVDbfnimhjO;HGN&
B$Es32112sVyxDXs2wSCtevrdfcvVZfgBVrdfVUtfbgTRsreAsdvBFteSertDljfuiehi664zgfzg34rugegewuzu
ujlx2iz3e9n67ztznom8oiumjoi7tds43wacsv5dHUIJ(O/F%§QWCSV$%&BIMJ9p8tb6v45e698nzmu,mn
bs5wax2a§"X32xaq§A43AS4354csf$%%3svd54evrDesewdwvdstvfwquftewgfcziztexeig76t437tf476t
cn8mz3763xrcbc6832mx984u6tc974893x387rxu948c875e43c%ED$"ASDR%D4eseV$&Csvd&B%&
S%C§S&D$C§f4sdWRCAs3Ax21q4323w$%4v&7bn(98u9,09,u(M)/n7Fv4c3sVDB%cs4vDV%CESv4
5d6fb5$S45cv5rdfb5TD4rsc3asVSDFB%FBV$%AX§4wcsvdb565fFB%Sw2§!"qx§!"q2qc5$e56b76nT/
9m8u,)(9ui;ztetedttdetvc7X4eX43wseX§$A4swxs§WAs3SC§4sCDE$%§$DVR%&%rv5§$W§X$sv%$E
$§XDV$%&RF&/N34w§"QWF$§Q"WF$%$%Er767tJ(/zJ(&TR%4S2$I§QxxAX23sx3asXa3swCXc3vb%/
&Fn/&Gb76tRe2Q"I2qw4E%/&587/)(676%&%45/&6576e&46%7R65r&5(/R%de§Q54%D54w
Dr44DUw5rD%W5d4r$%5d54d5$WED%ETeTeTDReRDRTZTRTZTZVRrecxreCrtCERTVRrTRczrTetCEszr
VZRCSXWAQ124ER/&(ZMI,iOMNIZTtcXEvtrdnzugcesXWAxwaxwaCVDnzugURFREsiwqtzeocftrbzxncrnzi
cizuroinvumwoizcuzqevxuftewdvcxuewzivzgoiwtuOw002987632f4cnzm,xuyb6vr5ecstefvREASREA§$X
ERTZZVRSRESCXCSDXCERredESWTGRDZFVTCEVBZVCDfuztewbxzri4tzivcewurxreweuewqtzrciubiuzzu
Mutter$
ZZ$
Uz6RRqV4dsiK9eQl
MA
hrHU65saswFjhgREzdxztrdzdtdZ5BvC
OTP$

Fig. 2a


K$
P$
SDe4gtqaP6zHHoWB
BvCHZGR44EwqaQQsarefdfkLJzvdSAlu
Ok1
Ok2
OK

Fig. 3

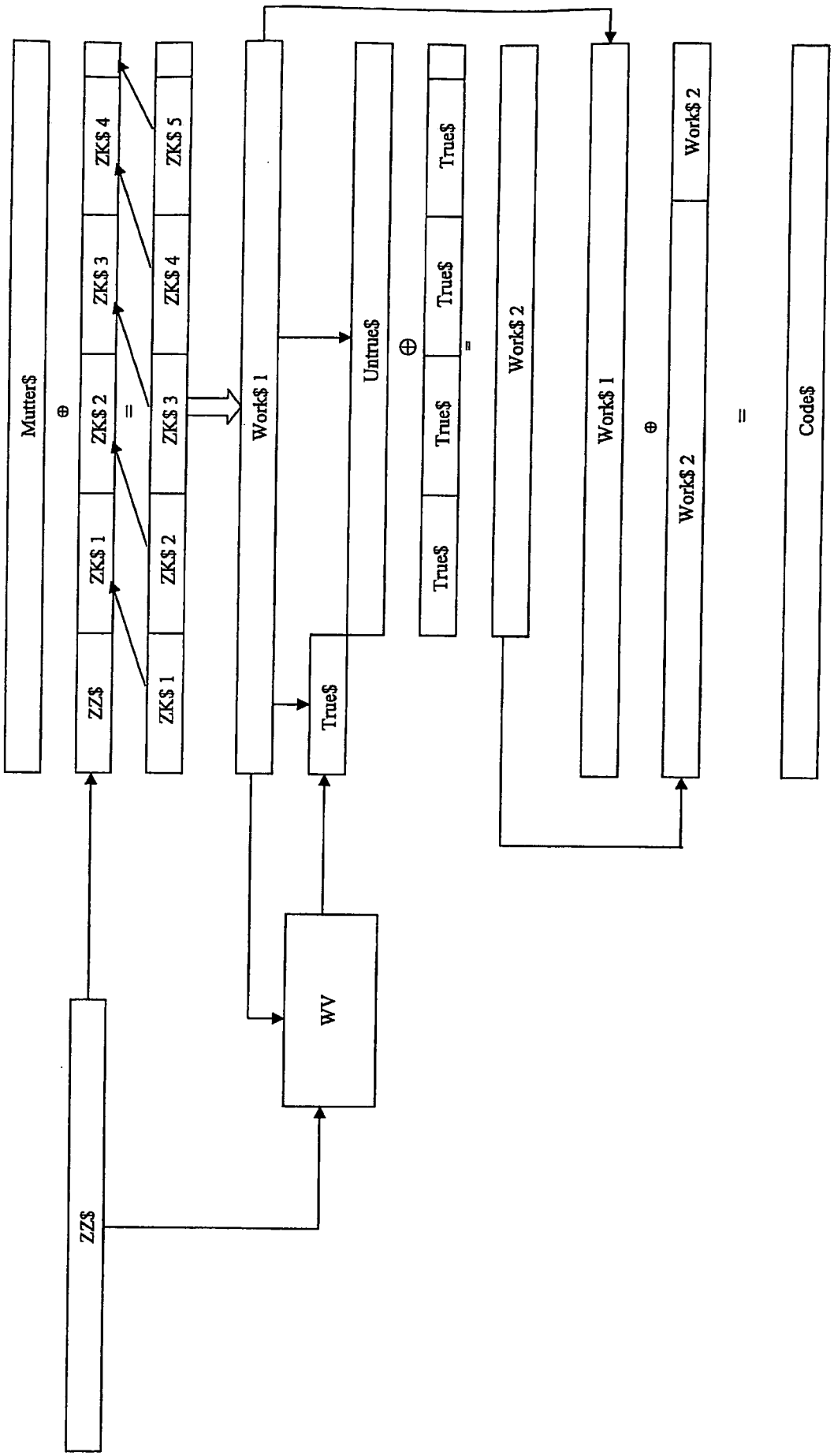

Mutter$
ZZ$
ZK$ 1
ZK$ 2
ZK$ 3
ZK$ 4
ZK$ 1
ZK$ 2
ZK$ 3
ZK$ 4
ZK$ 5
Work$ 1
True$
Untrue$
True$
True$
True$
Work$ 2
Work$ 1
Work$ 2
Work$ 2
Code$
ZZ$
WV

Fig. 4

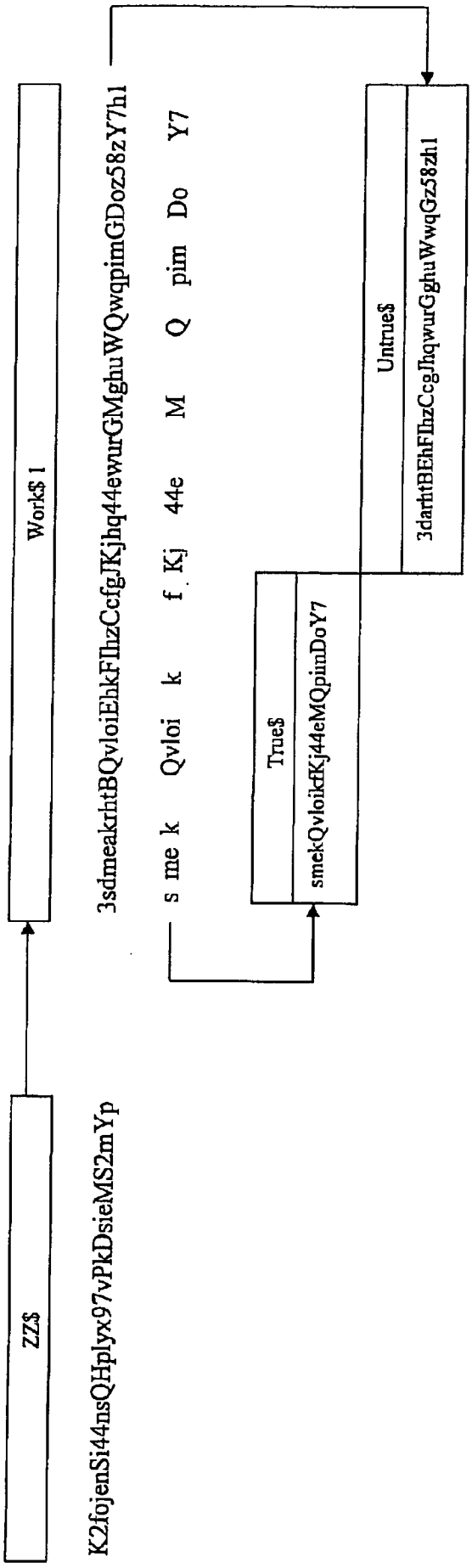

ZZ$
K2fojenSi44nsQHplyx97vPkDsieMS2mYp
Work$ 1
3sdmeakrhtBQvloiEhkFIhzCcfgJKjhq44ewurGMghuWQwqpimGDoz58zY7h1
s me k Qvloi k f Kj 44e M Q pim Do Y7
True$
smekQvloikfKj44eMQpinDoY7
Untrue$
3darhtBEhFIhzCcgIhqwurGghuWwqGz58zh1

Fig. 5

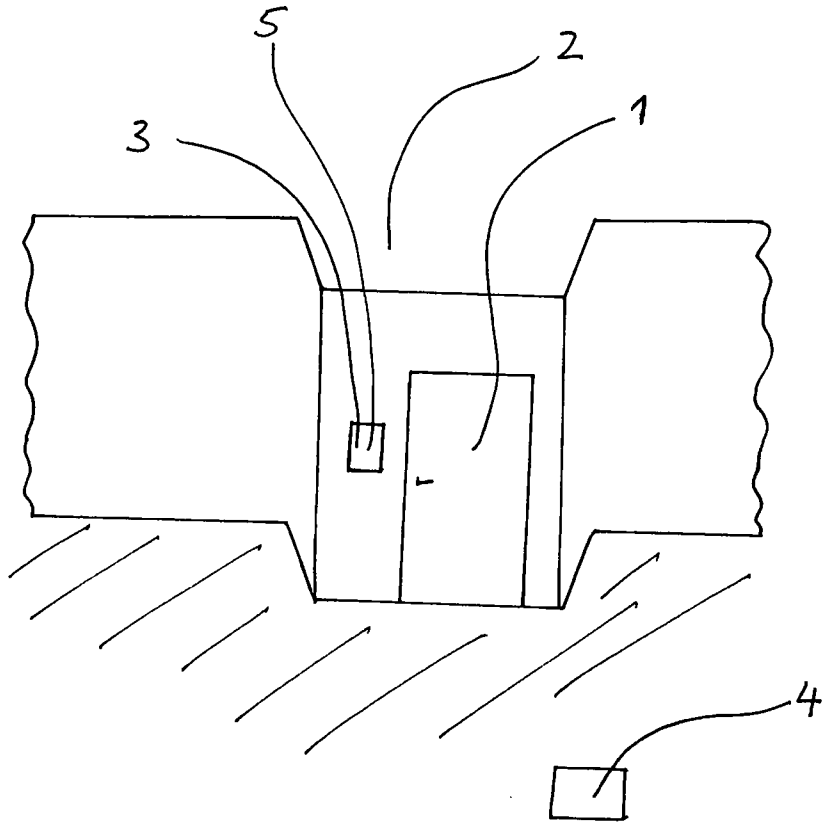


Fig. 6

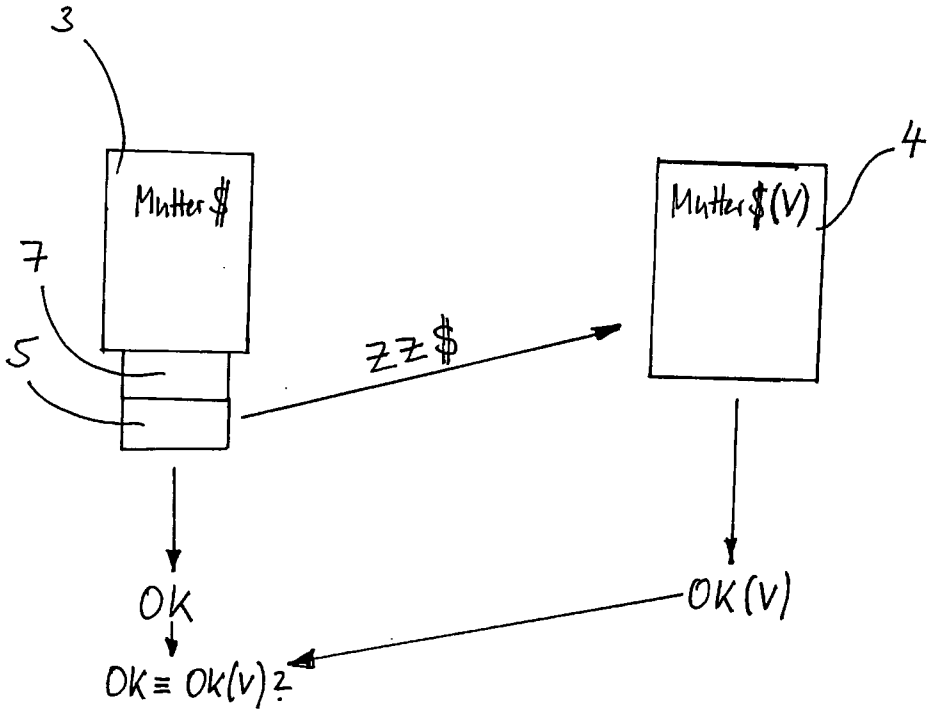


Fig. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/001356

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00 H04L9/32
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2005/024697 A2 (MOTOROLA INC [US]; COLLINS TIMOTHY J [US]; KUHLMAN DOUGLAS A [US]; MES) 17 March 2005 (2005-03-17) page 1 - page 2; figure 3	1-15
X	SCHNEIER B: "Applied Cryptography, PASSAGE" APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS AND SOURCE CODE IN C, WILEY, NEW YORK, NY, US, 1 January 1994 (1994-01-01), pages 30-37,42, XP002388093	1
Y	the whole document	1-15

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 July 2010	14/07/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Widera, Sabine

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/001356

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	BRUCE SCHNEIER ED - SCHNEIER B: "Applied Cryptography, One-Time Pads" 1 January 1996 (1996-01-01), APPLIED CRYPTOGRAPHY, PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C, JOHN WILEY & SONS, INC, NEW YORK, PAGE(S) 15 - 17 , XP002495601 ISBN: 978-0-471-11709-4 the whole document	1-15
Y	DE 10 2006 040228 A1 (GIESECKE & DEVRIENT GMBH [DE]) 6 March 2008 (2008-03-06) paragraphs [0011], [0039]; figures 1,2a,2b	1-15
X	WO 2008/148623 A1 (BUNDESDRUCKEREI GMBH [DE]; BYSZIO FRANK [DE]; WIRTH KLAUS-DIETER [DE]) 11 December 2008 (2008-12-11)	1
Y	page 5; figure 4	2-15
X	US 2006/235805 A1 (PENG FENG [US] ET AL) 19 October 2006 (2006-10-19)	1
Y	claim 1; figures 3-5	2-15
A	WO 2007/113464 A1 (BRITISH TELECOMM [GB]; SOPPERA ANDREA [GB]; BURBRIDGE TREVOR [GB]) 11 October 2007 (2007-10-11) * abstract	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2010/001356

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2005024697 A2	17-03-2005	EP 1661051 A2	31-05-2006
		US 2005049979 A1	03-03-2005
DE 102006040228 A1	06-03-2008	NONE	
WO 2008148623 A1	11-12-2008	DE 102007026836 A1	11-12-2008
		EP 2156602 A1	24-02-2010
US 2006235805 A1	19-10-2006	NONE	
WO 2007113464 A1	11-10-2007	CA 2644320 A1	11-10-2007
		CN 101410853 A	15-04-2009
		EP 2002382 A1	17-12-2008
		JP 2009531251 T	03-09-2009
		KR 20080108241 A	12-12-2008
		US 2009273451 A1	05-11-2009

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2010/001356

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F21/00 H04L9/32
ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F H04L

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 2005/024697 A2 (MOTOROLA INC [US]; COLLINS TIMOTHY J [US]; KUHLMAN DOUGLAS A [US]; MES) 17. März 2005 (2005-03-17) Seite 1 - Seite 2; Abbildung 3	1-15
X	SCHNEIER B: "Applied Cryptography, PASSAGE" APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS AND SOURCE CODE IN C, WILEY, NEW YORK, NY, US, 1. Januar 1994 (1994-01-01), Seiten 30-37,42, XP002388093	1
Y	das ganze Dokument	1-15
	-/--	

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
5. Juli 2010	14/07/2010

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Widera, Sabine

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2010/001356

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	BRUCE SCHNEIER ED - SCHNEIER B: "Applied Cryptography, One-Time Pads" 1. Januar 1996 (1996-01-01), APPLIED CRYPTOGRAPHY, PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C, JOHN WILEY & SONS, INC, NEW YORK, PAGE(S) 15 - 17 , XP002495601 ISBN: 978-0-471-11709-4 das ganze Dokument	1-15
Y	DE 10 2006 040228 A1 (GIESECKE & DEVRIENT GMBH [DE]) 6. März 2008 (2008-03-06) Absätze [0011], [0039]; Abbildungen 1,2a,2b	1-15
X	WO 2008/148623 A1 (BUNDESDRUCKEREI GMBH [DE]; BYSZIO FRANK [DE]; WIRTH KLAUS-DIETER [DE]) 11. Dezember 2008 (2008-12-11)	1
Y	Seite 5; Abbildung 4	2-15
X	US 2006/235805 A1 (PENG FENG [US] ET AL) 19. Oktober 2006 (2006-10-19)	1
Y	Anspruch 1; Abbildungen 3-5	2-15
A	WO 2007/113464 A1 (BRITISH TELECOMM [GB]; SOPPERA ANDREA [GB]; BURBRIDGE TREVOR [GB]) 11. Oktober 2007 (2007-10-11) * Zusammenfassung	1-15

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2010/001356

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 2005024697 A2	17-03-2005	EP 1661051 A2	31-05-2006
		US 2005049979 A1	03-03-2005
DE 102006040228 A1	06-03-2008	KEINE	
WO 2008148623 A1	11-12-2008	DE 102007026836 A1	11-12-2008
		EP 2156602 A1	24-02-2010
US 2006235805 A1	19-10-2006	KEINE	
WO 2007113464 A1	11-10-2007	CA 2644320 A1	11-10-2007
		CN 101410853 A	15-04-2009
		EP 2002382 A1	17-12-2008
		JP 2009531251 T	03-09-2009
		KR 20080108241 A	12-12-2008
		US 2009273451 A1	05-11-2009