(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 4 358 045 A1**

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
24.04.2024 Patentblatt 2024/17

(21) Anmeldenummer: **22203002.5**

(22) Anmeldetag: **21.10.2022**

(51) Internationale Patentklassifikation (IPC):
G07C 9/00 *(2020.01)* *G07C 9/21* *(2020.01)*
G07C 9/33 *(2020.01)*

(52) Gemeinsame Patentklassifikation (CPC):
G07C 9/00896; G07C 9/0069; G07C 9/21;
G07C 9/33; G07C 2009/0042; G07C 2009/00468

(84) Benannte Vertragsstaaten:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC ME MK MT NL NO PL PT RO RS SE SI SK SM TR
Benannte Erstreckungsstaaten:
BA
Benannte Validierungsstaaten:
KH MA MD TN

(71) Anmelder: **Carl Wittkopp GmbH**
42551 Velbert (DE)

(72) Erfinder: **Naumann, Jörg**
42555 Velbert (DE)

(74) Vertreter: **Brinkmann & Partner**
Patentanwälte
Partnerschaft mbB
Am Seestern 8
40547 Düsseldorf (DE)

(54) VERFAHREN ZUM BETRIEB EINES ELEKTRONISCHEN ZUGANGSSYSTEMS

(57) Die Erfindung betrifft ein Verfahren zum Betrieb eines elektronischen Zugangssystems mit zumindest einem elektronischen Schloss in einem, einem Nutzer temporär zur Verfügung gestellten Bereich, beispielsweise einem Zimmer in einem Hotel und/oder bei temporär vergebenen Wertaufbewahrungsverhältnissen, wie Hotelzimmertresoren oder Spinden in Sportstätten, an Arbeitsplätzen oder dgl., und einem vom Nutzer frei programmierbaren elektronischen Schlüssel zur Betätigung des elektronischen Schlosses, wobei das elektronische Schloss ergänzend mit einem zweiten, vom ersten elektronischen Schlüssel abweichenden elektronischen Schlüssel betätigbar ist, wobei im zweiten elektronischen Schlüssel ein Öffnungscode aus einem ersten Datensatz mit einem, im Schloss hinterlegten und für das Schloss eineindeutigen Installationscode und aus einem zweiten Datensatz mit einem Identifikationscode des Schlosses bereitgestellt wird, wobei aus dem Öffnungscode und einer einmaligen, aus dem Installationscode generierten Zufallskennung eine weitere, aus der Zufallskennung mit einer Streuwertfunktion berechneten Kennung erzeugt wird, wobei die weitere Kennung mit der Zufallskennung zu einem in das Schloss eingebbaren Notfallcode zusammengesetzt wird, der bei seiner Verwendung im Schloss überprüft wird, indem die Zufallskennung separiert und eine Rechenkennung aus dem Installationscode im Schloss und der Zufallskennung mit der identischen Streuwertfunktion berechnet und ein Ergebnis hieraus mit der berechneten Kennung verglichen wird, wobei ein Öffnungsvorgang des Schlosses ausgeführt wird, wenn die berechnete Kennung mit der Rechenkennung übereinstimmt, wobei anschließend die Rechenkennung und/oder die berechnete Kennung im Schloss und/oder im zweiten Schlüssel gelöscht oder für eine weitere Verwendung unbrauchbar gemacht wird.

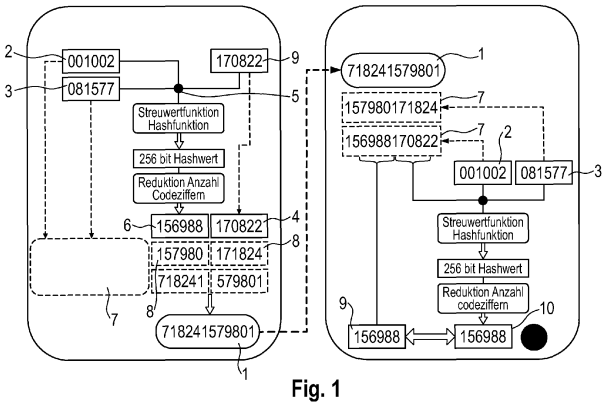

Fig. 1

EP 4 358 045 A1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Betrieb eines elektronischen Zugangssystems mit zumindest einem elektronischen Schloss in einem, einem Nutzer temporär zur Verfügung gestellten Bereich, beispielsweise einem Zimmer in einem Hotel und/oder bei temporär vergebenen Wertaufbewahrungsverhältnissen, wie Tresoren in Hotelzimmern oder Spinden in Sportstätten, an Arbeitsplätzen oder dgl, und einem vom Nutzer frei programmierbaren ersten elektronischen Schlüssel zur Betätigung des elektronischen Schlosses, wobei das elektronische Schloss ergänzend mit einem zweiten, vom ersten elektronischen Schlüssel abweichenden elektronischen Schlüssel betätigbar ist.

[0002] Aus dem Stand der Technik ist es bekannt, dass beispielsweise in Hotelzimmern Wertaufbewahrungsbehältnisse, beispielsweise in Kleiderschränken vorgesehen sind, die von einem Hotelgast zur Aufbewahrung von Wertgegenständen genutzt werden können. Um hier dem regelmäßigen Wechsel der Hotelgäste Rechnung tragen zu können ist eine einfache Programmierung eines in solchen Wertaufbewahrungsbehältnissen installierten elektronischen Schlosses erforderlich. In der Regel kann der Hotelgast einen persönlichen elektronischen Schlüssel in Form einer persönlichen Identifikationsnummer über eine nummerische Tastatur am Wertaufbewahrungsbehältnis generieren und über einen Programmierschritt das elektronische Schloss hierauf einstellen, so dass nachfolgend nur der Hotelgast diese persönliche Identifikationsnummer kennt und das Wertaufbewahrungsbehältnis öffnen kann. Die Programmierung des elektronischen Schlosses ist derart vorgesehen, dass die persönliche Identifikationsnummer immer wieder geändert werden kann, ohne dass es eines Eingriffs eines Administrators bedarf.

[0003] Somit kann der nachfolgende Hotelgast seine eigene persönliche Identifikationsnummer als elektronischen Schlüssel unabhängig von dem elektronischen Schlüssel des vorherigen Hotelgastes generieren und das elektronische Schloss entsprechend neu programmieren. Diese Vorgehensweise ist aber in der Regel nur dann möglich, wenn das Wertaufbewahrungsbehältnis geöffnet ist, d.h. das elektronische Schloss in einer Öffnungsstellung und nicht in der Schließstellung steht, so dass bei geschlossenem Wertaufbewahrungsbehältnis kein neuer elektronischer Schlüssel generiert werden kann.

[0004] Es ergeben sich somit zwei Szenarien, die eine Verwendung derartiger elektronischer Schlösser problematisch gestalten. Zum einen kann es sein, dass ein Hotelgast vor dem Verlassen seines Zimmers das elektronische Schloss des Wertaufbewahrungsbehältnisses mit seiner persönlichen Identifikationsnummer programmiert und geschlossen zurücklässt. Für den nachfolgenden Hotelgast ist ohne Kenntnis des elektronischen Schlüssels des vorherigen Hotelgastes die Nutzung des Wertaufbewahrungsbehältnisses nicht möglich. Zum anderen besteht die Möglichkeit, dass der Hotelgast seine persönliche Identifikationsnummer vergisst und somit das Wertaufbewahrungsbehältnis nicht mehr öffnen kann.

[0005] Für beide Fälle ist vorgesehen, dass das elektronische Schloss mit einem zweiten, vom ersten elektronischen Schlüssel abweichenden elektronischen Schlüssel betätigbar ist. Hierbei kann es sich auch um einen elektronischen Generalsschlüssel handeln, der auch das Öffnen einer Vielzahl von elektronischer Schlösser, beispielsweise in den Hotelzimmern installierter Wertaufbewahrungsbehältnisse ermöglicht. Dieser zweite elektronische Schlüssel beansprucht allerdings eine große Geheimhaltung, so dass dieser Schlüssel nur einem Administrator, im Zweifelsfall einer in einer Leitungsfunktion tätigen Person, beispielsweise einem Hotelmanager oder einer von einem Hotelmanager befugten Person übergeben wird.

[0006] Kommt es nun zu einer der beiden voranstehend beschriebenen Situationen und ist es erforderlich, dass das Wertaufbewahrungsbehältnis mit dem zweiten elektronischen Schlüssel geöffnet werden muss, so sollte dies nur durch die befugte Person erfolgen, die einen entsprechenden zweiten elektronischen Schlüssel kennt.

[0007] In der Praxis ist eine solche Vorgehensweise mitunter nicht durchführbar oder das Geheimhaltungsbedürfnis des zweiten elektronischen Schlüssels wird nicht ernst genommen, so dass der zweite elektronische Schlüssel einer beliebigen Person mitgeteilt wird, die diesen zweiten elektronischen Schlüssel dann unbefugt auch weiteren Personen mitteilen kann. Die gewünschte Sicherheit wird durch eine solche Vorgehensweise aufgeweicht und es können sich hieraus auch Haftungsprobleme für den Betreiber entsprechender Systeme aus einer Vielzahl von derartigen Wertaufbewahrungsbehältnissen ergeben, insoweit nachweislich eine unbegrenzte Zahl von Personen ggf. Kenntnis von dem zweiten elektronischen Schlüssel erhält und somit jedes Wertaufbewahrungsbehältnis, beispielsweise jeden Hotelzimmertresor öffnen kann.

[0008] Ein voranstehend beschriebenes Verfahren und die damit verbundenen Probleme sind auch bei Wertaufbewahrungsbehältnissen in Sportstätten, beispielsweise in Fitnesseinrichtungen gegeben. Auch hier werden den Mitgliedern oder Nutzern einer solchen Fitnesseinrichtung temporär Wertaufbewahrungsbehältnisse übergeben, um dort Kleidung und andere Wertgegenstände während des Aufenthalts in der Fitnesseinrichtung vor dem Zugriff Dritter zu schützen. Soweit in einer solchen Fitnesseinrichtung der zweite elektronische Schlüssel einer Vielzahl von Personen mitgeteilt wurde oder die Gefahr besteht, dass eine Person, die Kenntnis von dem zweiten elektronischen Schlüssel hat, diesen weitergegeben hat, bestehen auch hier große Gefahren für den Inhalt der temporär überlassenen Wertaufbewahrungsbehältnisse dahingehend, dass unbefugte mit dem zweiten elektronischen Schlüssel die Öffnung

des elektronischen Schlosses bewirken und die darin aufbewahrten Wertgegenstände unbefugt entnehmen können.

[0009] Auf der anderen Seite kann auf einen zweiten elektronischen Schlüssel nicht verzichtet werden, da Notöffnungen derartiger Wertaufbewahrungsbehältnisse regelmäßig erforderlich sind. Die diesbezüglich vorliegenden Gründe sind bereits voranstehend erläutert.

[0010] Ausgehend von dem voranstehend beschriebenen Stand der Technik ist es daher **Aufgabe** der Erfindung, ein gattungsgemäßes Verfahren zum Betrieb eines elektronischen Zugangssystems derart weiterzubilden, dass die Gefahr des unberechtigten Zugangs Dritter zu Wertaufbewahrungsbehältnissen deutlich reduziert wird, auch wenn der zweite elektronische Schlüssel an eine unbefugte Person weitergeben wird.

[0011] Die **Lösung** dieser Aufgabenstellung sieht bei einem erfindungsgemäßen Verfahren vor, dass im zweiten elektronischen Schlüssel ein Öffnungscode aus einem ersten Datensatz mit einem, im Schloss hinterlegten und für das Schloss eineindeutigen Installationscode und aus einem zweiten Datensatz mit einem Identifikationscode des Schlosses bereitgestellt wird, wobei aus dem Öffnungscode und einer einmaligen, aus dem Installationscode generierten Zufallskennung eine weitere, aus der Zufallskennung mit einer Streuwertfunktion berechneten Kennung erzeugt wird, wobei die weitere Kennung mit der Zufallskennung zu einem, in das Schloss eingebbaren Notfallcode zusammengesetzt wird, der bei seiner Verwendung im Schloss überprüft wird, indem die Zufallskennung separiert und eine Rechenkennung aus dem Installationscode im Schloss und der Zufallskennung mit der identischen Streuwertfunktion berechnet und ein Ergebnis hieraus mit der berechneten Kennung verglichen wird, wobei ein Öffnungsvorgang des Schlosses ausgeführt wird, wenn die berechnete Kennung mit der Rechenkennung übereinstimmt, wobei anschließend die Rechenkennung und/oder die berechnete Kennung im Schloss und/oder im zweiten Schlüssel gelöscht oder für eine weitere Verwendung unbrauchbar gemacht wird.

[0012] Der wesentliche Gedanke der Erfindung liegt somit darin, dass der zweite elektronische Schlüssel nur in einer begrenzten Anzahl zur Notöffnung, insbesondere nur einmal verwendbar ist. Hierdurch wird vermieden, dass ein einmal herausgegebener zweiter elektronischer Schlüssel fortan Verwendung auch durch unberechtigte Personen finden kann. Um nun dieses vorteilhafte Verfahren umsetzen zu können, sind weitere erfindungsgemäße Verfahrensschritte notwendig.

[0013] Zu diesem Zweck ist in einem ersten Schritt ein Öffnungscode im zweiten elektronischen Schlüssel zu generieren. Dieser Öffnungscode setzt sich aus einem ersten Datensatz und einem zweiten Datensatz zusammen. Der erste Datensatz enthält einen, im elektronischen Schloss hinterlegten und für das elektronische Schloss eineindeutigen Installationscode. Der zweite Datensatz enthält einen Identifikationscode des elektrischen Schlosses, wobei es sich beispielsweise um eine räumliche Anordnung in beispielsweise einem Hotelzimmer handeln kann. Dieser Identifikationscode kann beispielsweise die Zimmernummer sein, die ergänzend verschlüsselt sein kann. Es ist möglich, dass neben dem Installationscode und dem Identifikationscode weitere Bestandteile eines Codes hinterlegt sind.

[0014] Der Öffnungscode wird nun aus einer einmaligen, aus dem Installationscode generierten Zufallskennung und einer weiteren, aus der Zufallskennung mit einer Streuwertfunktion berechneten Kennung erzeugt. Anschließend wird die weitere Kennung, nämlich die aus der Zufallskennung mit der Streuwertfunktion berechnete Kennung mit der Zufallskennung zu einem in das Schloss eingebbaren Notfallcode zusammengesetzt. Dieser Notfallcode wird an die Person übertragen, die das elektronische Schloss mit dem zweiten elektronischen Schlüssel öffnen soll. Nach Eingabe des Notfallcodes wird dieser bei seiner Verwendung im elektronischen Schloss überprüft. Hierzu wird die Zufallskennung im Notfallcode von der weiteren Kennung separiert und eine Rechenkennung aus dem Installationscode im Schloss und der Zufallskennung mit der identischen Streuwertfunktion berechnet. Ein hieraus erzieltes Ergebnis wird anschließend mit der berechneten Kennung verglichen, wobei ein Öffnungsvorgang des Schlosses ausgeführt wird, wenn die berechnete Kennung mit der Rechenkennung übereinstimmt. Wird somit bei einer solchen Übereinstimmung ein zutreffender Notfallcode verwendet, öffnet das elektronische Schloss durch Verwendung des zweiten elektronischen Schlüssels. Im Anschluss an einen solchen Öffnungsvorgang wird sodann die Rechenkennung und/oder die berechnete Kennung im elektronischen Schloss und/oder im zweiten Schlüssel gelöscht bzw. für eine weitere Verwendung unbrauchbar gemacht. Beispielsweise kann dies dadurch erfolgen, dass die Rechenkennung und/oder die berechnete Kennung im elektronischen Schloss und/oder im zweiten Schlüssel auf eine sogenannte Black-List gesetzt wird, so dass eine weitere Verwendung nicht möglich ist.

[0015] Durch das erfindungsgemäße Verfahren kann somit für jede Öffnung eines elektronischen Schlosses ein singulärer zweiter elektronischer Schlüssel generiert und einmalig zur Öffnung des elektronischen Schlosses verwendet werden. Zur Überprüfung des elektronischen Schlosses findet zum einen eine Berechnung im elektronischen Schlüssel und eine weitere Berechnung im elektronischen Schloss statt, die bei übereinstimmendem Ergebnis den zuvor im elektronischen Schlüssel zusammengesetzten Notfallcode ein Öffnen des elektronischen Schlosses ermöglicht.

[0016] Von Bedeutung ist hierbei die Generierung einer Zufallskennung im zweiten elektronischen Schlüssel, die unter anderem auch in einem zentralen Rechner eines Administrators erfolgen kann, auf deren Basis dann mit einer bestimmten Streuwertfunktion eine Kennung berechnet wird. Die Streuwertfunktion ist auch dem elektronischen Schloss bekannt und aus der Übermittlung eines erkennbar zweiteiligen Notfallcodes an das elek-

tronische Schloss ist das elektronische Schloss durch Kenntnis der Streuwertfunktion und durch die Möglichkeit des Zerlegens des Notfallcodes und Separierung der Zufallskennung in der Lage, den Notfallcode auf Zulässigkeit zu überprüfen.

[0017] In der Praxis kann somit der zweite elektronische Schlüssel, bei dem es sich beispielsweise um eine persönliche Identifikationsnummer handeln kann, die über eine Tastatur als Schlüssel eingegeben werden kann, von einer berechtigten Person, beispielsweise einem Hotelmanager an zentraler Stelle als Administrator erzeugt werden. Der zweite elektronische Schlüssel wird nach seiner Erzeugung in Klarschrift, beispielsweise in Form eines vier- oder sechsstelligen Zifferncodes ausgegeben und in der Folge in das mit dem zweiten elektronischen Schlüssel zu öffnende elektronische Schloss eingegeben, so dass auch im elektronischen Schloss in einer Art Rückwärtsrechnung eine Überprüfung des Notfallcodes stattfindet, bevor das elektronische Schloss bei Überprüfung und richtigem Ergebnis geöffnet wird.

[0018] Nach einem weiteren Merkmal der Erfindung ist vorgesehen, dass der im zweiten elektronischen Schlüssel und im Schloss hinterlegte Installationscode zum einen aus einer lokalen Anordnung und zum anderen aus einer Identifikation des Schlosses ausgebildet wird. Bei der Installation des elektronischen Schlosses wird diesem einmal eine individuelle Kennzeichnung gegeben. Diese besteht beispielsweise aus einer Kennung für die lokale Anordnung, beispielsweise in Form einer Gebäude- oder Bereichsnummer sowie einer Kennung für das Schloss, beispielsweise eine Zimmernummer.

[0019] Grundsätzlich ist die Länge eines einzugebenden Codes, somit auch des Installationscodes oder einer Identifikationsnummer beliebig skalierbar. Dennoch hat es sich als vorteilhaft erwiesen, die berechnete Kennung und/oder die Zufallskennung auf eine bestimmte Länge, insbesondere bestehend aus einzelnen Ziffern, zu verkürzen. Vorzugsweise handelt es sich um eine jeweils sechsstellige dezimale Ziffernfolge. Die Kennung, beispielsweise die Gebäudenummer ist nur einer Person bekanntzugeben. Die alleinige Weitergabe dieser Kennung ist aber nicht ausreichend, um einen Notöffnungscode zu generieren.

[0020] Vorzugsweise wird die einmalige Zufallskennung in einem zentralen Rechnersystem generiert. Soll nun also eine Notöffnung eines elektronischen Schlosses durchgeführt werden, so muss der berechtigten Person die Kennung, beispielsweise die Zimmernummer mitgeteilt werden, anhand derer die Schlossidentifikation ermittelt werden kann. Die weitere Kennung, beispielsweise die Gebäudenummer ist der handhabenden und berechtigten Person bekannt bzw. kann in einer Softwareapplikation hinterlegt sein. Diese Softwareapplikation kann sodann einen sechsstelligen Zufallswert erzeugen.

[0021] Aus dem Zufallswert, der Kennung für das Gebäude und der Kennung für das elektronische Schloss wird unter Zuhilfenahme der Streuwertfunktion ein im Prinzip nicht rückrechenbarer Wert erzeugt. Hierzu wird ein SHA-Algorithmus genutzt. Im Anschluss hieran wird der Wert auf sechs Stellen reduziert. Hierbei handelt es sich um den Zufallswert. Ausgegeben wird aber ein Notfallcode, bestehend aus zwölf Stellen und bestehend aus der Zufallszahl und einem berechneten, reduzierten Wert. Der ausgegebene Notfallcode kann dann in das elektronische Schloss eingegeben werden. Zuvor kann es erforderlich sein, einen bestimmten Menüpunkt im elektronischen Schloss anzuwählen, beispielsweise durch Bestätigung einer bestimmten Tastenkombination oder durch Betätigung einer bestimmten Taste über einen bestimmten längeren Zeitraum. Hierdurch erhält das elektronische Schloss die Information, einen Menüpunkt anzuwählen, in dem die Aufnahme des Notfallcodes möglich ist.

[0022] Im Schloss selbst wird aus Zufallswert, gespeicherter Kennung für das Gebäude und der Kennung des Schlosses, beispielsweise der Zimmernummer über die gleiche Streuwertfunktion ein Rechenwert errechnet und nach, bei der Generierung des Notfallcodes verwendeten gleichem eineindeutigem Schema reduziert und mit dem eingegebenen Wert verglichen. Wird bei diesem Vergleich festgestellt, dass die Werte identisch sind, wird der Öffnungsvorgang des elektronischen Schlosses bewirkt.

[0023] Demzufolge ist es weiterhin vorteilhaft, dass die einmalige Zufallskennung in einem zentralen Rechnersystem generiert wird, da in diesem Rechnersystem beispielsweise die Zugangsberechtigungen, insbesondere der zugangsberechtigten Person hinterlegt sein können, so dass diese auch nur nach Eingabe ihrer Zugangsberechtigung eine einmalige Zufallskennung generieren kann. Es ist demnach nicht notwendig, dass die berechtigte Person neben einer Zugangsberechtigung und einer Identifikation des mit dem Notfallcode zu öffnenden Schlosses weitere Werte kennt. Der Notfallcode kann in diesem Fall durch ausschließliche Eingabe der Zugangsberechtigung der berechtigten Person und der Identifikation des zu öffnenden Schlosses generiert werden und auch nur einmalig bei diesem Schloss verwendet werden.

[0024] Der in das Schloss einzugebende Notfallcode wird sodann im Schloss in die berechnete Kennung und die Zufallskennung aufgeteilt.

[0025] Um nachträglichen Missbrauch mit einem solchen Notfallcode zu vermeiden, wird die Rechenkennung nach Eingabe des Notfallcodes in das Schloss einer Black-List hinzugefügt und für weitere Öffnungsvorgänge unbrauchbar gemacht. Diese Rechenkennung kann daher auch für weitere Berechnungen nicht verwendet werden.

[0026] Es ist ferner nach einem weiteren Merkmal der Erfindung vorgesehen, dass der Identifikationscode kodiert im zweiten Datensatz abgelegt wird, wobei eine Dekodierung des Identifikationscodes vorzugsweise über eine, insbesondere auf einem Smartphone und/oder Tablet-PC installierten Anwendungssoftware (App) durch-

geführt wird. Hierdurch werden weitere Sicherheitskriterien geschaffen, nämlich eine weitergehende Berechnung und Verschlüsselung des Identifikationscodes durch die Anwendungssoftware.

[0027] Der Installationscode wird nicht auslesbar im Schloss und/oder Schlüssel abgelegt. Es handelt sich aber ohnehin um eine einmalige individuelle Kennzeichnung des Schlosses, so dass dieser Installationscode auch nur für dieses Schloss und nicht für ein weiteres Schloss existiert.

[0028] Als geeignete Streuwertfunktion hat sich eine Streuwertfunktion SHA 256bit als verwendbar und ausreichend sicher erwiesen. Diese Streuwertfunktion erzeugt größere Hashwerte, wobei die SHA 256bit die Länge des Hashwerts in bit angibt.

[0029] Wie bereits ausgeführt, wird der Notfallcode zwölfstellig ausgebildet und die berechnete Kennung und die Rechenkennung werden mit einer übereinstimmenden Länge ausgebildet. Demzufolge haben die berechnete Kennung und die Rechenkennung jeweils sechs Ziffern.

[0030] Um eine höhere Sicherheit zu gewähren, kann die Berechnung unter einer Verrauschung, beispielsweise durch Substitution und/oder Rotation ausgeführt werden. Die Verrauschung wird im elektronischen Schloss herausgerechnet, so dass die Zufallszahl extrahiert und ein one-time-Code über denselben Hashwert-Algorithmus berechnet wird.

[0031] Weitere Merkmale und Vorteile der Erfindung ergeben sich aus der nachfolgenden Beschreibung eines Ausführungsbeispiels, das in der Figur als Ablaufdiagramm dargestellt ist.

[0032] Die Figur zeigt in ihrem linken Teil die Verfahrensschritte zur Generierung eines Notfallcodes 1 als zweiten elektronischen Schlüssel für die Öffnung eines elektronischen Schlosses. Im rechten Teil der Figur ist die Verarbeitung des generierten Notfallcodes 1 im elektronischen Schloss dargestellt.

[0033] Das elektronische Schloss hat eine Schlosskennung, die als Installationscode 2 vorgesehen ist. Des Weiteren ist ein Institutsschlüssel als Identifikationscode 3 hinterlegt. Sowohl der Installationscode 2 als auch der Identifikationscode 3 sind im elektronischen Schloss hinterlegt und werden später zur Überprüfung des generierten Notfallcodes 1 benötigt.

[0034] Bei der Generierung des Notfallcodes 1 wird nun in einer Softwareapplikation eine Zufallszahl generiert, die als Zufallskennung 4 dient.

[0035] Ein Öffnungscode 5 wird aus dem Installationscode 2 und dem Identifikationscode 3 bereitgestellt, wobei aus dem Öffnungscode 5 und der einmaligen, aus dem Installationscode 3 generierten Zufallskennung 4 eine weitere, aus der Zufallskennung 4 mit einer Streuwertfunktion berechneten Kennung 6 erzeugt wird, der hier als OTC-Code dient.

[0036] Diese berechnete Kennung 6 wird mit der Zufallskennung 4 zu dem in das Schloss eingebbaren Notfallcode 1 zusammengesetzt, nachdem sowohl die berechnete Kennung 6, als auch die Zufallskennung 4 einer Verrauschung 7 unterworfen wird, indem in einem ersten Schritt der Verrauschung 7 zu der berechneten Kennung 6 und zu der Zufallskennung 4 jeweils der Installationscode 2, also eine spezifische Größe des Schlosses addiert wird, bevor bei Zufallskennung 4 und berechneter Kennung 6 ergänzend die erste Ziffer 8 gelöscht und identisch an die verbleibende Ziffernfolge der berechneten Kennung 6 und der Zufallskennung 4 angehängt wird. In einem weiteren Schritt wird sodann die Zufallskennung 4 kreuzweise mit der berechneten Kennung 6 ausgetauscht und die Zufallskennung 4 und die berechnete Kennung 6 zum Notfallcode 1 zusammengesetzt.

[0037] Die Zufallskennung 4 und die berechnete Kennung 6 bestehen aus jeweils sechs Ziffern, so dass der daraus zusammengesetzte Notfallcode 1 zwölf Ziffern aufweist.

[0038] Dieser Notfallcode 1, der beispielsweise von einem Administrator an einem Rechner unter Heranziehung einer Software im Zuge eines Algorithmus erstellt wird, kann sodann an eine Person als zweiter Schlüssel für die Öffnung des elektronischen Schlosses übergeben werden. Dies kann auch durch eine digitale Übermittlung des Notfallcodes 1 erfolgen. Denkbar ist auch, dass der Notfallcode 1 als Barcode oder als QR-Code übermittelt werden, soweit das Schloss ein Lesegerät zur Einlesung eines solchen Codes aufweist.

[0039] Gemäß dem rechten Teil der Figur wird dieser Notfallcode 1 sodann, beispielsweise über eine nicht dargestellte Tastatur in das elektronische Schloss eingegeben.

[0040] In dem elektronischen Schloss wird in einem ersten Schritt der Notfallcode 1 in zwei Teile mit übereinstimmender Anzahl von Ziffern unterteilt. Im vorliegenden Ausführungsbeispiel wird der zwölfstellige Notfallcode 1 in zwei sechsstellige Teile unterteilt, bevor sodann die zuvor bei der Generierung des Notfallcodes 1 ausgeführte Rotation rückgängig gemacht wird, d.h. die letzte Ziffer der beiden sechsstelligen Teile des Notfallcodes 1 jeweils gestrichen und an die erste Stelle der jeweils sechsstelligen Teile des getrennt Notfallcodes 1 gesetzt werden. Nachfolgend wird sodann der Installationscode 2, der in dem elektronischen Schloss zur eineindeutigen Identifikation hinterlegt ist, von beiden Teilen des Notfallcodes 1 subtrahiert. Hieraus ergibt sich zum einen ein erster Teil des Notfallcodes 1, der als Prüfcode 9 bereitgehalten wird.

[0041] Aus einem zweiten Teil des bearbeiteten Notfallcodes 1 wird sodann unter Zuhilfenahme des Installationscodes 2 und des Identifikationscodes 3 und der identischen Streuwertfunktion eine weitere Kennung 10 berechnet, die mit dem Prüfcode 9 verglichen wird und sollte dieser Vergleich zu einer Identität der weiteren Kennung 10 und des Prüfcodes 9, wird das elektronische Schloss geöffnet.

[0042] Die ermittelte Zufallskennung und deren Veränderungen bei der Generierung des Notfallcodes 1 werden abschließend in einem Ringspeicher in einer soge-

nannten Black-List geführt, so dass deren mehrmalige Verwendung ausgeschlossen ist.

Bezugszeichen

[0043]

1 Notfallcode
2 Installationscode
3 Identifikationscode
4 Zufallskennung
5 Öffnungscode
6 berechnete Kennung
7 Verrauschung
8 erste Ziffer
9 Prüfcode
10 weitere Kennung

Patentansprüche

1. Verfahren zum Betrieb eines elektronischen Zugangssystems mit zumindest einem elektronischen Schloss in einem, einem Nutzer temporär zur Verfügung gestellten Bereich, beispielsweise einem Zimmer in einem Hotel und/oder bei temporär vergebenen Wertaufbewahrungsbehältnissen, wie Tresoren in Hotelzimmern oder Spinden in Sportstätten, an Arbeitsplätzen oder dergleichen, und einem vom Nutzer frei programmierbaren ersten elektronischen Schlüssel zur Betätigung des elektronischen Schlosses, wobei das elektronische Schloss ergänzend mit einem zweiten, vom ersten elektronischen Schlüssel abweichenden elektronischen Schlüssel betätigbar ist,
dadurch gekennzeichnet,
dass im zweiten elektronischen Schlüssel ein Öffnungscode aus einem ersten Datensatz mit einem, im Schloss hinterlegten und für das Schloss eineindeutigen Installationscode und aus einem zweiten Datensatz mit einem Identifikationscode des Schlosses bereitgestellt wird, wobei aus dem Öffnungscode und einer einmaligen, aus dem Installationscode generierten Zufallskennung eine weitere, aus der Zufallskennung mit einer Streuwertfunktion berechneten Kennung erzeugt wird, wobei die weitere Kennung mit der Zufallskennung zu einem in das Schloss eingebbaren Notfallcode zusammengesetzt wird, der bei seiner Verwendung im Schloss überprüft wird, indem die Zufallskennung separiert und eine Rechenkennung aus dem Installationscode im Schloss und der Zufallskennung mit der identischen Streuwertfunktion berechnet und ein Ergebnis hieraus mit der berechneten Kennung verglichen wird, wobei ein Öffnungsvorgang des Schlosses ausgeführt wird, wenn die berechnete Kennung mit der Rechenkennung übereinstimmt, wobei anschließend die Rechenkennung und/oder die berechnete Kennung im Schloss und/oder im zweiten Schlüssel gelöscht oder für eine weitere Verwendung unbrauchbar gemacht wird.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
dass der im zweiten elektronischen Schlüssel und im Schloss hinterlegte Installationscode zum einen aus einer lokalen Anordnung und zum anderen aus einer Identifikation des Schlosses ausgebildet wird.

3. Verfahren nach Anspruch 1 oder 2,
dadurch gekennzeichnet,
dass die berechnete Kennung und/oder die Zufallskennung auf eine bestimmte Länge, insbesondere bestehend aus einzelnen Ziffern verkürzt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet,
dass die einmalige Zufallskennung in einem zentralen Rechnersystem generiert wird.

5. Verfahren nach einem der Ansprüche 1 bis 4,
dadurch gekennzeichnet,
dass der in das Schloss eingegebene Notfallcode im Schloss in die berechnete Kennung und die Zufallskennung aufgeteilt wird.

6. Verfahren nach einem der Ansprüche 1 bis 5,
dadurch gekennzeichnet,
dass die Rechenkennung nach Eingabe in das Schloss einer Black-List hinzugefügt und für weitere Öffnungsvorgänge unbrauchbar gemacht wird.

7. Verfahren nach einem der Ansprüche 1 bis 6,
dadurch gekennzeichnet,
dass der Identifikationscode codiert im zweiten Datensatz abgelegt wird, wobei eine Decodierung des Identifikationscodes vorzugsweise über eine insbesondere auf einem Smartphone und/oder Tablett-PC installierten Anwendungssoftware (APP) durchgeführt wird.

8. Verfahren nach einem der Ansprüche 1 bis 7,
dadurch gekennzeichnet,
dass der Installationscode nicht auslesbar im Schloss und/oder Schlüssel abgelegt wird.

9. Verfahren nach einem der Ansprüche 1 bis 8,
dadurch gekennzeichnet,
dass als Streuwertfunktion eine SHA 256 bit verwendet wird.

10. Verfahren nach einem der Ansprüche 1 bis 9,
dadurch gekennzeichnet,
dass der Notöffnungscode 12-stellig ausgebildet wird und die berechnete Kennung und die Rechenkennung eine übereistimmende Länge haben.

11. Verfahren nach einem der Ansprüche 1 bis 10,
dadurch gekennzeichnet,
dass die Berechnung unter einer Verrauschung, beispielsweise durch Substitution und/oder Rotation ausgeführt wird.

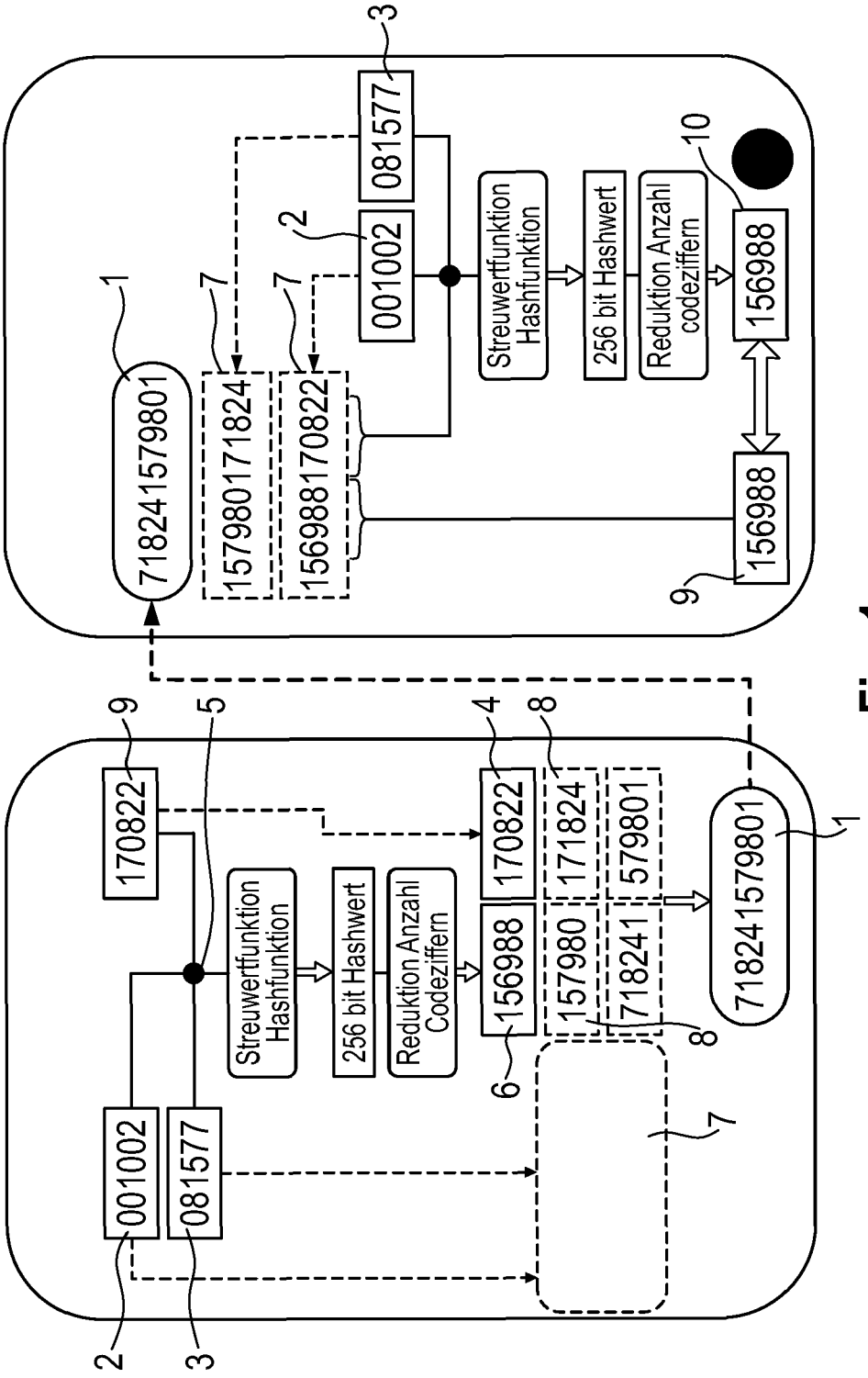
718241579801
157980171824
156988170822
001002
081577
Streuwertfunktion Hashfunktion
256 bit Hashwert
Reduktion Anzahl codeziffern
156988
170822
171824
157980
718241
579801
1
2
3
4
5
6
7
8
9
10

Fig. 1

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 22 20 3002

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X	DE 38 12 201 A1 (SCHULTE SCHLAGBAUM AG [DE]) 26. Oktober 1989 (1989-10-26) * das ganze Dokument *	1-11	INV. G07C9/00 ADD. G07C9/21 G07C9/33
A	US 5 349 345 A (VANDERSCHEL DAVID J [US]) 20. September 1994 (1994-09-20) * Spalte 13 - Spalte 14 *	1-11	
A	US 2005/219037 A1 (HUANG TAO [CA]) 6. Oktober 2005 (2005-10-06) * Absätze [0063] - [0088] *	1-11	
A	CN 114 495 333 A (QINGDAO HAIXIN MOBILE COMMUNICATION TECH CO LTD) 13. Mai 2022 (2022-05-13) * Abbildung 12 * * Absätze [0163] - [0168] *	1-11	

RECHERCHIERTE SACHGEBIETE (IPC)

G07C

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
Den Haag	22. März 2023	Pfyffer, Gregor

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 22 20 3002

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

22-03-2023

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 3812201 A1	26-10-1989	KEINE	
US 5349345 A	20-09-1994	KEINE	
US 2005219037 A1	06-10-2005	KEINE	
CN 114495333 A	13-05-2022	KEINE	

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82