

(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
18. Mai 2017 (18.05.2017)



(10) Internationale Veröffentlichungsnummer
WO 2017/080907 A1

(51) Internationale Patentklassifikation:

H04L 29/06 (2006.01) **H04B 10/116** (2013.01)
H04L 9/08 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2016/076547

(22) Internationales Anmeldedatum:
3. November 2016 (03.11.2016)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2015 222 450.3
13. November 2015 (13.11.2015) DE

(71) Anmelder: **OSRAM GMBH** [DE/DE]; Marcel-Breuer-
Straße 6, 80807 München (DE). **OSRAM SYLVANIA**
INC. [US/US]; 200 Ballardvale Street, Wilmington, MA
01887 (US).

(72) Erfinder: **FEIL, Henry**; Nordstrasse 5, 82008
Unterhaching (DE). **STOUT, Barry**; 9 Old Town Road,
Beverly, Massachusetts 01915 (US).

(81) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare nationale Schutzrechtsart): AE, AG, AL,

AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW,
BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK,
DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM,
GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP,
KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,
NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU,
RW, SA, 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.

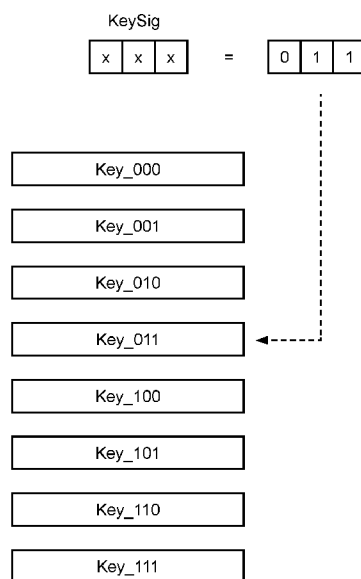
(84) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare regionale Schutzrechtsart): ARIPO (BW,
GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST,
SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG,
KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH,
CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR,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

Veröffentlicht:

— mit internationalem Recherchenbericht (Artikel 21 Absatz
3)

(54) Title: LIGHTING DEVICE AND METHOD FOR PROVIDING DATA TRANSFER TO A MOBILE TERMINAL

(54) Bezeichnung : BELEUCHTUNGSEINRICHTUNG UND VERFAHREN ZUR BEREITSTELLUNG EINER
DATENÜBERTRAGUNG AN EIN MOBILES ENDGERÄT



(57) Abstract: The invention relates to a lighting device (12) for providing data transfer to a mobile terminal (14), comprising a lighting means (13) and an electronic operating device (11) for operating the lighting means. In a data memory unit, a set of first keys (Key_000 to Key_111) is stored in a memory area reserved therefor. A selection unit selects a first key from the set of first keys in accordance with a key-change signal that can be provided at a data interface of the lighting device and/or in accordance with a key-change signal that is internal to the lighting device and that can be provided by a key-change timing generator of the lighting device. An encryption unit reads out the selected first key from the reserved memory area and, in accordance with a specifiable encryption operation, converts measurement value data and/or identification data (ID) intended to be transferred to the mobile terminal into a message (code) encrypted by means of the selected first key. A transmitting unit (13, 16) transmits the encrypted message to the mobile terminal. The invention further relates to a system (100) having at least two lighting devices according to the invention, each having a separate set of first keys. The invention further relates to a corresponding method.

(57) Zusammenfassung:

[Fortsetzung auf der nächsten Seite]

Fig.8



Die Erfindung betrifft eine Beleuchtungseinrichtung (12) zur Bereitstellung einer Datenübertragung an ein mobiles Endgerät (14), umfassend ein Leuchtmittel (13) und ein elektronisches Betriebsgerät (11) zum Betreiben des Leuchtmittels. In einer Datenspeichereinheit ist in einem dafür reservierten Speicherbereich ein Satz von ersten Schlüsseln (Key_000 bis Key_III) gespeichert. Eine Auswahleinheit wählt in Abhängigkeit von einem an einer Datenschnittstelle der Beleuchtungseinrichtung bereitstellbaren Schlüsselwechselsignal und/oder in Abhängigkeit von einem durch einen Schlüsselwechseltaktgeber der Beleuchtungseinrichtung bereitstellbaren beleuchtungseinrichtungsinternen Schlüsselwechselsignal einen ersten Schlüssel aus dem Satz von ersten Schlüsseln aus. Eine Verschlüsselungseinheit liest den ausgewählten ersten Schlüssel aus dem reservierten Speicherbereich aus und setzt Messwertedaten und/oder Identifikationsdaten (ID), welche zur Übertragung an das mobile Endgerät bestimmt sind, gemäß einer vorgebbaren Verschlüsselungsoperation in eine mit dem ausgewählten ersten Schlüssel verschlüsselte Nachricht (Code) um. Eine Sendeeinheit (13, 16) sendet die verschlüsselte Nachricht an das mobile Endgerät. Die Erfindung betrifft weiterhin ein System (100) mit mindestens zwei erfindungsgemäßen Beleuchtungseinrichtungen mit jeweils einem eigenen Satz von ersten Schlüsseln. Die Erfindung betrifft weiterhin ein entsprechendes Verfahren.

Beschreibung

Beleuchtungseinrichtung und Verfahren zur Bereitstellung einer Datenübertragung an ein mobiles Endgerät

5

Die Erfindung betrifft eine Beleuchtungseinrichtung zur Bereitstellung einer Datenübertragung an ein mobiles Endgerät gemäß dem Oberbegriff des Patentanspruchs 1. Weiterhin betrifft die Erfindung ein System mit mindestens zwei
10 derartigen Beleuchtungseinrichtungen. Überdies betrifft die Erfindung ein Verfahren zur Bereitstellung einer Datenübertragung an ein mobiles Endgerät gemäß dem Oberbegriff des Patentanspruchs 8.

15 Eine Beleuchtungseinrichtung, welche Daten an ein mobiles Endgerät überträgt, ist beispielsweise aus der WO 2015/148696 A1 bekannt. Diese offenbart Techniken für positionsbasierte Aktionen mithilfe von lichtbasierter Kommunikation. Überdies ist aus der EP 1 263 150 B1 ein
20 Daten-Übertragungssystem mit einer lokalen Bake bekannt, die auf der einen Seite mit steuernden und/oder Informationen übermittelnden Infrastruktur-Einrichtungen, beispielsweise einem zentralen Diensteserver oder dem Internet, und/oder mit einer oder mehreren weiteren lokalen Baken in
25 Kommunikationsverbindung steht und die auf der anderen Seite zur drahtlosen Kommunikationsverbindung mit einem oder mehreren, sich in ihrer Umgebung befindenden Endgeräten eine kombinierte Sende-/Empfangseinrichtung oder in besonderen Fällen nur eine reine Sendeeinrichtung enthält und die in, an
30 oder an der Stelle einer elektrischen Beleuchtungsvorrichtung angeordnet ist. Die lokale Bake ist mit einer die drahtlos zu übertragenden Daten betreffenden, in intelligenter Weise betriebenen Speicher- und/oder Verarbeitungsfunktionalität versehen, wobei die Speicherfunktionalität der lokalen Bake
35 darin besteht, Informationen vorzuhalten, so dass diese Informationen dann mehrfach an mit einem passenden Endgerät ausgerüstete Nutzer abgegeben werden können, ohne jedes Mal von den Infrastruktur-Einrichtungen eingeholt werden zu

müssen, und dass die Verarbeitungsfunktionalität darin besteht, dass bestimmte Verarbeitungsvorgänge, die sonst in einer zentralen Verarbeitungseinheit der Infrastruktur-Einrichtungen oder im Endgerät selber ausgeführt werden, auf
5 die lokale Bake ausgelagert werden.

Die aus dem Stand der Technik bekannten Wege zur Datenübertragung, insbesondere die Datenübertragung über ein von einer Leuchte ausgestrahltes Licht, ermöglichen Dritten
10 den Zugang zu den übertragenen Daten und macht diese für Dritte somit für die Erstellung eigener Dienstleistungen verwendbar.

Es ist daher Aufgabe der vorliegenden Erfindung, eine
15 Beleuchtungseinrichtung, ein System sowie ein Verfahren bereitzustellen, durch welche die Nutzbarkeit der übertragenen Daten für die Erstellung von fremden Diensten durch Drittanbieter eingeschränkt wird.

20 Diese Aufgabe wird gelöst durch eine Beleuchtungseinrichtung mit den Merkmalen des Patentanspruchs 1, ein System mit den Merkmalen des Patentanspruchs 5 sowie durch ein Verfahren mit den Merkmalen des Patentanspruchs 8. Vorteilhafte
Weiterbildungen der vorliegenden Erfindung sind Gegenstand
25 der abhängigen Ansprüche.

Die Erfindung geht aus von einer Beleuchtungseinrichtung zur Bereitstellung einer Datenübertragung an ein mobiles Endgerät, umfassend ein Leuchtmittel und ein elektronisches
30 Betriebsgerät zum Betreiben des Leuchtmittels. Erfindungsgemäß wird die Beleuchtungseinrichtung weitergebildet durch eine Datenspeichereinheit, in der in einem dafür reservierten Speicherbereich ein Satz von ersten Schlüsseln gespeichert ist, eine Auswahlereinheit, welche dazu
35 ausgelegt ist, in Abhängigkeit von einem an einer Datenschnittstelle der Beleuchtungseinrichtung bereitstellbaren Schlüsselwechselsignal und/oder in Abhängigkeit von einem durch einen Schlüsselwechseltaktgeber

der Beleuchtungseinrichtung bereitstellbaren
beleuchtungseinrichtungsinternen Schlüsselwechselsignal einen
ersten Schlüssel aus dem Satz von ersten Schlüsseln
auszuwählen, eine Verschlüsselungseinheit, welche dazu
5 ausgelegt ist, den ausgewählten ersten Schlüssel aus dem
reservierten Speicherbereich auszulesen und Messwertedaten
und/oder Identifikationsdaten, welche zur Übertragung an das
mobile Endgerät bestimmt sind, gemäß einer vorgebbaren
Verschlüsselungsoperation in eine mit dem ausgewählten ersten
10 Schlüssel verschlüsselte Nachricht umzusetzen, und eine
Sendeeinheit, welche dazu ausgelegt ist, die verschlüsselte
Nachricht an das mobile Endgerät zu senden.

Die Erfinder haben erkannt, dass statische
15 Identifikationsnummern, die von einer Beleuchtungseinrichtung
ausgesendet werden, auch von anderen ausgelesen und benutzt
werden können. Die Identifikationsnummer kann somit von einem
Dritten ausgelesen werden und in eigene Karten eingetragen
werden, sodass eine Verknüpfung zwischen
20 Identifikationsnummer und Position entsteht. Somit können
Dienstleistungsangebote von Dritten erstellt werden, ohne
dafür ein eigenes System aus Informations- und Sendequellen
aufzubauen, oder sich an den Kosten für die bestehende
Infrastruktur zu beteiligen. Somit ist dieser Service nicht
25 mehr exklusiv für den denjenigen verfügbar, der das System
und die Infrastruktur finanziert.

Der Erfindung liegt die weitere Erkenntnis zugrunde, dass
beispielsweise die Identifikationsnummer einer
30 Beleuchtungseinrichtung (Leuchte) stets eine statische
Identifikationsnummer ist. Dies gilt in gleicher Weise für
Sende-Baken (Beacons), welche Teil einer
Beleuchtungseinrichtung sein können und ebenfalls über eine
eindeutige Identifikationsnummer verfügen können. Wird eine
35 feste Identifikationsnummer mit einem festen Schlüssel
verschlüsselt, entsteht wieder eine feststehende Code-
Sequenz. Da die feste Code-Sequenz ebenfalls als Pseudo-
Identifikationsnummer benutzt werden kann, ohne die

eigentliche, dahinterliegende Identifikationsnummer zu kennen, lässt sich ein Pseudo-Identifikationsnummer-basiertes Positionsbestimmungssystem aufbauen. Dies gilt in gleicher Weise, wenn anstelle einer eindeutigen Identifikationsnummer

5 die Bauposition der Beleuchtungseinrichtung direkt als Ortsinformation gemäß einem vorgebbaren Koordinatensystem ausgesendet wird, was ebenfalls zu einem gleichbleibenden Dateninhalt führt. Daher ist gemäß der Erfindung vorgesehen, dass wechselnde Schlüssel verwendet werden. So verändert sich

10 das von der Beleuchtungseinrichtung ausgesendete Signal mit jedem neuen Schlüssel. Wird der Schlüssel zum Beispiel wöchentlich verändert, so lohnt es sich für einen unbefugten Dritten nicht, einen Dienst immer wieder aufs Neue auf die neuen Pseudo-Identifikationsnummern umzustellen. Zu diesem

15 Zweck werden deshalb eine Reihe von Schlüsseln, nämlich ein Satz von ersten Schlüsseln, in der Beleuchtungseinrichtung vorgehalten, aus welchen dann eine Auswahl vorgenommen werden kann.

20 Die Beleuchtungseinrichtung kann neben einer lichttechnisch wirksamen Komponente in Form einer Leuchte weitere Komponenten umfassen, welche außerhalb der eigentlichen Leuchte angeordnet sind. Das Leuchtmittel kann durch ein LED-Leuchtmittel oder durch eine Niederdruckentladungslampe

25 (Leuchtstofflampe) gebildet sein. Das elektronische Betriebsgerät kann eine programmgesteuerte Recheneinheit umfassen, beispielsweise in Form eines Mikroprozessors oder eines Mikrocontrollers. Bevorzugt kann die Datenspeichereinheit in einem Datenspeicher eines solchen

30 Mikrocontrollers/Mikroprozessors realisiert sein. Besonders bevorzugt ist die Auswahlereinheit und/oder die Verschlüsselungseinheit als ausführbarer Programmcode in einem Programmspeicher eines solchen Mikrocontrollers/Mikroprozessors gespeichert, insbesondere in

35 demselben. Die Sendeeinheit kann das Leuchtmittel umfassen, wenn es sich bei der Datenübertragung um eine lichtbasierte Datenübertragung handelt. Alternativ oder zusätzlich kann

vorgesehen sein, dass die Sendeeinheit durch eine Funk-Bake gegeben ist.

Gemäß einer vorteilhaften Weiterbildung ist die

5 Auswahleinheit dazu ausgelegt, den ausgewählten ersten Schlüssel in Abhängigkeit von dem Schlüsselwechselsignal gemäß einem vorgebbaren Schema aus dem Satz von ersten Schlüsseln zu ermitteln. Beispielsweise können die ersten Schlüssel in einer Tabelle angeordnet sein, wobei die
10 Ermittlung des ausgewählten ersten Schlüssels durch Ermittlung einer Tabellenposition anhand einer Rechenvorschrift ermittelt wird, und der ausgewählte erste Schlüssel somit derjenige Schlüssel ist, welcher in dieser Tabelle an der jeweiligen Tabellenposition angeordnet ist.

15 Alternativ kann vorgesehen sein, die Tabellenposition des ausgewählten ersten Schlüssels aus einer Folge von gespeicherten Zeigern zu ermitteln, welche jeweils auf eine Tabellenposition der Tabelle zeigen. Bevorzugt ist die Folge
20 von gespeicherten Zeigern in einem Datenspeicher eines Mikrocontrollers/Mikroprozessors gespeichert, besonders bevorzugt in demselben Datenspeicher.

Eine derartige Ausgestaltung ermöglicht eine Vielzahl von
25 unterschiedlichen Codierungen der jeweiligen Identifikationsnummern, und gleichzeitig eine einfache Möglichkeit, die Schlüssel auf der Sende- und Empfangsseite synchron zu halten. Ein Empfangsgerät, welches Kenntnis von dem vorgebbaren Schema und dem Satz von ersten Schlüsseln
30 hat, kann somit auf sehr einfache Weise mit der Beleuchtungseinrichtung synchronisiert werden. Beispielsweise kann vorgesehen sein, dass die Beleuchtungseinrichtung selbst zusammen mit dem verschlüsselten Signal einen codierten Hinweis sendet, welcher Schlüssel aktuell verwendet wird.
35 Hierzu kann beispielsweise eine Signalisierungsfolge mit einzelnen Signalisierungsbits vorgesehen sein, welche eine vorab definierbare Bedeutung zur Schlüsselfindung aufweisen, insbesondere einen direkten Adressierungswert, welcher auf

die Tabellenposition zeigt, oder einen indirekten Adressierungswert, welcher auf eine Folge von gespeicherten Zeigern weist.

5 Weitere Signalisierungsbits können beispielsweise anzeigen, ob der jeweils ausgewählte Schlüssel direkt in der ausgelesenen Form verwendet werden soll, oder ob zuvor bestimmte mathematische Operationen mit diesem Schlüssel durchzuführen sind, beispielsweise ein Verschieben des
10 Schlüssel in einem Schieberegister, genauer ein Rotieren, bei welchem die einzelnen Bits des Schlüssels zyklisch verschoben werden können. Hierbei können sowohl eine Richtung als auch eine Länge der Verschiebung, d.h. um wie viele Bits der Schlüssel zu verschieben ist, festgelegt sein.

15 Gemäß einer weiteren vorteilhaften Ausführungsform ist die Auswahlseinheit dazu ausgelegt, die Auswahl des ersten Schlüssels zumindest anteilig in Abhängigkeit von einer Zufallsvariablen zu treffen, welche mittels eines
20 Zufallsgenerators bereitstellbar ist. Hierdurch kann vermieden werden, dass bei einer ausreichend langen Aufzeichnungsdauer eines ausgewerteten Signals eine zugrunde liegende Gesetzmäßigkeit erkannt und analysiert wird und basierend auf dieser Gesetzmäßigkeit eine Vorhersage
25 getroffen werden kann, zu welchem Zeitpunkt welcher Schlüssel aktiv ist bzw. welche verschlüsselte Wert zu welchem Zeitpunkt vorliegen wird.

Gemäß einer weiteren vorteilhaften Ausführungsform ist die
30 Verschlüsselungseinheit dazu ausgelegt, den ausgewählten ersten Schlüssel vor der Verwendung mit der Verschlüsselungsoperation um eine vorgebbare Anzahl von Bitpositionen in einem Schieberegister zu verschieben und dabei in Schieberichtung aus dem Schieberegister
35 herausgeschobene Bits auf der gegenüberliegenden Seite wieder einzuschieben. Mittels einer derartigen Rotation von Schlüsseln kann eine Erhöhung der Anzahl der Schlüssel realisiert werden. Die Länge des ersten Schlüssels und die

Anzahl und Art der Schlüssel-Verschiebungen bestimmt hierbei den zusätzlichen Verschlüsselungsraum. Wenn beispielsweise die Länge einer Identifikationsnummer zehn Bit beträgt und die Länge des ersten Schlüssels ebenfalls zehn Bit, so
5 wiederholt sich der erste Schlüssel nach zehn Schritten im Schieberegister wieder. In dem genannten Beispiel bedeutet dies, dass jeder erste Schlüssel aus dem Satz von ersten Schlüsseln zehnmal benutzt werden kann, ehe er sich wiederholt.

10

Bevorzugt weist ein System mindestens eine erste erfindungsgemäße Beleuchtungseinrichtung und mindestens eine zweite erfindungsgemäße Beleuchtungseinrichtung auf, wobei die mindestens eine erste und die mindestens eine zweite
15 Beleuchtungseinrichtung jeweils einen eigenen Satz von ersten Schlüsseln aufweist, wodurch sich ein erfindungsgemäßes System ergibt. Besonders bevorzugt kann vorgesehen sein, dass der Satz von ersten Schlüsseln der mindestens einen ersten Beleuchtungseinrichtung und der Satz von ersten Schlüsseln
20 der mindestens einen zweiten Beleuchtungseinrichtung durch zwei vollständig verschiedene Schlüsselsätze gebildet sind. Der Aufwand, der notwendig ist, ein derartiges erfindungsgemäßes System zu entschlüsseln, ohne die Kenntnis der Schlüssel zu besitzen, kann somit erhöht werden, wenn die
25 Gültigkeit von Schlüsseln in eine lokale Abhängigkeit gesetzt wird. Beispielsweise kann vorgesehen sein, dass ein bestimmter Satz von ersten Schlüsseln nur für Beleuchtungseinrichtungen innerhalb eines bestimmten Raums gültig ist.

30

Gemäß einer vorteilhaften Weiterbildung umfasst das System eine Bake zur Bereitstellung von Positionsbestimmungsdaten mittels eines Funksignals, wobei die Positionsbestimmungsdaten in dem System einem Bereich
35 zugeordnet sind, der eine Montageposition der ersten Beleuchtungseinrichtung umfasst. Insbesondere umfasst der Bereich nicht eine Montageposition der zweiten Beleuchtungseinrichtung. Auf diese Weise ergibt sich der

Vorteil, dass eine Gültigkeitszuordnung der lokal vergebenen ersten Schlüsselsätze möglich ist, indem über die Bake (Beacon) eine grobe Lokalisierung erfolgen kann, aus der dann weiter ermittelbar ist, welcher Schlüsselsatz in diesem Bereich gültig ist.

Gemäß einer weiteren vorteilhaften Ausführungsform umfasst das System eine zentrale Schlüsselverwaltungseinheit, welche dazu ausgelegt ist, ein Schlüsselwechselsignal an die mindestens eine erste und die mindestens eine zweite Beleuchtungseinrichtung zu senden, wobei das Schlüsselwechselsignal zumindest anteilig Schlüsselgenerierungsmaterial umfasst, und wobei die jeweilige Verschlüsselungseinheit dazu ausgelegt ist, in Abhängigkeit von dem jeweils ausgewählten ersten Schlüssel und von dem übertragenen Schlüsselgenerierungsmaterial gemäß einer vorgebbaren Berechnungsvorschrift einen jeweils neuen zweiten Schlüssel zu ermitteln, wobei die jeweilige Datenspeichereinheit dazu ausgelegt ist, den jeweiligen zweiten Schlüssel als zusätzlichen ersten Schlüssel in dem jeweiligen Satz von ersten Schlüsseln zu ergänzen. Somit können unter Verwendung von einem für alle Beleuchtungseinrichtungen innerhalb des Systems verwendbaren Schlüsselgenerierungsmaterial individuelle lokale Schlüssel erzeugt werden, welche aufgrund der Einbindung eines der ersten Schlüssel, welche innerhalb des jeweiligen Satzes von ersten Schlüsseln gespeichert sind, eine unabhängige Schlüsseldiversifizierung erhalten. Damit kann auch unter Verwendung von Schlüsselgenerierungsmaterial mit im Vergleich zu dem Satz von ersten Schlüsseln geringen Datenumfang eine Vielfalt von ersten Schlüsselsätzen erhalten und ausgebaut werden.

Bevorzugt kann vorgesehen sein, dass ein derart erzeugter zusätzlicher erster Schlüssel in einer Datentabelle, welche den Satz von ersten Schlüsseln umfasst, an einem noch freien, für derartige Ergänzungen reservierten Speicherplatz eingefügt wird, um damit jeweils neue, noch nicht verwendete

Schlüssel zu generieren. Besonders bevorzugt kann vorgesehen sein, einen vorgebbaren Bereich vorzuhalten, in dem zusätzliche erste Schlüssel, die in Abhängigkeit von Schlüsselgenerierungsmaterial erzeugt wurden, abgespeichert werden. Dabei kann vorgesehen sein, dass dieser Bereich zyklisch überschrieben wird, wenn ein Schlüsselwechselsignal an die Beleuchtungseinrichtungen gesendet wird. Bevorzugt kann der vorgebbare Bereich zur Ergänzung mit zusätzlichen ersten Schlüsseln dieselbe Größe aufweisen wie der Satz von ersten Schlüsseln, sodass für jeden der ersten Schlüssel aus dem Satz von ersten Schlüsseln durch die Anwendung der vorgebbaren Berechnungsvorschrift zusammen mit dem Schlüsselgenerierungsmaterial jeweils ein zusätzlicher neuer Schlüssel in den erweiterten Bereich eingetragen wird.

Die Erfindung geht weiterhin aus von einem Verfahren zur Bereitstellung einer Datenübertragung an ein mobiles Endgerät mittels einer Beleuchtungseinrichtung. Erfindungsgemäß wird das Verfahren weitergebildet durch Speichern eines Satzes von ersten Schlüsseln in einem dafür reservierten Speicherbereich einer Datenspeichereinheit der Beleuchtungseinrichtung, Auswählen eines ersten Schlüssels aus dem Satz von ersten Schlüsseln in Abhängigkeit von einem an einer Datenschnittstelle der Beleuchtungseinrichtung bereitstellbaren Schlüsselwechselsignal und/oder in Abhängigkeit von einem durch einen Schlüsselwechseltaktgeber der Beleuchtungseinrichtung bereitstellbaren beleuchtungseinrichtungsinternen Schlüsselwechselsignal. Das Verfahren umfasst weiterhin Auslesen des ausgewählten ersten Schlüssels aus dem reservierten Speicherbereich, Umsetzen von Messwertedaten und/oder Identifikationsdaten, welche zur Übertragung an das mobile Endgerät bestimmt sind, gemäß einer vorgebbaren Verschlüsselungsoperation in eine mit dem ausgewählten ersten Schlüssel verschlüsselte Nachricht, und Senden der verschlüsselten Nachricht an das mobile Endgerät durch eine Sendeeinheit der Beleuchtungseinrichtung.

Insbesondere in Fällen, in denen das Schlüsselmanagement über eine Datenschnittstelle der Beleuchtungseinrichtung mit einer in der Regel begrenzte Datenübertragungskapazität erfolgt, beispielsweise über eine Steuerungsschnittstelle mit

5 Anschluss an ein übergeordnetes Beleuchtungssteuerungssystem (Lichtmanagementsystem/Gebäudemanagementsystem), kann auf diese Weise mittels Bereitstellung von Schlüsselwechselsignalen mit im Vergleich zu den Schlüsseln geringem Datenumfang eine Verschlüsselung der Messwertedaten und/oder Identifikationsdaten auf vielfältige Weise erfolgen,
10 sodass eine Rekonstruktion praktisch unmöglich ist. Die Erfindung dient somit nicht nur dazu, einen Dateninhalt zu verschlüsseln, sondern gleichzeitig auch dazu, die Identität des zugrunde liegenden Datenpakets, beispielsweise der
15 Identifikationsdaten, zu verbergen.

Gemäß einer vorteilhaften Weiterbildung umfasst das Verfahren Senden eines Schlüsselwechselsignals an die Beleuchtungseinrichtung, wobei das Schlüsselwechselsignal
20 zumindest anteilig Schlüsselgenerierungsmaterial umfasst, Ermitteln eines zweiten Schlüssels in Abhängigkeit von dem ausgewählten ersten Schlüssel und von dem übertragenen Schlüsselgenerierungsmaterial gemäß einer vorgebbaren Berechnungsvorschrift, und Ergänzen des zweiten Schlüssels
25 als zusätzlichen ersten Schlüssel in dem Satz von ersten Schlüsseln. Dadurch können weitere, von den innerhalb der Beleuchtungseinrichtung vorhandenen ersten Schlüsseln aufgrund des zusätzlich eingebrachten Schlüsselgenerierungsmaterial nicht ableitbare weitere
30 Schlüssel erzeugt werden, deren Bildungsvorschriften von einem Dritten, welcher die verschlüsselten Nachrichten analysiert, nicht mehr rekonstruiert werden können.

Insbesondere dadurch, dass die beispielsweise über eine
35 Steuerungsschnittstelle bereitgestellten Schlüsselgenerierungsmaterialien für einen unbefugten Dritten nicht zugänglich sind, wird durch dieses Verfahren ein hoher Schutz erreicht. Ein für den Empfang der Datenübertragung von

der Beleuchtungseinrichtung bzw. dem System autorisierter Benutzer kann beispielsweise von der zentralen Schlüsselverwaltungseinheit, beispielsweise einem Schlüsselservers im Netzwerk, welches über einen WLAN-Zugang oder einen Mobilfunkzugang abfragbar ist, das zu dem aktuellen Zeitpunkt verwendete Schlüsselgenerierungsmaterial zugesendet bekommen, um damit basierend auf dem ursprünglichen Satz von ersten Schlüsseln den jeweils geltenden zweiten Schlüssel zu berechnen.

Gemäß einer weiteren vorteilhaften Ausführungsform umfasst das Verfahren Erzeugen eines zweiten Schlüssels zur Verwendung mit der Verschlüsselungsoperation durch Kombination von zumindest zwei ersten Schlüsseln aus dem Satz von ersten Schlüsseln gemäß einer vorgebbaren Kombinationsrechenvorschrift. Hierdurch können weitere Schlüssel aus den ursprünglich vorhandenen ersten Schlüsseln sowie aus den weiteren, durch Kombination mit einem Schlüsselgenerierungsmaterial gewonnenen Schlüsseln erzeugt werden. Die Verfahrensschritte können hierbei beliebig miteinander kombiniert werden.

Eine derartige Kombinationsrechenvorschrift kann beispielsweise derart gebildet werden, dass eine bitweise Exklusiv-Oder-Verknüpfung der beiden Operanden ausgeführt wird. Weitere Kombinationsmöglichkeiten und/oder Kaskadierungen von Verfahrensschritten sind ebenfalls möglich und ermöglichen eine nahezu unerschöpfliche Vielfalt von verwendbaren ersten Schlüsseln, sodass selbst bei einem täglichen Wechsel des Schlüssels in dem System insbesondere die Wiederholung einer ganzen Schlüsselsequenz auszuschließen ist.

Die für die erfindungsgemäße Beleuchtungseinrichtung beschriebenen Vorteile und bevorzugten Ausführungsformen gelten auch für das erfindungsgemäße System. Ebenso gelten die für die erfindungsgemäßen Vorrichtungen beschriebenen Vorteile und Merkmale sowie Ausführungsformen gleichermaßen

für entsprechende Verfahren und umgekehrt. Folglich können für Vorrichtungsmerkmale entsprechende Verfahrensmerkmale und umgekehrt vorgesehen sein.

5 Die vorstehend in der Beschreibung genannten Merkmale und Merkmalskombinationen sowie die nachfolgend in der Figurenbeschreibung genannten und/oder in den Figuren alleine gezeigten Merkmale und Merkmalskombinationen sind nicht nur in der jeweils angegebenen Kombination, sondern auch in
10 anderen Kombinationen oder in Alleinstellung verwendbar, ohne den Rahmen der Erfindung zu verlassen. Es sind somit auch Ausführungen als von der Erfindung offenbart anzusehen, die in den Figuren nicht explizit gezeigt oder erläutert sind, jedoch durch separierte Merkmalskombinationen aus den
15 erläuterten Ausführungen hervorgehen und erzeugbar sind.

Weitere Vorteile und Merkmale ergeben sich anhand der folgenden Beschreibung von Ausführungsbeispielen unter Berücksichtigung der beigefügten Figuren. In den Figuren
20 bezeichnen gleiche Bezugszeichen gleiche Merkmale und Funktionen.

Es zeigen:

25 Fig. 1 in vereinfachter schematischer Darstellung ein Beleuchtungssystem mit einer lokalen clientbasierten Entschlüsselung,

30 Fig. 2 in vereinfachter schematischer Darstellung ein Beleuchtungssystem mit einem asymmetrischen Kryptosystem,

35 Fig. 3 in vereinfachter schematischer Darstellung ein Beleuchtungssystem mit einer serverbasierten Entschlüsselung,

Fig. 4 in vereinfachter schematischer Darstellung das Aufbringen und den Transport der Schlüssel für die Verwendung in einem Beleuchtungssystem,

5 Fig. 5 in vereinfachter schematischer Darstellung eine beispielhafte Schlüsselverteilung über ein unter Nutzung einer Beacon-Funktionalität aufgebautes drahtloses Netzwerk zur Schlüsselverteilung für die Verwendung in einem Beleuchtungssystem,

10

Fig. 6 in schematischer Darstellung ein vereinfachtes Beispiel für eine symmetrische Verschlüsselung einer Leuchten-Identifikationsnummer und deren Entschlüsselung,

15

Fig. 7 in vereinfachter schematischer Darstellung eine beispielhafte Zusammensetzung einer verschlüsselten Nachricht,

20 Fig. 8 in vereinfachter schematischer Darstellung die Auswahl eines Schlüssels aus einem Satz von Schlüsseln gemäß einer bevorzugten Ausführungsform der Erfindung,

25 Fig. 9 in vereinfachter schematischer Darstellung eine beispielhafte Bedeutungszuweisung der Signalisierungsbits für Rotation und Rotationsrichtung eines Schlüssels zur Verwendung mit der Erfindung,

30

Fig. 10 in vereinfachter schematischer Darstellung die Erzeugung neuer Schlüssel durch bitweise Rotation eines vorhandenen Schlüssels zur Verwendung mit der Erfindung, und

35

Fig. 11 in vereinfachter schematischer Darstellung die Erzeugung eines neuen Schlüssels aus zwei

vorhandenen Schlüsseln zum Einsatz mit der Erfindung.

Ein Beleuchtungssystem 100 umfasst zumindest eine Leuchte 12
5 beispielsweise in Form einer Deckenleuchte. Die Leuchte 12 umfasst ein Leuchtmittel 13. Weiterhin umfasst das Beleuchtungssystem 100 ein mobiles Endgerät 14.

Das Beleuchtungssystem 100 kann des Weiteren unabhängig
10 voneinander und in beliebiger Kombination mindestens eine der nachfolgenden Komponenten aufweisen: eine Bake 16, einen WLAN-Router 18 sowie eine Servereinheit 20. Eine Bake 16, welche in einer direkten Datenverbindung mit der Leuchte 12 steht, wird ebenso wie das Leuchtmittel 13 und ein
15 zugehöriges Betriebsgerät (Treiber) als Teil der jeweiligen Beleuchtungseinrichtung betrachtet.

Das Leuchtmittel 13 kann zur lichtbasierten Kommunikation ausgelegt sein. Diese ist beispielsweise für die Navigation
20 im Innenraum von Gebäuden, sogenannte Indoor-Navigation, geeignet. Lichtbasierte Indoor-Navigation beruht auf der Aussendung einer Licht-ID (LID), die mithilfe des mobilen Endgeräts 14 empfangen und detektiert werden kann. Die Licht-ID wird hierzu in den Lichtstrom - unsichtbar für das
25 menschliche Auge - aufmoduliert. Um das Signal mit dem mobilen Endgerät 14 zu detektieren, muss eine Sichtverbindung (line-of-sight) zwischen dem Detektor, beispielsweise einer Kamera des mobilen Endgeräts 14, und dem Leuchtmittel 13 bestehen, welches die modulierte Lichtquelle darstellt. Die
30 Licht-ID wird von dem mobilen Endgerät 14 wieder aus dem Licht herausgefiltert und demoduliert.

Der Erfindung liegt die weitere Erkenntnis zugrunde, dass Sendeeinheiten, welche zur lokalen Abstrahlung von Signalen,
35 welche ortsspezifische Messwertedaten und/oder Identifikationsdaten beinhalten, vielfach keinen Rückkanal aufweisen, wie es bei der lichtbasierten Kommunikation über das Leuchtmittel 13 der Fall ist, wodurch Verschlüsselungen,

die auf bidirektionaler Kommunikation beruhen, nicht einsetzbar sind.

Die Licht-ID selbst kann direkt eine Positionsinformation der
5 Lichtquelle beinhalten oder aber indirekt über eine Look-up-
Tabelle ermittelt werden. Hierzu findet in der Look-up-
Tabelle eine Zuordnung von Licht-ID und
Positionsinformationen der Lichtquelle statt. Um die
Positionsgenauigkeit weiter zu erhöhen, kann eine optische
10 Auswertung über einen Bildsensor (Kamera) durchgeführt
werden. Hierzu werden die unterschiedlichen Winkel ermittelt,
unter welchen der Bildsensor die verschiedenen Licht-IDs
empfängt. Aus drei verschiedenen Licht-IDs lässt sich somit
im Raum über Triangulation eine eindeutige Position
15 ermitteln. Die eigene Lage des Empfängers, beispielsweise der
Kamera, in dem mobilen Endgerät 14 wird in dem Empfänger
mittels Sensoren (3D-Beschleunigungssensoren) ermittelt, um
die eigene Lage zu detektieren und einen daraus
resultierenden lageabhängigen Fehler in der
20 Positionsermittlung zu kompensieren.

Neben der Positionsinformation können beliebige weitere Meta-
Daten, beispielsweise ortsspezifische Messwertedaten, welche
von der Leuchte 12 bereitgestellt werden, mit der Licht-ID
25 verknüpft werden. Die Look-up-Tabelle kann als integrierter
Teil in einer Anwendung hinterlegt sein, welche auf dem
mobilen Endgerät 14 abläuft, oder aber auf der externen
Serverreinheit 20 hinterlegt sein, auf welche das mobile
Endgerät 14 zugreift.

30 Umgekehrt kann die Look-up-Tabelle auch dynamische
Informationen aufnehmen, beispielsweise welches mobile
Endgerät 14 welche Positionsinformationen abgefragt hat.
Somit lässt sich ein dynamisches Bewegungsprofil aufzeichnen
35 (tracking) und mit einem Zeitstempel abspeichern (tracing).
Diese Bewegungsinformationen bilden die Grundlage für
verschiedenste ortsbezogene Dienste und Analysen.

Es gibt verschiedene drahtlose funkbasierte Systeme wie WLAN oder Bluetooth, die für eine Indoor-Positionsbestimmung verwendet werden können. Hierbei ist zum einen die Position des Senders (WLAN Access Point) in der Fig. 1 als optionaler WLAN-Router 18 dargestellt oder einer Bake 16 - bei Bluetooth-basierten Funksystemen auch als Beacon bezeichnet - bekannt und anhand der Signalfeldstärke des empfangenen Signals (received signal strength, RSSI) kann der Abstand zwischen Sender und mobilem Empfänger abgeschätzt werden. Für eine eindeutige Positionsbestimmung werden mindestens drei verschiedene Sendequellen benötigt (Trilateration).

Erschwerend tritt hinzu, dass die Licht-ID , welche also beispielsweise eine Identifikationsnummer einer Leuchte sein kann, stets einen statischen Wert annimmt. Das gleiche gilt für (Sende-)Baken 16 (Beacons), was der Einfachheit halber nachfolgend am Beispiel einer Leuchten-ID (im Folgenden synonym mit Licht-ID verwendet) und der zugehörigen Verschlüsselung beschrieben wird. Wird eine feste Leuchten-ID mit einem festen Verschlüsselungsschlüssel EKey verschlüsselt, entsteht wieder eine feststehende Code-Sequenz, nämlich die verschlüsselte Nachricht Code. Diese feste Code-Sequenz kann ebenfalls als Pseudo-ID genutzt werden. Ohne die eigentliche dahinterliegende Leuchten-ID zu kennen, lässt sich ein Pseudo-ID-basiertes Positionsbestimmungssystem aufbauen.

Gemäß der Erfindung wird nun in dem Beleuchtungssystem 100 die Licht-ID nicht statisch offen übertragen, sondern verschlüsselt. Eine besondere Herausforderung besteht darin, dass Licht zur Standard-Beleuchtung keinen direkten Rückkanal besitzt. Insofern lassen sich klassische Verfahren nicht einsetzen, die auf dem Prinzip der bidirektionalen Kommunikation beruhen. In der Fig. 1 sind verschiedene Wege dargestellt, wie ein Entschlüsselungsschlüssel DKey zur Entschlüsselung einer verschlüsselten Nachricht Code, welcher über das Leuchtmittel 13 auf dem Wege einer lichtbasierten Kommunikation bereitgestellt wird, bezogen werden kann.

Zur Verhinderung einer unberechtigten Mitbenutzung können wechselnde Verschlüsselungsschlüssel EKey verwendet werden. So verändert sich das die verschlüsselte Nachricht Code transportierende Signal mit jedem neuen Verschlüsselungsschlüssel EKey. Wird der Verschlüsselungsschlüssel EKey beispielsweise wöchentlich verändert, so lohnt es sich für einen unberechtigten Mitbenutzer nicht, seine parasitäre Applikation immer wieder neu auf die neuen Pseudo-IDs umzustellen. Zu diesem Zweck kann vorgesehen sein, eine Reihe von Verschlüsselungsschlüsseln EKey[1..m] in dem Beleuchtungssystem 100 vorzuhalten, die dann nach einem vorgegebenen Muster verwendet werden. Der jeweils aktive Verschlüsselungsschlüssel EKey[n] und das Muster sind dann auf Sende- und Empfangsseite synchron zu halten.

Bei Anwendung von symmetrischen Kryptographieverfahren sind der erste Schlüssel, das heißt der Verschlüsselungsschlüssel EKey, und der zweite Schlüssel, das heißt der Entschlüsselungsschlüssel DKey, identisch.

Nachfolgend wird eine Abhängigkeit des Verschlüsselungsschlüssels EKey vom Ort durch Ekey[loc] gekennzeichnet, eine Abhängigkeit des Verschlüsselungsschlüssels EKey von der Zeit durch Ekey[temp], und eine Abhängigkeit von sowohl von der Zeit als auch vom Ort EKey[temp,loc]. So kennzeichnet beispielsweise EKey[n,loc] einen jeweils aktuell aktivierten und für die Verschlüsselungsoperation verwendeten Verschlüsselungsschlüssel der jeweiligen lokalen Beleuchtungseinrichtungen, welche gemeinsam denselben Schlüssel benutzen, also im Extremfall jeweils einer einzigen Beleuchtungseinrichtung, wenn alle Beleuchtungseinrichtungen innerhalb des Beleuchtungssystems eigene Schlüssel verwenden. In letzterem Fall repräsentiert loc einen Laufindex von 1 bis Anzahl der einzelnen Beleuchtungseinrichtungen in dem Beleuchtungssystem.

Ein Verschlüsselungsschlüssel EKey[n-1,loc] kennzeichnet einen Schlüssel, der vor dem Verschlüsselungsschlüssel EKey[n,loc] aktiv war und durch letzteren ersetzt wurde. In gleicher Weise beschreibt EKey[n+1,loc] einen Verschlüsselungsschlüssel, der noch nicht aktiviert ist, aber dazu bestimmt ist, an die Stelle des aktuellen Verschlüsselungsschlüssels EKey[n,loc] zu treten.

10 Dasselbe gilt entsprechend für Entschlüsselungsschlüssel DKey, welche - sofern nicht ohnehin identisch bei Verwendung einer symmetrischen Verschlüsselung - zu dem jeweiligen Verschlüsselungsschlüssel EKey passend zuzuordnen sind.

15 Für eine clientseitige Entschlüsselung, also eine Entschlüsselung auf dem mobilen Endgerät 14, benötigt das mobile Endgerät 14 den Entschlüsselungsschlüssel DKey, um die verschlüsselte Nachricht Code zu entschlüsseln. Der Entschlüsselungsschlüssel DKey kann hierzu bereits ein Teil
20 der Anwendung sein, die auf dem mobilen Endgerät beispielsweise als Smartphone-App ausgeführt wird.

Alternativ kann der Entschlüsselungsschlüssel DKey dem mobilen Endgerät 14 beziehungsweise der darauf ablaufenden
25 Anwendung während des Betriebs bereitgestellt werden. Die Bereitstellung des Entschlüsselungsschlüssels DKey kann i.) über eine externe Servereinheit 20 erfolgen, wobei wahlweise ein lokal gültiger Entschlüsselungsschlüssel DKey[loc], der für jede Leuchte 12 individuell zugewiesen wird, oder ein
30 globaler Entschlüsselungsschlüssel DKey, der für alle Leuchten 12 innerhalb des Beleuchtungssystems 100 gleich, aber gegebenenfalls nur zeitlich begrenzt gültig ist, erfolgen. Gemäß ii.) kann der Entschlüsselungsschlüssel DKey über die Leuchte 12 selbst zur Verfügung gestellt werden.
35 Zusätzlich oder alternativ kann gemäß iii.) über eine lokale Informationsquelle der Entschlüsselungsschlüssel DKey zur Verfügung gestellt werden, beispielsweise über die Bake 16 oder über den WLAN-Router 18.

Bevorzugt kann vorgesehen sein, dass ein jeweils lokal zur Verfügung gestellter Schlüssel auch nur lokale Gültigkeit hat. Die Bereitstellung des Entschlüsselungsschlüssels DKey erfolgt nur nach vorangegangener Authentifizierung des mobilen Endgeräts 14 und zeitlich begrenzt. Der Entschlüsselungsschlüssel DKey wird über sichere Verbindungen, beispielsweise Bluetooth oder WLAN, übertragen.

Die Verschlüsselung kann auch gemäß der Darstellung in Fig. 2 individuell pro mobilem Endgerät 14 erfolgen. Hierzu erzeugt das mobile Endgerät 14 ein Schlüsselpaar bestehend aus einem öffentlichen Schlüssel PuKey und einen privaten Schlüssel PrKey, wobei in einem ersten Schritt der öffentliche Schlüssel PuKey an die Leuchte 12 übertragen wird. Der öffentliche Schlüssel PuKey kann beispielsweise über die Bake 16, den WLAN-Router 18 oder die Servereinheit 20 an die Leuchte 12 übertragen werden. Von der Leuchte 12 werden die Identifikationsdaten ID verschlüsselt und mittels des Leuchtmittels 13 gesendet, sodass nur das mobile Endgerät 14, welches den zugehörigen privaten Schlüssel PrKey besitzt, diese Identifikationsdaten ID wieder entschlüsseln kann.

Eine Datenverbindung zwischen der Servereinheit 20 und der Leuchte 12 ist gemäß der Darstellung in der Fig. 2 über ein Lichtmanagementsystem beziehungsweise Gebäudemanagementsystem 21 gegeben.

Eine serverseitige Entschlüsselung und Rückübertragung zu dem mobilen Endgerät 14 ist in der Fig. 3 dargestellt. Die verschlüsselte Nachricht Code wird zu der Servereinheit 20 übertragen und dort entschlüsselt. Von dort werden die aus der verschlüsselten Nachricht Code gewonnen Identifikationsdaten ID zurück zu dem mobilen Endgerät 14 übertragen. Dies hat den Vorteil, dass die Verschlüsselung beliebig verändert werden kann und der Entschlüsselungsschlüssel DKey nicht auf viele lokale Endgeräte 14 oder andere vergleichbare Clients übertragen

werden muss, was somit ein sichereres System darstellt. Die Identifikationsdaten ID können vor Ort für die Freischaltung von weiteren Dienstleistungen wie beispielsweise einer Lichtsteuerung verwendet werden.

5

Um die Sicherheit weiter zu erhöhen, kann eine „lokale Authentifizierung“ stattfinden. Hier kann durch weitere lokale Signale und Informationsquellen sichergestellt werden, dass die Anfragen an die Servereinheit 20 mit den lokalen Identifikationsdaten ID tatsächlich vor Ort erfolgt und kein Auslesen der Daten von Dritten beispielsweise durch automatisierte Abfragen erfolgt. Eine lokale Authentifizierung LocAuth kann beispielsweise dadurch erfolgen, dass über die Bake 16 oder den WLAN-Router 18 eine Ortsverifikation VerLoc bei der Servereinheit 20 vorgenommen wird.

Bei einer serverseitigen Entschlüsselung der verschlüsselten Nachricht Code können auch direkt Positionsinformationen Pos zu dem mobilen Endgerät 14 zurückgesendet werden. Die verschlüsselte Nachricht Code wird hierzu auf die Servereinheit 20 übertragen und dort mittels des Entschlüsselungsschlüssels DKey entschlüsselt. Weiterhin erfolgt dort auch die Umsetzung der Identifikationsdaten ID in die Positionsinformation Pos, wobei die Positionsinformationen Pos auch für beliebig andere Daten, welche eindeutig den Identifikationsdaten ID zugeordnet werden können, repräsentieren. Somit können die Positionsdaten Pos stellvertretend für beliebig weitere der Leuchte 12 zuordenbare Daten betrachtet werden. Die Positionsdaten Pos (oder weitere der Leuchte 12 zuordenbare Daten) werden dann zurück an das mobile Endgerät 14 übertragen. Vorteil dieser Ausführung ist, dass auf der Seite des mobilen Endgeräts 14 kein Zusammenhang zwischen der verschlüsselten Nachricht Code und den unverschlüsselten Identifikationsdaten ID hergestellt werden kann, da nur die verschlüsselte Nachricht Code dem mobilen Endgerät 14 bekannt ist.

Die Übertragung eines Verschlüsselungsschlüssels EKey in eine Leuchte 12 ist in der Fig. 4 dargestellt. Die Übertragung des Verschlüsselungsschlüssels EKey kann beispielsweise in der
5 Produktion der jeweiligen Leuchte 12, also statisch, erfolgen. Die Abspeicherung eines oder mehrerer lokaler Verschlüsselungsschlüssel EKey in einer Leuchte 12 beziehungsweise in einem Treiber 11 (Betriebsgerät) einer Leuchte 12 kann bereits während der Produktion erfolgen.
10 Insbesondere kann die Übertragung des lokalen Verschlüsselungsschlüssels EKey gemeinsam mit dem Programmieren einer Leuchten-ID in Form der Identifikationsdaten ID erfolgen. Anhand der Identifikationsdaten ID kann bei der Inbetriebnahme und
15 Lokalisierung einer Leuchte 12 an einer bestimmten Position auch die Schlüsselzuordnung erfolgen.

Während des Betriebs einer Leuchte 12 in einem Beleuchtungssystem 100 kann die Übertragung eines
20 Verschlüsselungsschlüssels EKey auch dynamisch erfolgen. Während des Betriebs lassen sich neue Verschlüsselungsschlüssel EKey in den Treiber 11 der Leuchte 12 einspielen. Dabei kann die Einspielung manuell über eine drahtgebundene oder drahtlose Schnittstelle stattfinden.

25 Hierzu eignet sich auch in besonderer Weise ein bereits bestehendes Netzwerk zur Lichtsteuerung, da hierfür in der Regel nur geringe Daten notwendig sind und es sich um ein nicht öffentlich zugängliches Netzwerk handelt. Dieses
30 Netzwerk zur Lichtsteuerung ist über ein Gebäudebeziehungsweise Lichtmanagementsystem 21 bei entsprechender Autorisierung zugänglich. Beispielsweise kann die Servereinheit 20 als Schlüsselserver auf das Gebäudebeziehungsweise Lichtmanagementsystem 21 zugreifen.

35 Auch funkbasierte Sende- und Empfangseinheiten, die mit dem Treiber 11 verbunden sind, beispielsweise die Bake 16, die in diesem Fall zweckmäßigerweise für bidirektionale

Funkübertragungen ausgelegt ist, können für das Einspielen der Verschlüsselungsschlüssel EKey dienen. Hier bieten sich Baken oder Beacons an, die mit dem Leuchten-Treiber 11 verbunden sind. Diese lassen sich auch als Empfänger für
5 Daten verwenden und somit auch als Datenpfad für die Schlüsselverteilung nutzen. Die Sende-Empfangs-Einheiten in Form der bidirektional arbeitenden Baken 16 können untereinander ein drahtloses Netzwerk (Mesh) aufbauen, sodass an nur einem Zugangspunkt dieses drahtlosen Netzwerkes ein
10 Gateway 22 vorgesehen ist, an welchem die Verschlüsselungsschlüssel EKey eingespielt werden können.

In der Fig. 5 sind mehrere Leuchten 12 sowie mehrere Baken 16 dargestellt, die ein drahtloses Kommunikationsnetzwerk
15 bilden. Ein solches Netzwerk wird als Maschennetz Mesh bezeichnet. Für den Zugang zu diesem drahtlosen Kommunikationsnetzwerk ist das Gateway 22 vorgesehen. Die Verteilung der Entschlüsselungsschlüssel DKey an die verschiedenen Leuchten 12 erfolgt hierbei entsprechend der
20 Vermaschung des Netzes jeweils von einer Bake 16 zu einer im Maschennetz folgenden Bake 16.

Die Verschlüsselungsschlüssel EKey können von einer Servereinheit 20 an das lokale Gateway 22 übertragen werden
25 oder über das mobile Endgerät 14 an das Gateway 22 übertragen werden.

Ebenso kann auch vorgesehen sein, den Verschlüsselungsschlüssel EKey in eine Sende-Empfangs-
30 Einheit, beispielsweise in eine bidirektional betreibbare Bake 16, zu übertragen. Auch derartige Sende-Empfangs-Einheiten können statische Identifikationsdaten ID aussenden, die nicht geschützt sind. Um die Identifikationsdaten ID auch bei diesen Sende-Empfangs-Einheiten zu schützen, kann die
35 gleiche Methode zur Schlüsselverteilung verwendet werden. Nur wird hierzu der Entschlüsselungsschlüssel DKey nicht an die Leuchte 12 weitergereicht, sondern direkt von den Sende-Empfangs-Einheiten (Bake 16) verwendet.

Falls nicht ein zentraler, für alle Leuchten 12 und/oder Sende-Empfangs-Einheiten einheitlich gültiger Verschlüsselungsschlüssel EKey verwendet werden soll ist, sondern für jede Leuchte 12 / Sende-Empfangs-Einheit individuelle Verschlüsselungsschlüssel EKey verteilt werden sollen, kann für die Adressierung der Entschlüsselungsschlüssel DKey bei der Verteilung vorgesehen sein, die Schlüssel individuell zuzuordnen, wie in der Fig. 2 dargestellt. Hierbei ist es wichtig, den richtigen Verschlüsselungsschlüssel EKey der vorgesehenen Leuchte 12 beziehungsweise den Sende-Empfangs-Einheiten (welche im Übrigen als Teil derjenigen Beleuchtungseinrichtung betrachtet werden, mit der sie in direkter Kommunikationsverbindung stehen) zu senden. Dies kann über eine Routing-Tabelle geschehen, wo alle Leuchten 12 beziehungsweise Sende-Empfangs-Einheiten lokal abgebildet sind. In dieser Routing-Tabelle sind die möglichen Kommunikationswege eingezeichnet, über die ein Verschlüsselungsschlüssel EKey an die richtige Position gebracht werden kann. Die Synchronisierung der Schlüsselauswahl und Abfolge kann durch eine zeitliche Synchronisierung erreicht werden, wofür eine einheitliche Zeitbasis auf beiden Seiten erforderlich ist, was den Nachteil aufweist, dass beide Komponenten (Sender und Empfänger) einen synchronen Taktgeber benötigen, was einen nicht unerheblichen Aufwand bedeutet.

Die Synchronisierung der Schlüssel kann vorteilhaft über den Datenstrom der verschlüsselten Nachricht Code selbst erfolgen. Hierzu werden neben den eigentlichen verschlüsselten Identifikationsdaten ID weitere Signalisierungsbits x in einer Signalisierungsbitfolge KeySig der verschlüsselten Nachricht Code verwendet, wie in der Fig. 6 dargestellt. Über diese Signalisierungsbits x kann dem Empfänger mitgeteilt werden, welcher der jeweiligen Entschlüsselungsschlüssel DKey[1...m] zur Entschlüsselung verwendet werden muss.

Gemäß der Darstellung in der Fig. 6 kann eine Leuchten-ID mit dem binären Wert 1010101 durch einen Verschlüsselungsschlüssel EKey mit dem binären Wert 1110000
5 mittels einer XOR-Operation zu dem binären Wert 0100101 codiert werden. Dem codierten Wert wird außerdem noch eine Signalisierungsbitfolge KeySig bestehend aus drei Signalisierungsbits x angehängt, mittels derer der Empfänger erkennen kann, welchen Schlüssel er zur Entschlüsselung der
10 Nachricht Code anwenden muss. In dem dargestellten Beispiel handelt es sich um eine Form der symmetrischen Verschlüsselung, bei der der Verschlüsselungsschlüssel EKey gleich dem Entschlüsselungsschlüssel DKey ist. Durch die bitweise Anwendung eines XOR-Operators auf die Nachricht Code
15 und den Entschlüsselungsschlüssels DKey ergibt sich wiederum die ursprüngliche Leuchten-ID L-ID.

Fig. 7 zeigt beispielhaft, welche Informationen mittels einer Signalisierungsbitfolge KeySig an einen Empfänger der
20 verschlüsselten Nachricht Code bereitgestellt werden können. Beispielsweise kann die Bitfolge signalisieren, dass eine Verschlüsselung aktiv ist (EncryptionActive), einen der aktuellen Verschlüsselung zugrundeliegenden Schlüssel aus einem Pool von zur Verfügung stehenden Schlüsseln zu
25 referenzieren (KeySelection), sowie eine mögliche Verschiebung des jeweiligen Ausgangsschlüssels durch eine bitweise Rotation in eine vorgebbare Anzahl Bits mit vorgebbbarer Richtung anzuzeigen (Shift&Direction).

30 Fig. 8 zeigt die Möglichkeit, aus einem Pool vorgegebener Schlüssel Key_000, Key_001, Key_010, Key_011 ... Key_111 in Abhängigkeit von der Signalisierungsbitfolge KeySig den jeweiligen Schlüssel auszuwählen. Bei einer Anzahl $N = 3$ der Signalisierungsbits x ergibt sich somit über $2^N = 8$ mögliche
35 Schlüssel.

Weiterhin kann die Generierung eines eindeutigen Verschlüsselungsschlüssels EKey jeweils in der lokalen

Leuchte 12, insbesondere in deren Treiber 11, beziehungsweise in der jeweiligen lokalen Sende-Empfangs-Einheit, stellvertretend in der Fig. 5 dargestellt durch die Baken 16, erfolgen. Werden die Verschlüsselungsschlüssel EKey[loc] lokal erzeugt und diese erzeugten individuell lokalen Verschlüsselungsschlüssel EKey[loc] an die Servereinheit 20 zur Verwaltung übermittelt, entsteht eine wesentlich geringere Komplexität, da es nur einen Empfänger gibt und somit keine Routing-Tabelle erzeugt und gepflegt werden muss. Jede Leuchte 12 sendet hierzu ihren eigenen individuell erzeugten Verschlüsselungsschlüssel EKey[loc] zusammen mit den jeweils festen Identifikationsdaten ID aus, die der Leuchte 12 zugeordnet wurden. Anstatt der Identifikationsdaten ID kann auch die genaue lokale Position der Leuchte 12 übermittelt werden, wo dieser Schlüssel zum Einsatz kommt. So wird auf der Servereinheit 20 eine Tabelle aufgebaut, welche die lokalen Schlüssel und die individuellen Identifikationsdaten ID beziehungsweise die Position der Leuchte 12 / der Bake 16 (Sende-Empfangs-Einheit) enthält.

Um das Beleuchtungssystem 100 noch besser zu schützen, kann die Schlüsselgenerierung von der Servereinheit 20 ausgelöst werden. Hierzu wird ein Signal an alle Baken 16 / Leuchten 12 / Sende-Empfangs-Einheiten gesendet, wie in der Fig. 5 dargestellt. Idealerweise wird dieser Prozess in Zeiten ausgeführt, wo das Beleuchtungssystem 100 nicht im Einsatz ist beziehungsweise kein oder nur ein geringes Datenaufkommen herrscht, beispielsweise nachts. Somit wechselt auf der Seite der Servereinheit 20 jeweils nur einmal der Verschlüsselungsschlüssel EKey[temp], während die Leuchten 12 beziehungsweise die Baken 16 dann lokal jeweils einen unabhängigen Verschlüsselungsschlüssel EKey[temp,loc] daraus erzeugen.

Um die Datenmenge zu verteilen, die bei der Rückmeldung der neuen Verschlüsselungsschlüssel EKey entsteht, kann ein individueller zeitlicher Versatz definiert werden. Um nicht jeder Einheit, also den in dem Maschennetz Mesh eingebundenen

Komponenten in Form der Leuchte 12, Baken 16 sowie sonstige Sende-Empfangs-Einheiten wie WLAN-Router 18, welche jeweils über einen eigenen Schlüsselgenerator verfügen, einen individuellen Zeitversatz zwischen dem Signal zur neuen
5 Schlüsselgenerierung und dem Senden der neuen Verschlüsselungsschlüssel EKey an die Servereinheit 20 mitteilen zu müssen, was einen erheblichen Adressierungs- und Kommunikationsaufwand bedeutet, kann dieser Zeitversatz bei der Herstellung der jeweiligen Geräte einprogrammiert werden.

10

Alternativ oder zusätzlich kann eine fest abgelegte individuelle Identifikationsnummer beziehungsweise Herstellernummer als Offset/Zeitversatz verwendet werden. An dem Netzwerk wechseln somit nicht alle Teilnehmer
15 gleichzeitig den Verschlüsselungsschlüssel EKey, sondern schalten diesen zeitversetzt gültig und übermitteln ihn dann. Die Erzeugung und die Aktivierung des Schlüssels können somit getrennt vorgenommen werden.

20 Die Anzahl N der Signalisierungsbits x bestimmt die Anzahl der möglichen Schlüssel $m = 2^N$. Bei $N = 8$ ergibt sich eine Auswahl von $m=256$ verschiedenen Schlüsseln, oder bei $N = 3$ wie in der Fig. 8 dargestellt $m = 8$. Um die Anzahl der Schlüssel weiter zu erhöhen, aber die Anzahl der
25 Signalisierungsbits x nicht weiter ansteigen zu lassen oder den Adressraum für die eigentliche Identifikationsdaten ID nicht weiter zu verringern, können auch ganze Gruppen von Schlüsseln verwendet werden, die über die Signalisierungsbits x adressiert werden. Bei der Verwendung von 256 Gruppen mit
30 jeweils 100 Schlüsseln ergeben sich somit 25.600 verschiedene Schlüssel. Bei einer Übertragungsrate von 100 Millisekunden je verschlüsselter Identifikationsdaten ID würde sich also ein Schlüssel alle 2.560 Sekunden beziehungsweise nach circa 42 Minuten wiederholen, sodass ein Auslesen entsprechend
35 lange dauern würde.

Um den Schutz des Beleuchtungssystems 100 noch weiter zu erhöhen, kann anstatt einer zentralen Aufforderung zur

Schlüsselerzeugung auch eine lokale individuelle zufallsgesteuerte Schlüsselerzeugung erfolgen. Diese Zufallssteuerung kann über interne Zähler ausgelöst werden, die mit Zufallswerten starten. Die Zeitbasis kann so gewählt werden, dass eine Schlüsselerzeugung innerhalb von Stunden, Tagen oder Wochen erfolgen kann. Sobald ein neuer lokaler Verschlüsselungsschlüssel EKey[n+1,loc] erzeugt wird, wird dieser an die Servereinheit 20 übermittelt.

10 Solange die Servereinheit 20 den neuen individuellen Verschlüsselungsschlüssel EKey[n,loc] noch nicht empfangen und zugeordnet hat, ist es vorteilhaft, wenn der alte Verschlüsselungsschlüssel EKey[n-1,loc] temporär beibehalten wird, sodass der Dienst unterbrechungsfrei sichergestellt wird. Auf der Servereinheit 20 sind alter und neuer Verschlüsselungsschlüssel EKey[n-1,loc], EKey[n,loc] bekannt und können somit beispielsweise sowohl eine alte als auch eine neue Abfrage der Identifikationsdaten ID beantworten.

20 Zur Detektion und Lokalisierung von unerlaubten Serviceabfragen beziehungsweise Positionsabfragen können auf der Servereinheit 20 die „alten“ Verschlüsselungsschlüssel EKey[n-1,loc], EKey[n-2,loc], EKey[n-2,loc] etc. weiter abgespeichert werden, sodass eine Schlüsselhistorie entsteht.

25 Erfolgt nun eine Abfrage von Identifikationsdaten ID, welche mit einem veralteten Verschlüsselungsschlüssel EKey[n-2,loc] verschlüsselt wurde, ist dies ein Hinweis darauf, dass es sich hierbei um einen nicht authentifizierten Zugriff handelt. Hierdurch lassen sich weitere Maßnahmen ableiten, beispielsweise eine gezielte Deaktivierung einer eventuell veralteten App auf dem mobilen Endgerät 14, welche Verschlüsselung noch nicht unterstützt, oder das Anbieten einer neuen App-Version. Ebenso kann eine Lokalisierung des mobilen Endgeräts 14 vorgenommen werden, welches die nicht

30 authentifizierten Zugriffe durchführt.

Alternativ oder zusätzlich können die Signalisierungsbits x über einen weiteren Kanal lokal verteilt werden,

beispielsweise über eine mit dem jeweiligen Treiber 11 einer Leuchte 12 verbundenen Bake 16 (Beacon) oder über einen Mobilfunkkanal zwischen der Servereinheit 20 beziehungsweise dem mobilen Endgerät 14 und der Leuchte 12.

5

Der Aufwand, auf ein solches Beleuchtungssystem 100 zugreifen zu können ohne die Kenntnis der Entschlüsselungsschlüssel DKey, kann weiter erhöht werden, wenn die Gültigkeit von Entschlüsselungsschlüsseln DKey in eine lokale Abhängigkeit gesetzt werden, das heißt ein bestimmter Satz an Entschlüsselungsschlüsseln DKey[loc] nur für Teile des Beleuchtungssystems 100 innerhalb eines bestimmten Raumes gültig ist. So kann über eine Bake 16 (Beacon) eine grobe Lokalisierung erfolgen. Hieraus kann abgeleitet werden, welcher Entschlüsselungsschlüssel DKey[loc] in diesem Bereich gültig ist.

Um die Zugriffsmöglichkeiten auf eine statische Leuchten-ID durch statische Verschlüsselungsschlüssel EKey – insbesondere bei einer symmetrischen Verschlüsselung – einzuschränken, kann neben der Erhöhung der Anzahl N der Schlüssel und Rotation dieser Schlüssel auch der Schlüssel selbst wie in der Fig. 9 dargestellt rotieren. Die Länge des Schlüssels und die Anzahl und Art der Schlüsselverschiebungen bestimmen dabei den zusätzlichen Verschlüsselungsraum. Unter der Annahme, dass die Länge der Identifikationsdaten ID 10 Bit und die Länge des Schlüssels ebenfalls 10 Bit beträgt, so wiederholt sich der Schlüssel nach zehn Schritten in einem Schieberegister wieder. Für das oben genannte Beispiel bedeutet dies, dass jeder der 100 Schlüssel zehnmal benutzt werden kann, ehe er sich wiederholt. Hierdurch erhöht sich die Zeit, bis sich ein Schlüssel wiederholt, auf 420 Minuten.

Durch eine Verlängerung der Schlüssellänge von 10 Bit auf 1024 Bit erhöht sich linear auch die Dauer auf das 1.224-fache ($1.024 * 420 \text{ Minuten} = 7.168 \text{ Stunden} = \text{ungefähr } 300 \text{ Tage}$).

Aus vorhandenen Schlüsseln können durch Kombination neue Schlüssel erzeugt werden. Wird ein Schlüssel Key_1 mit einem anderen Schlüssel Key_2 über eine Rechenvorschrift verknüpft, beispielsweise eine XOR-Verknüpfung, entsteht ein neuer

5 Schlüssel Key_12 wie in der Fig. 11 dargestellt. Bei 100 Schlüsseln lassen sich somit 4.950 neue Schlüssel erzeugen ($N * (N-1)/2$) mit $N = \text{Anzahl der Schlüssel}$). In diesem weiterentwickelten Beispiel würde dies eine Zeitdauer bis zum Wiederholen der gleichen Nachricht Code, welche die

10 verschlüsselten Identifikationsdaten ID beinhaltet, auf das ungefähr 50-fache verlängern, also auf 15.000 Tage oder 41 Jahre.

Diese Methoden für die Verschlüsselung einer Leuchten-ID als

15 Identifikationsdaten ID lassen sich auch auf Daten erweitern, die ebenfalls über Licht übertragen werden könnten und nach diesem Verfahren gesichert übertragen werden können.

Fig. 9 zeigt mögliche Operationen, die auf einen vorhandenen

20 Schlüssel angewendet werden können. Beispielsweise kann das linke Bit anzeigen, dass ein Schlüssel nach links zu verschieben ist (key shift left, KSL) und/oder das rechte Bit in der Signalisierungsbitfolge KeySig kann anzeigen, dass der Schlüssel nach rechts geschoben werden soll (key shift right,

25 KSR). Tatsächlich ist auf Bitebene mit Verschieben/Shift das Rotieren der Bits in einem Schieberegister gemeint, bei welchem ein aus dem Schieberegister herausgeschobenes Bit auf der gegenüberliegenden Seite wieder eingeschoben wird. Das mittlere Bit kann dazu benutzt werden anzuzeigen, dass ein

30 vordefinierter Algorithmus Calc zur Veränderung des Schlüssels beziehungsweise der Parameter zur Anwendung einer Rechenvorschrift ausgeführt werden soll.

Fig. 10 zeigt, wie ausgehend von einem Ausgangsschlüssel Key0

35 ein erster Schlüssel Key1, ein zweiter Schlüssel Key2, ein dritter Schlüssel Key3, ein vierter Schlüssel Key4 und so weiter durch bitweise Rotation des Schlüssels erzeugt werden. Die Anwendung des ersten Schlüssels Key1 auf die

Identifikationsdaten ID ergibt somit eine erste Nachricht Code_1, eine Anwendung des zweiten Schlüssels Key2 auf die Identifikationsdaten ID ergibt dementsprechend eine zweite Nachricht Code_2 und entsprechend weiter.

5

Fig. 11 zeigt schließlich, wie aus dem Schlüssel Key_1 und dem Schlüssel Key_2 durch bitweise Anwendung eines XOR-Operators der neue Schlüssel Key_12 erzeugt werden kann.

- 10 Die Ausführungsbeispiele dienen lediglich der Erläuterung der Erfindung und sind für diese nicht beschränkend. So kann insbesondere die Erzeugung von neuen zweiten Schlüsseln in Abhängigkeit von vorhandenen ersten und/oder zweiten Schlüsseln und/oder Schlüsselgenerierungsmaterial beliebig
15 gestaltet sein, ohne den Gedanken der Erfindung zu verlassen.

Somit wurde voranstehend gezeigt, wie eine Schlüsselerzeugung und/oder eine Schlüsselrotation für die Verschlüsselung von ortsgebundenen Informationen zweckmäßig ausgestaltet sein
20 können.

Patentansprüche

1. Beleuchtungseinrichtung (12) zur Bereitstellung einer Datenübertragung an ein mobiles Endgerät (14), umfassend:

- 5 - ein Leuchtmittel (13), und
 - ein elektronisches Betriebsgerät (11) zum Betreiben des Leuchtmittels,
 gekennzeichnet durch:
 - eine Datenspeichereinheit, in der in einem dafür
10 reservierten Speicherbereich ein Satz von ersten Schlüsseln
 (Key_000 bis Key_111) gespeichert ist,
 - eine Auswahleinheit, welche dazu ausgelegt ist, in
 Abhängigkeit von einem an einer Datenschnittstelle der
 Beleuchtungseinrichtung bereitstellbaren
15 Schlüsselwechselsignal und/oder in Abhängigkeit von einem
 durch einen Schlüsselwechseltaktgeber der
 Beleuchtungseinrichtung bereitstellbaren
 beleuchtungseinrichtungsinternen Schlüsselwechselsignal einen
 ersten Schlüssel aus dem Satz von ersten Schlüsseln
20 auszuwählen,
 - eine Verschlüsselungseinheit, welche dazu ausgelegt ist,
 den ausgewählten ersten Schlüssel aus dem reservierten
 Speicherbereich auszulesen und Messwertedaten und/oder
 Identifikationsdaten (ID), welche zur Übertragung an das
25 mobile Endgerät bestimmt sind, gemäß einer vorgebbaren
 Verschlüsselungsoperation in eine mit dem ausgewählten ersten
 Schlüssel verschlüsselte Nachricht (Code) umzusetzen, und
 - eine Sendeeinheit (13, 16), welche dazu ausgelegt ist, die
 verschlüsselte Nachricht an das mobile Endgerät zu senden.

30

2. Beleuchtungseinrichtung (12) nach Anspruch 1,
dadurch gekennzeichnet,

- dass die Auswahleinheit dazu ausgelegt ist, den ausgewählten
 ersten Schlüssel in Abhängigkeit von dem
35 Schlüsselwechselsignal gemäß einem vorgebbaren Schema aus dem
 Satz von ersten Schlüsseln zu ermitteln.

3. Beleuchtungseinrichtung (12) nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

dass die Auswahleinheit dazu ausgelegt ist, die Auswahl des
5 ersten Schlüssels zumindest anteilig in Abhängigkeit von
einer Zufallsvariablen zu treffen, welche mittels eines
Zufallsgenerators bereitstellbar ist.

4. Beleuchtungseinrichtung (12) nach einem der vorhergehenden
10 Ansprüche,

dadurch gekennzeichnet,

dass die Verschlüsselungseinheit dazu ausgelegt ist, den
ausgewählten ersten Schlüssel vor der Verwendung mit der
Verschlüsselungsoperation um eine vorgebbare Anzahl von

15 Bitpositionen in einem Schieberegister zu verschieben und
dabei in Schieberichtung aus dem Schieberegister

herausgeschobene Bits auf der gegenüberliegenden Seite wieder
einzuschieben.

20 5. System (100) mit mindestens einer ersten und mindestens
einer zweiten Beleuchtungseinrichtung (12) nach jeweils einem
der vorhergehenden Ansprüche, wobei die mindestens eine erste
und die mindestens eine zweite Beleuchtungseinrichtung
jeweils einen eigenen Satz von ersten Schlüsseln (Key_000 bis
25 Key_111) aufweist.

6. System (100) nach Anspruch 5,

gekennzeichnet durch,

eine Bake (16) zur Bereitstellung von

30 Positionsbestimmungsdaten mittels eines Funksignals, wobei
die Positionsbestimmungsdaten in dem System einem Bereich
zugeordnet sind, der eine Montageposition der ersten
Beleuchtungseinrichtung umfasst.

35 7. System nach Anspruch 5 oder 6,

gekennzeichnet durch

eine zentrale Schlüsselverwaltungseinheit(20), welche dazu
ausgelegt ist, ein Schlüsselwechselsignal an die mindestens

eine erste und die mindestens eine zweite Beleuchtungseinrichtung (12) zu senden, wobei das Schlüsselwechselsignal zumindest anteilig Schlüsselgenerierungsmaterial umfasst, und wobei die

5 jeweilige Verschlüsselungseinheit dazu ausgelegt ist, in Abhängigkeit von dem jeweils ausgewählten ersten Schlüssel und von dem übertragenen Schlüsselgenerierungsmaterial gemäß einer vorgebbaren Berechnungsvorschrift einen jeweils neuen zweiten Schlüssel zu ermitteln, wobei die jeweilige

10 Datenspeichereinheit dazu ausgelegt ist, den jeweiligen zweiten Schlüssel als zusätzlichen ersten Schlüssel in dem jeweiligen Satz von ersten Schlüsseln zu ergänzen.

8. Verfahren zur Bereitstellung einer Datenübertragung an ein

15 mobiles Endgerät (14) mittels einer Beleuchtungseinrichtung (12)

gekennzeichnet durch:

- Speichern eines Satzes von ersten Schlüsseln (Key_000 bis Key_111) in einem dafür reservierten Speicherbereich einer

20 Datenspeichereinheit der Beleuchtungseinrichtung,

- Auswählen eines ersten Schlüssels aus dem Satz von ersten Schlüsseln in Abhängigkeit von einem an einer Datenschnittstelle der Beleuchtungseinrichtung bereitstellbaren Schlüsselwechselsignal und/oder in

25 Abhängigkeit von einem durch einen Schlüsselwechseltaktgeber der Beleuchtungseinrichtung bereitstellbaren beleuchtungseinrichtungsinternen Schlüsselwechselsignal,

- Auslesen des ausgewählten ersten Schlüssels aus dem reservierten Speicherbereich,

30 - Umsetzen von Messwertedaten und/oder Identifikationsdaten (ID), welche zur Übertragung an das mobile Endgerät bestimmt sind, gemäß einer vorgebbaren Verschlüsselungsoperation in eine mit dem ausgewählten ersten Schlüssel verschlüsselte Nachricht (Code), und

35 - Senden der verschlüsselten Nachricht an das mobile Endgerät durch eine Sendeeinheit (13, 16) der Beleuchtungseinrichtung.

9. Verfahren nach Anspruch 8,

gekennzeichnet durch:

- Senden eines Schlüsselwechselsignals an die Beleuchtungseinrichtung, wobei das Schlüsselwechselsignal zumindest anteilig Schlüsselgenerierungsmaterial umfasst,
- 5 - Ermitteln eines zweiten Schlüssels in Abhängigkeit von dem ausgewählten ersten Schlüssel und von dem übertragenen Schlüsselgenerierungsmaterial gemäß einer vorgebbaren Berechnungsvorschrift, und
- Ergänzen des zweiten Schlüssels als zusätzlichen ersten
- 10 Schlüssel in dem Satz von ersten Schlüsseln.

10. Verfahren nach Anspruch 8 oder 9,

gekennzeichnet durch:

- Erzeugen eines zweiten Schlüssels (Key_12) zur Verwendung
- 15 mit der Verschlüsselungsoperation durch Kombination von zumindest zwei ersten Schlüsseln (Key_1, Key_2) aus dem Satz von ersten Schlüsseln gemäß einer vorgebbaren Kombinationsrechenvorschrift.

20

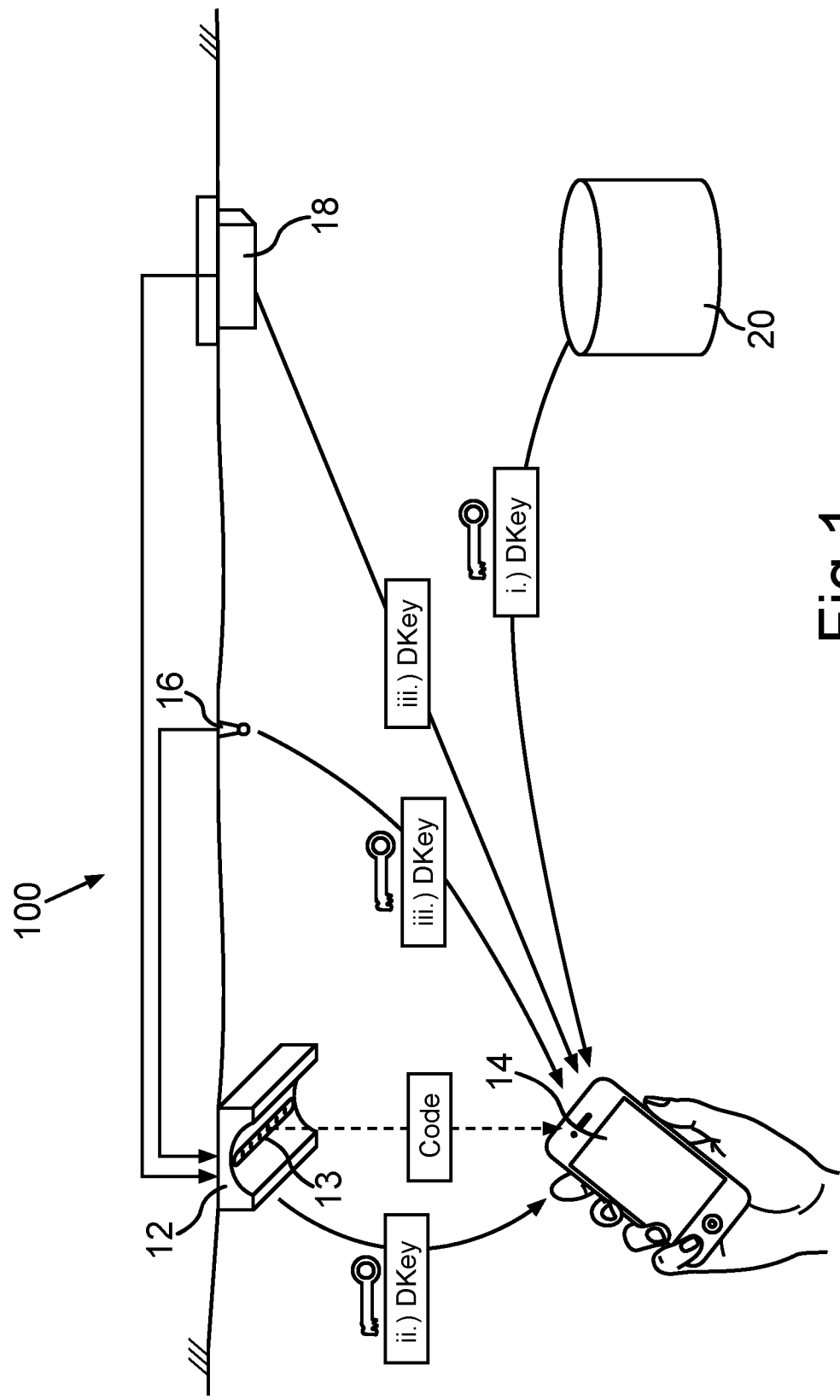


Fig.1

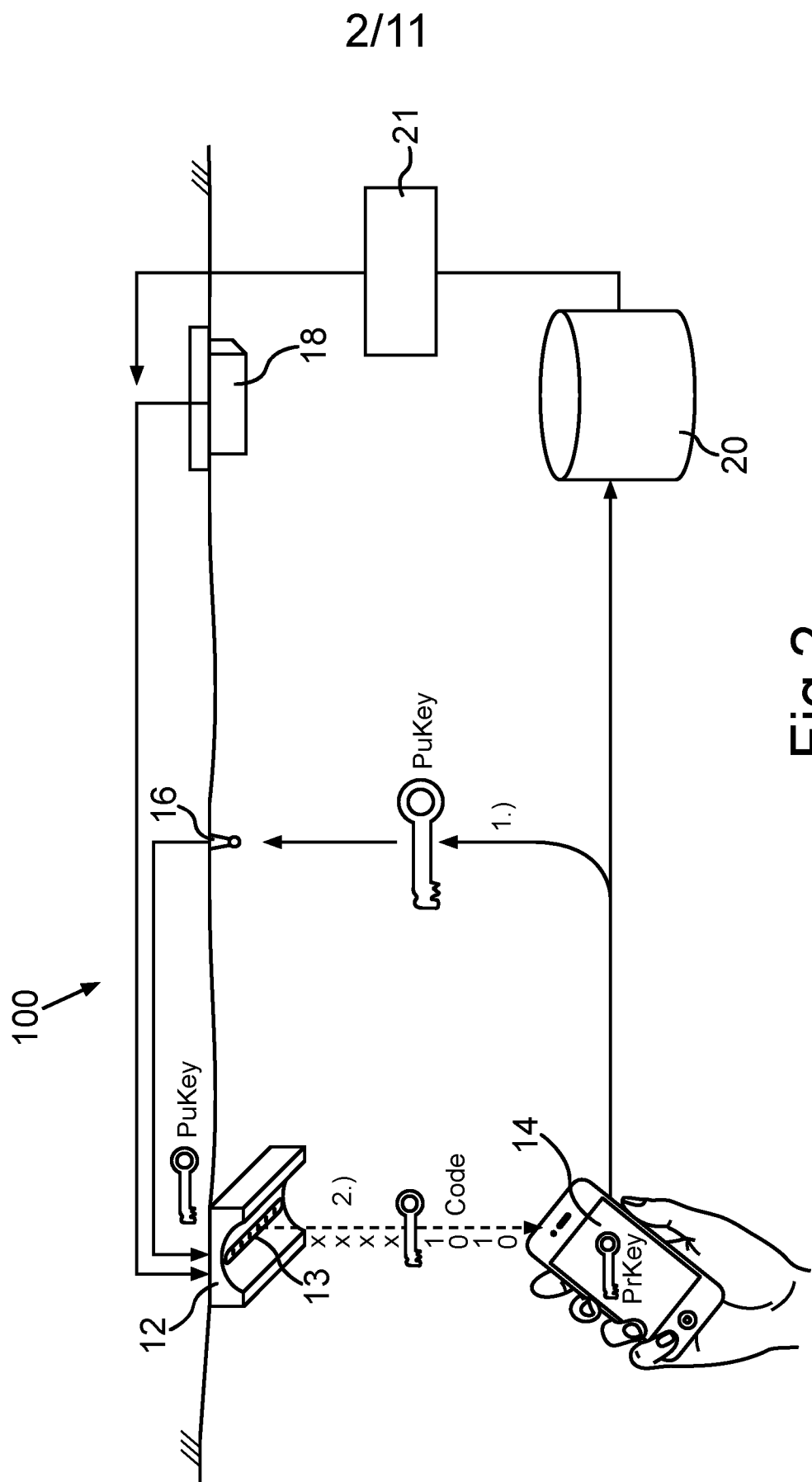


Fig.2

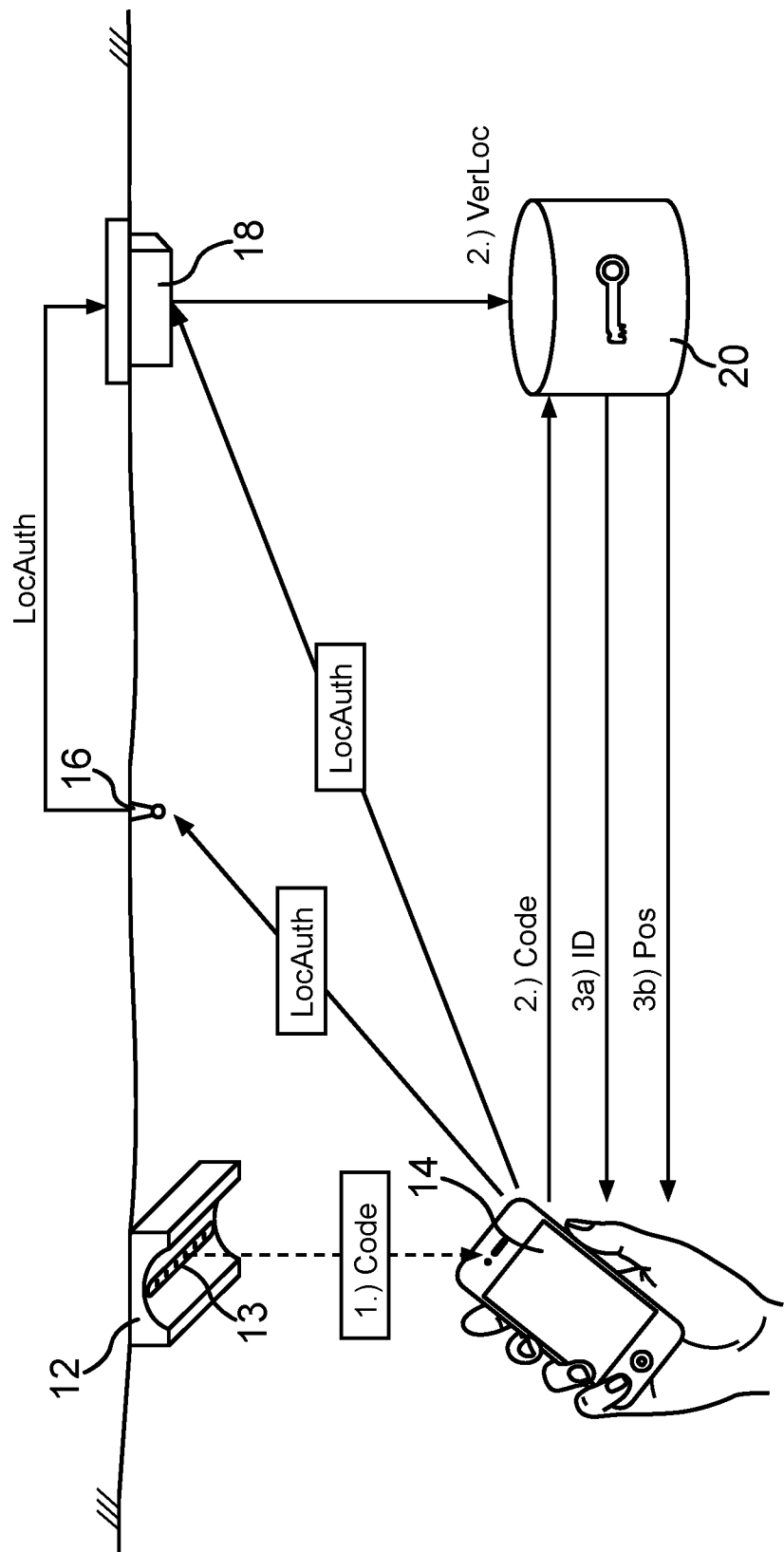


Fig.3

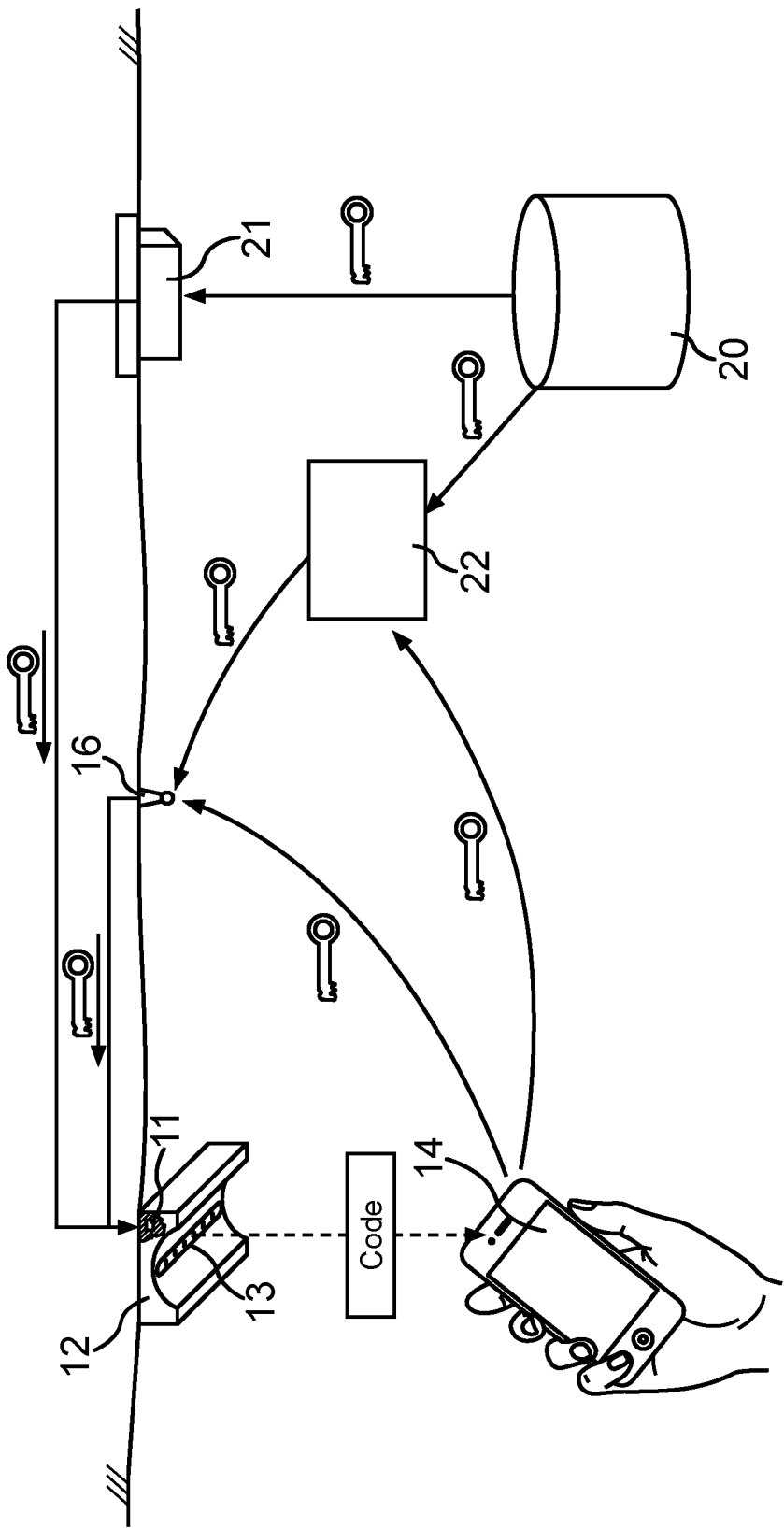


Fig.4

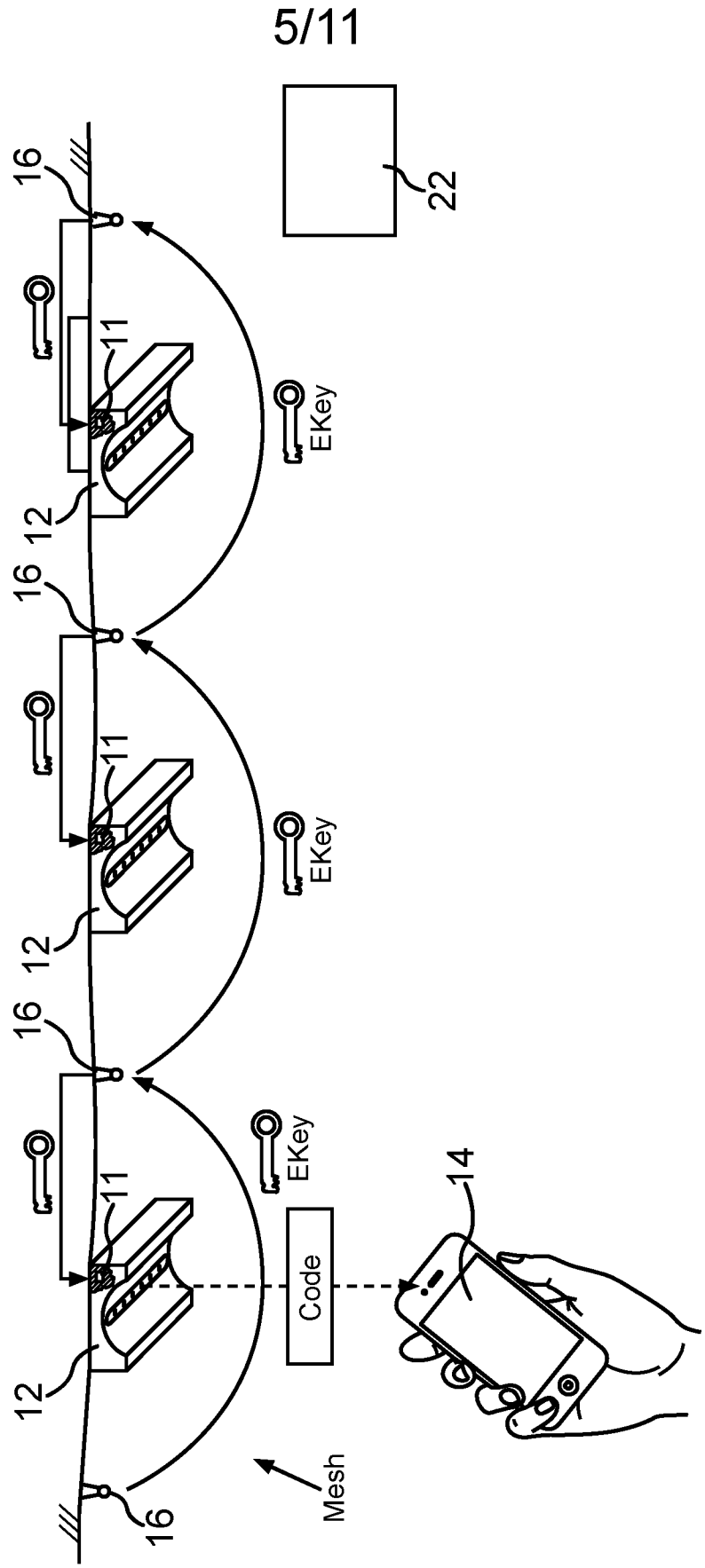


Fig.5

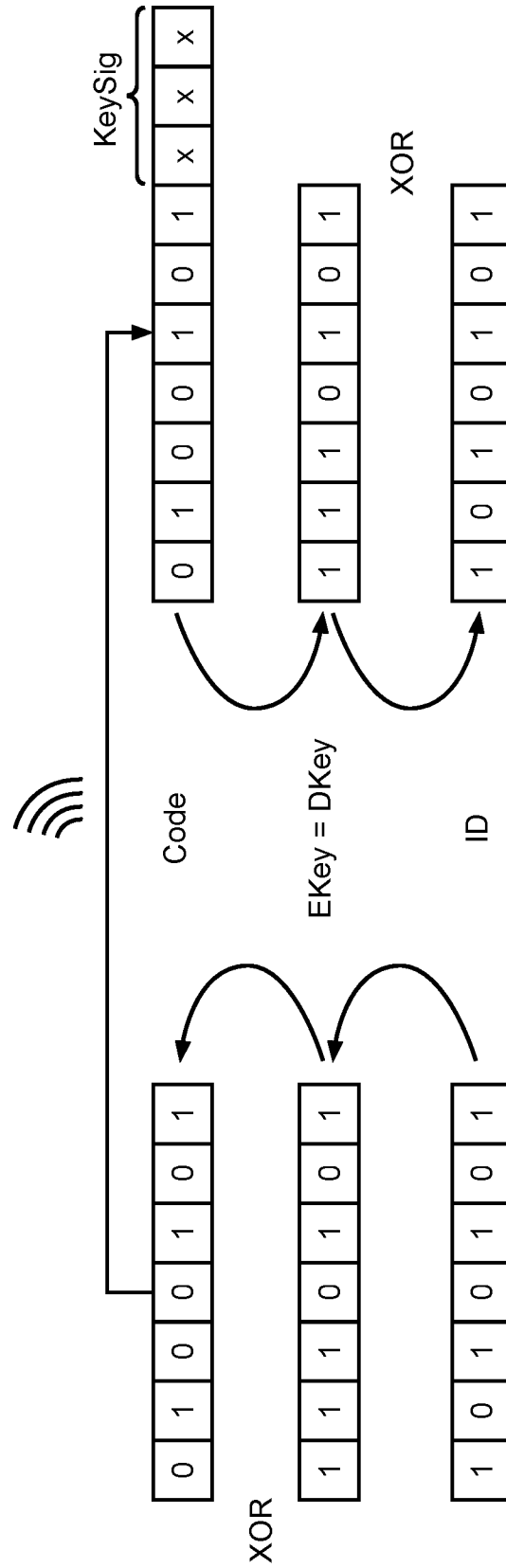


Fig. 6

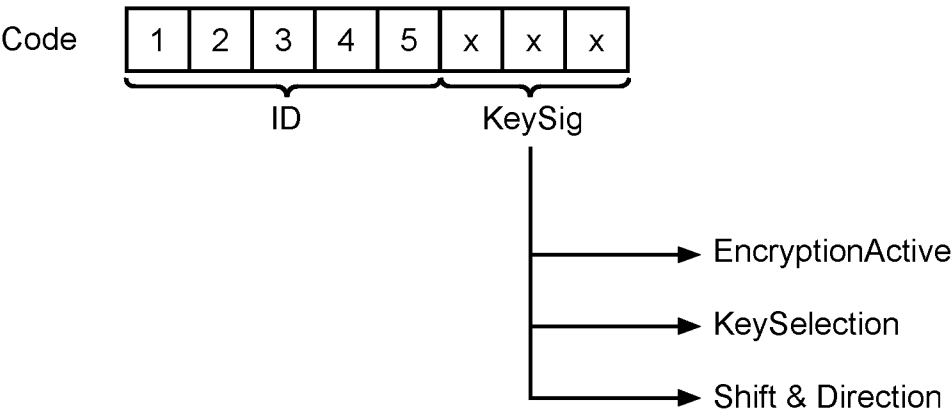


Fig.7

8/11

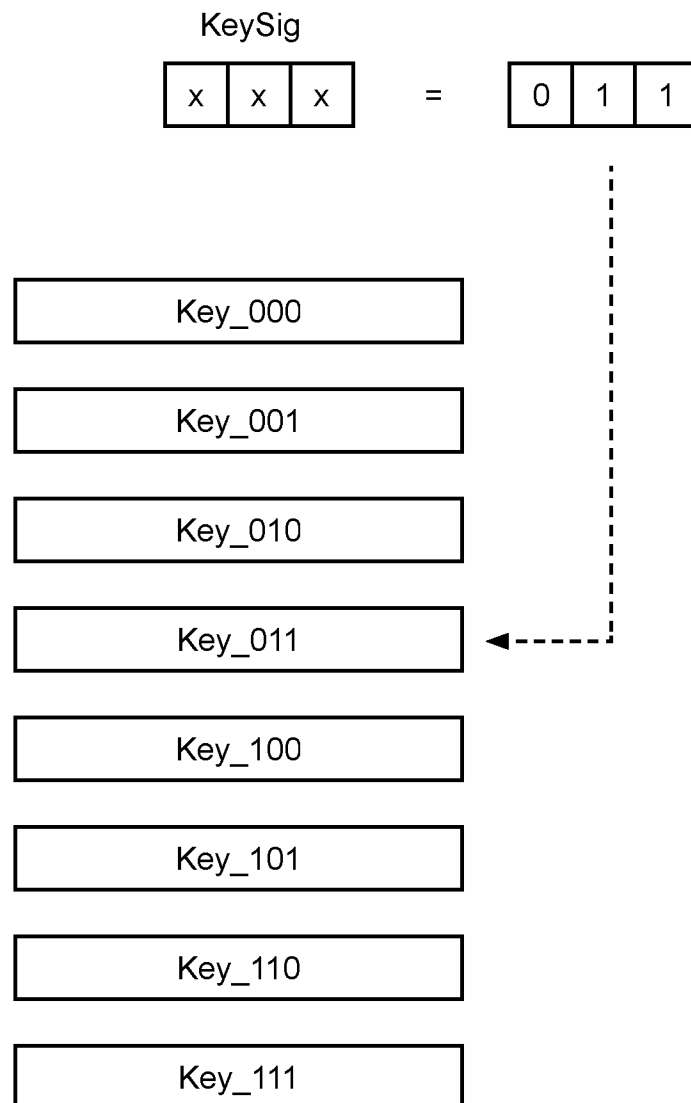


Fig.8

9/11

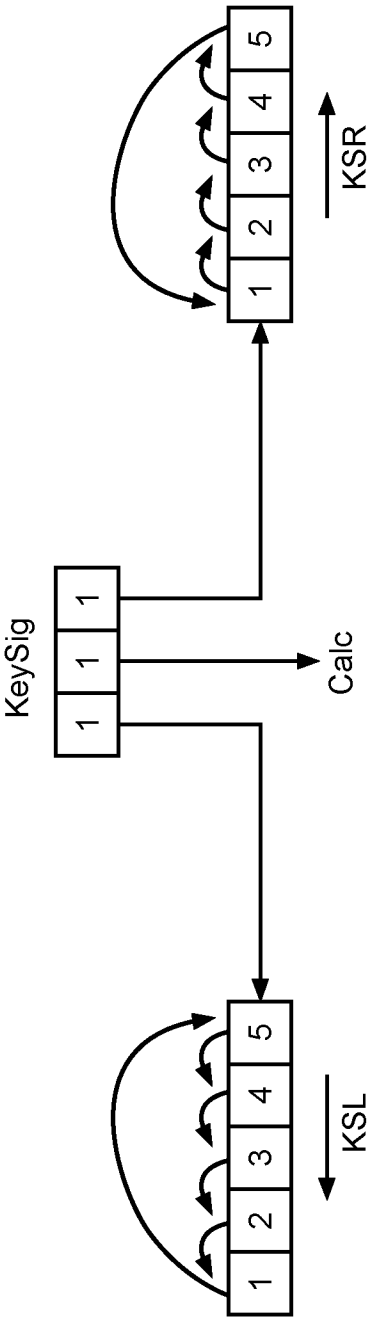


Fig.9

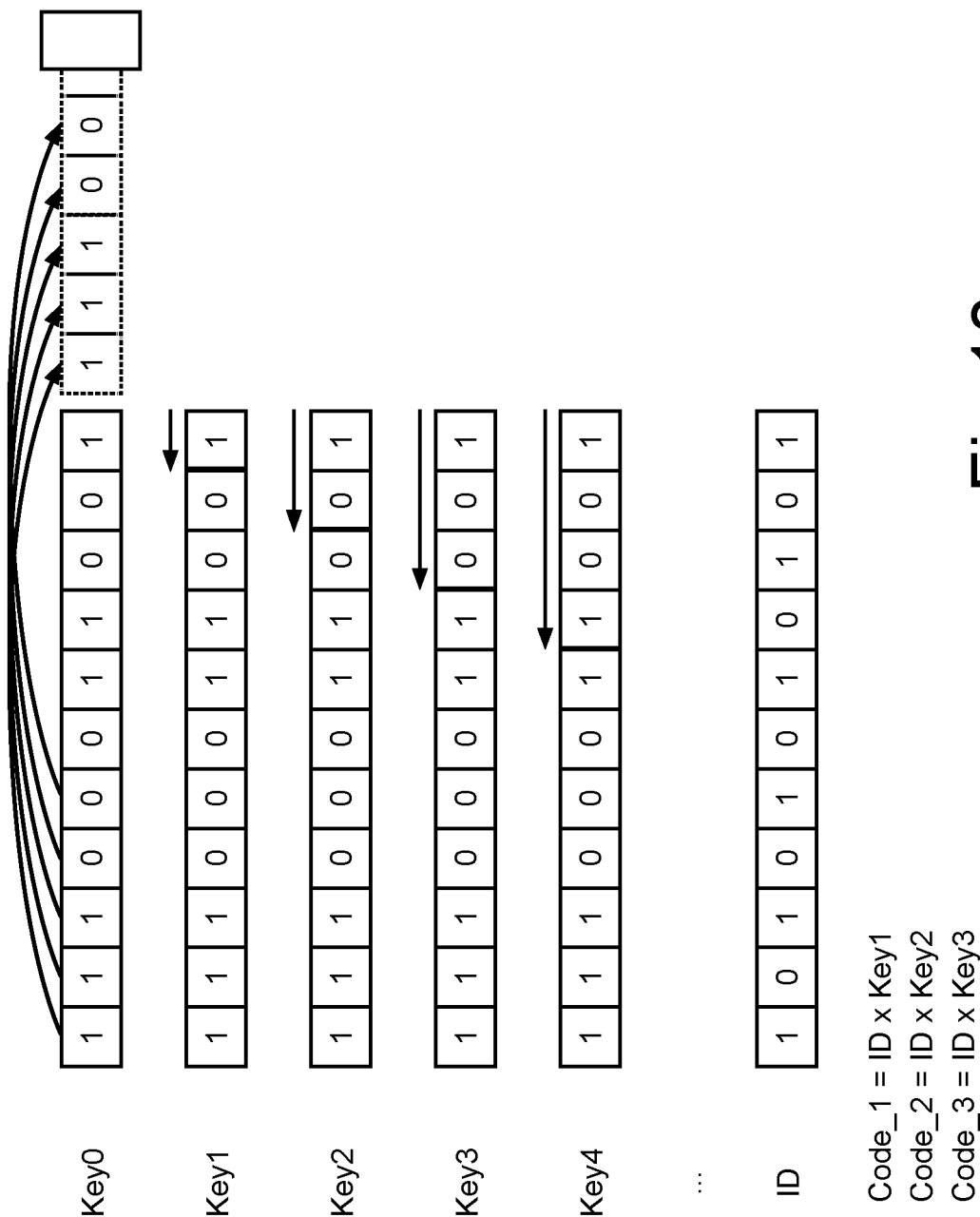


Fig.10

11/11

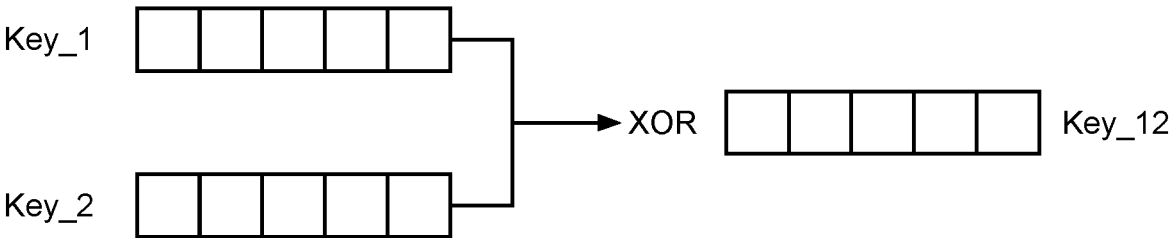


Fig.11

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/076547

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L9/08 H04B10/116
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)
H04W H04L H04B G08C

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 practicable, search terms used)

EPO-Internal, WPI Data, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 882 117 A1 (KUANG CHI INNOVATIVE TECH LTD [CN]) 10 June 2015 (2015-06-10) abstract; figures a1, a2, a3, a4, b1, b2, c1, c5 paragraphs [0003], [0072], [0077] paragraphs [0085] - [0088] paragraphs [0095], [0103], [0105] paragraphs [0132], [0134], [0146] ----- -/-	1-10



Further documents are listed in the continuation of Box C.



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 application or patent 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

10 January 2017

Date of mailing of the international search report

19/01/2017

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Schossmaier, Klaus

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/076547

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MOUSA FARAG ET AL: "Investigation of data encryption impact on broadcasting visible light communications", 2014 9TH INTERNATIONAL SYMPOSIUM ON COMMUNICATION SYSTEMS, NETWORKS & DIGITAL SIGN (CSNDSP), IEEE, 23 July 2014 (2014-07-23), pages 390-394, XP032660587, DOI: 10.1109/CSNDSP.2014.6923860 [retrieved on 2014-10-14] abstract; figures 1, 2, 3 Abschnitt I Abschnitt II Abschnitt III.A -----	1-10
A	WO 2015/148696 A1 (OSRAM SYLVANIA INC [US]) 1 October 2015 (2015-10-01) cited in the application abstract; figures 1, 2A, 2B, 5 paragraphs [0018] - [0020] paragraphs [0022], [0030], [0037] paragraphs [0058] - [0062] -----	1-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2016/076547

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2882117	A1	10-06-2015	EP 2882117 A1 10-06-2015
			JP 2015532030 A 05-11-2015
			KR 20150038018 A 08-04-2015
			US 2015146871 A1 28-05-2015
			WO 2014019526 A1 06-02-2014

WO 2015148696	A1	01-10-2015	NONE

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
 INV. H04L29/06 H04L9/08 H04B10/116
 ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
 H04W H04L H04B G08C

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, WPI Data, COMPENDEX, INSPEC, IBM-TDB

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 2 882 117 A1 (KUANG CHI INNOVATIVE TECH LTD [CN]) 10. Juni 2015 (2015-06-10) Zusammenfassung; Abbildungen a1, a2, a3, a4, b1, b2, c1, c5 Absätze [0003], [0072], [0077] Absätze [0085] - [0088] Absätze [0095], [0103], [0105] Absätze [0132], [0134], [0146] ----- -/--	1-10



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



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" frühere Anmeldung oder Patent, die bzw. 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 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

10. Januar 2017

Absendedatum des internationalen Recherchenberichts

19/01/2017

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040,
 Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Schossmaier, Klaus

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	MOUSA FARAG ET AL: "Investigation of data encryption impact on broadcasting visible light communications", 2014 9TH INTERNATIONAL SYMPOSIUM ON COMMUNICATION SYSTEMS, NETWORKS & DIGITAL SIGN (CSNDSP), IEEE, 23. Juli 2014 (2014-07-23), Seiten 390-394, XP032660587, DOI: 10.1109/CSNDSP.2014.6923860 [gefunden am 2014-10-14] Zusammenfassung; Abbildungen 1, 2, 3 Abschnitt I Abschnitt II Abschnitt III.A -----	1-10
A	WO 2015/148696 A1 (OSRAM SYLVANIA INC [US]) 1. Oktober 2015 (2015-10-01) in der Anmeldung erwähnt Zusammenfassung; Abbildungen 1, 2A, 2B, 5 Absätze [0018] - [0020] Absätze [0022], [0030], [0037] Absätze [0058] - [0062] -----	1-10

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2016/076547

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 2882117	A1	10-06-2015	EP 2882117 A1 10-06-2015
			JP 2015532030 A 05-11-2015
			KR 20150038018 A 08-04-2015
			US 2015146871 A1 28-05-2015
			WO 2014019526 A1 06-02-2014

WO 2015148696	A1	01-10-2015	KEINE
