(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
2. Februar 2017 (02.02.2017)

W I P O **I P C T**

(10) Internationale Veröffentlichungsnummer
WO 2017/016548 AI

(51) **Internationale Patentklassifikation:**
H04L 9/08 (2006.01) ***H04L 29/06*** (2006.01)

(21) **Internationales Aktenzeichen:** PCT/DE2016/100338

(22) **Internationales Anmeldedatum:**
26. Juli 2016 (26.07.2016)

(25) **Einreichungssprache:** Deutsch

(26) **Veröffentlichungssprache:** Deutsch

(30) **Angaben zur Priorität:**
10 2015 112 224.3 27. Juli 2015 (27.07.2015) DE

(71) **Anmelder: JACOBS UNIVERSITY BREMEN GGMBH** [DE/DE]; Campus Ring 1, 28759 Bremen (DE).

(72) **Erfinder: HENKEL, Werner;** Im Rucksort 10, 28832 Achim (DE).

(74) **Anwalt: WEIDNER STERN JESCHKE PATENTANWÄLTE PARTNERSCHAFT;** Rubianusstraße 8, 99084 Erfurt (DE).

(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, 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, 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 V*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eingehen (Regel 48 Absatz 2 Buchstabe h)*

(54) Title: METHOD FOR GENERATING A CRYPTOGRAPHIC KEY FOR A CABLE-BASED COMMUNICATION

(54) Bezeichnung : VERFAHREN ZUM ERZEUGEN EINES KRYPTOGRAPHISCHEN SCHLÜSSELS FÜR EINE KABELBASIERTE KOMMUNIKATION

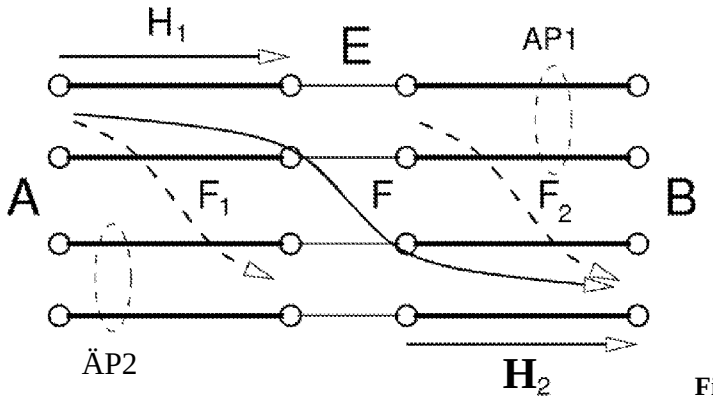

Fig. 1

(57) Abstract: The invention relates to a method for generating a cryptographic key for a cable-based communication for a first user and a second user, wherein the cable-based communication occurs between the first user and the second user by means of an information Channel, wherein the method comprises the following Steps: measuring a transmission function between the first and the second user by the first or the second user, quantizing the transmission function such that quantized values of the transmission function are available, and assigning a bit pattern to the quantized values of the transmission function, wherein the bit pattern forms the cryptographic key. The direct transmission function or the far-end crosstalk transmission function can be used as the transmission function. In place of the values of the transmission function, the frequencies of the local minimums or local maximums of the transmission function can be used for key generation.

(57) Zusammenfassung:

[Fortsetzung auf der nächsten Seite]

WO 2017/016548 A1

Die Erfindung betrifft ein Verfahren zum Erzeugen eines kryptographischen Schlüssels für eine kabelbasierte Kommunikation für einen ersten Benutzer als auch einen zweiten Benutzer, wobei die kabelbasierte Kommunikation zwischen dem ersten Benutzer und dem zweiten Benutzer mittels eines Informationskanals erfolgt, wobei das Verfahren folgende Schritte aufweist: Messen einer Übertragungsfunktion zwischen dem ersten und dem zweiten Benutzer durch den ersten oder den zweiten Benutzer, Quantisieren der Übertragungsfunktion, sodass quantisierte Werte der Übertragungsfunktion vorliegen, und Zuweisen eines Bitmusters zu den quantisierten Werten der Ütertragungsfunktion, wobei das Bitmuster den kryptographischen Schlüssel bildet. Hierbei kann als Ütertragungsfunktion die direkte Ütertragungsfunktion oder die Fernnebensprechübertragungsfunktion verwendet werden. Anstelle der Werte der Übertragungsfunktion können auch die Frequenzen der lokalen Minima oder lokalen Maxima der Ütertragungsfunktion zur Schlüsselgenerierung herangezogen werden.

Verfahren zum Erzeugen eines kryptographischen Schlüssels für eine kabelbasierte Kommunikation

Die Erfindung betrifft ein Verfahren zum Erzeugen eines kryptographischen Schlüssels für eine kabelbasierte Kommunikation und einen Rechner, welcher derart eingerichtet ist, dass ein solches Verfahren durchführbar ist .

Moderne asymmetrische Verschlüsselungsverfahren wie z.B. das Public-Key-Verschlüsselungsverf ahren benutzen einen öffentlichen Schlüssel, um einen Klartext in einen Geheimtext umzuwandeln, aus dem der Klartext mit einem geheimen Schlüssel wieder gewonnen werden kann. Hierbei muss der geheime Schlüssel unter allen Umständen geheim gehalten werden, und es muss praktisch unmöglich sein, ihn aus dem öffentlichen Schlüssel zu berechnen. Ferner muss sichergestellt sein, dass der öffentliche Schlüssel auch wirklich dem Empfänger zugeordnet ist.

Um die mit der Geheimhaltung verbundenen Probleme zu vermeiden, wurden Verfahren entwickelt, welche zum Ziel haben, den beiden Kommunikationspartner einen geheimen Schlüssel zu verschaffen, ohne, dass ein Dritter diesen geheimen Schlüssel erhalten kann. Neben den Methoden der Quantenkryptographie sind Verfahren bekannt, die die physikalischen Eigenschaften des verwendeten Kommunikationssystems benutzen.

US 2007/0177729 AI offenbart das Erzeugen eines geheimen Schlüssels in drahtlosen Kommunikationsnetzwerken.

WO 2010/030927 A2 offenbart ein Verfahren und ein System zum geheimen Schlüsselaustausch mittels der Eigenschaften der Draht losverbindung und der zufälligen Bewegung der Vorrichtung .

Aufgabe der Erfindung ist es, den Stand der Technik zu verbessern .

Gelöst wird die Aufgabe durch ein Verfahren zum Erzeugen eines kryptographischen Schlüssels für eine elektronische, kabelbasierte Kommunikation für einen ersten Benutzer als auch einen zweiten Benutzer,

wobei das Verfahren folgende Schritte aufweist:

- Messen einer Übertragungsfunktion oder Bestimmen einer aus der gemessenen Übertragungsfunktion abgeleiteten Größe zwischen dem ersten und dem zweiten Benutzer durch den ersten oder den zweiten Benutzer,

- Quantisieren der Übertragungsfunktion oder der daraus abgeleiteten Größe, sodass quantisierte Werte der Übertragungsfunktion oder der abgeleiteten Größe vorliegen, und

- Zuweisen eines Bitmusters zu den quant isierten Werten der Übertragungsfunktion oder der abgeleiteten Größe, wobei das Bitmuster zumindest einen Teil des kryptographischen Schlüssels bildet.

Mit dem vorliegenden Verfahren kann über eine elektronische, kabelbasierte Kommunikation bei zwei kommunizierenden Benutzern ein kryptographischer Schlüssel erzeugt werden, ohne dass der Schlüssel selbst übertragen werden muss und

ohne dass ein Dritter den Schlüssel erlangen kann. Dieses Erzeugen des Schlüssels basiert auf den physikalischen Eigenschaften des durch das Kabel charakterisierten Informationskanals. Dabei macht sich das Verfahren Die Tatsache zunutze, dass diese Übertragungsfunktionen zwischen einem Sender und Empfänger bei Vertauschen von Sender und Empfänger weitgehend symmetrisch, d.h. näherungsweise gleich, sind. Diese Symmetrie ermöglicht es, dass die beiden Benutzer der Kommunikation einen geheimen kryptographischer Schlüssel jeweils selbst generieren können, ohne dass der kryptographische Schlüssel selbst zwischen den beiden Benutzern über die kabelbasierte Kommunikation ausgetauscht werden müsste.

Die Übertragungs- und Fernnebensprechübertragungsf unkt ion sind bei einem idealen Kabel ohne Abzweigungen bis auf unterschiedliches Rauschen auf beiden Seiten und nichtideale Eigenschaften der Sende- und Empfangsein–richtungen gegenüber Vertauschen von Sender und Empfänger symmetrisch. Bei Fernnebensprechübertragungsf unkt ionen in einem Netzsegment mit Stichleitungen können sich Asymmetrien ergeben.

Folgendes Begriffliche sei vorab erläutert und soll für den gesamten Text gelten.

Ein „kryptographischer Schlüssel" ist insbesondere ein Schlüssel, welcher durch eine Bitfolge repräsentiert wird.

Die Kommunikation zwischen dem ersten und dem zweiten Benutzer erfolgt mittels eines insbesondere elektrischen Kabels, welches mindestens eine elektrisch leitende Ader

aufweist. In diesem Fall kann die direkte Übertragungsfunktion gemessen werden.

Um eine bessere Abschirmung zu erzielen, kann das Kabel mindestens ein Adernpaar aufweisen.

Um eine Fernnebensprechubertragungsf unktion messen zu können, kann das Kabel insbesondere mindestens zwei Adernpaare aufweisen.

Eine leitende Ader kann auch durch Erdverbindung ersetzt werden. Verbindungen zu den leitenden Adern können z.B. durch Steckdosen, Schneid- oder Klemmverbindungen gegeben sein .

Die Kommunikation erfolgt zwischen dem ersten und zweiten Benutzer. Der erste Benutzer wird insbesondere Alice und der zweite Benutzer insbesondere Bob genannt.

Der erste als auch der zweite Benutzer können Nachrichten senden und empfangen. Vor dem Verwenden wird die Nachricht mittels des kryptographischen Schlüssels verschlüsselt und nach dem Empfangen wird die empfangene Nachricht mittels des kryptographischen Schlüssels entschlüsselt.

Der Dritte, der eine Kommunikation zwischen dem ersten Benutzer und dem zweiten Benutzer abhören will, wird insbesondere auch Eve genannt.

Für diesen Dritten wird angenommen, dass ein gewisser Zugang zu dem Kabel besteht. Der Zugang kann durch weitere Steckdosen im Netzsegment gegeben sein. Ferner kann der Zugang auch durch direktes Kontaktieren der Adern mit Messspitzen oder Schneidverbindern geschehen.

Bevorzugt hat Eve zu Alice und/oder Bob einen Mindestabstand, welcher so gewählt sein soll, dass die von Eve abgehörten Übertragungsfunktion sich so deutlich von der zwischen Alice und Bob verwendeten Übertragungsfunktion unterscheidet, dass es Eve nicht möglich ist, den kryptographischen Schlüssel zu bestimmen. Dieser Mindestabstand beträgt einige Meter bis zu 100m. Grundsätzlich gilt je größer der Abstand, desto sicherer ist das Verfahren.

Falls die direkte Übertragungsfunktion verwendet wird, sind die Übertragungsfunktionen beispielsweise dann zwischen unterschiedlichen Steckdosenpaaren ausreichend unterschiedlich. Diese Unterschiede resultieren aus den verschiedenen Netzbeschaltungen, die sich - von den einzelnen Steckdosen aus gesehen - ergeben. Bei einem isolierten Kabel für eine Punkt-zu-Punkt-Verbindung, bei dem Eve als Angreifer zwischen Alice und Bob eine Verbindung zum Kabel herstellt, bietet sich die Fernnebensprechübertragungsfunktion zur Schlüsselgenerierung an. Bevorzugt sind im Kabelnetzsegment Stichleitungen vorgesehen. An dieser Stelle sei folgendes Begriffliche erläutert. Hierzu sei auch insbesondere die Figur 1 herangezogen. In Figur 1 ist Alice mit dem Buchstaben A, Bob mit dem Buchstaben B und Eve mit dem Buchstaben E bezeichnet.

Die direkte Übertragungsfunktion von Alice zu Eve wird mit H1 und die direkte Übertragungsfunktion von Eve zu Bob wird mit H2 bezeichnet. Die direkte Übertragungsfunktion von Alice zu Bob wird mit H bezeichnet.

Die Fernnebensprechubertragungsf unkt ion von Alice zu Eve wird mit F l und die Fernnebensprechubertragungsf unkt ion von Eve zu Bob wird mit F2 bezeichnet. Die Fernnebensprechübertragungsf unkt ion von Alice zu Bob wird mit F bezeichnet. Sowohl Fl, F2, F , Hl, H2 und H sind frequenzabhängige Funktionen.

Figur 1 zeigt eine Anordnung, mit der die Fernneben–sprechübertragungsf unkt ion zwischen Alice und Bob gemessen werden kann. Hier wird ferner ein Angreifer Eve dargestellt, der zwischen Alice und Bob Zugriff auf die kabelbasierte Kommunikation zwischen Alice und Bob hat. Figur 1 zeigt zwei nebeneinander verlaufende Adernpaare API, AP2 . Sowohl Adernpaar API als auch Adernpaar AP2 weist jeweils zwei Adern oder Leitungen auf. An dieser Stelle sei angemerkt, dass Kabel und Adernpaare, wo technisch sinnvoll, synonym verwendet werden

Bei dem genannten „Man-in-the-Middle-Angrif fs" ist es Eve jedoch eventuell möglich, Teile der Fernnebensprech–übertragungsf unkt ion von Alice zu Eve - auch F l genannt - und von Eve zu Bob - auch F2 genannt- und ebenfalls die direkten Übertragungsfunktion von Alice zu Eve - H l genannt - und von Eve zu Bob - H2 genannt - zu erfassen.

Ein Fachmann könnte nun annehmen, dass die gesamte Fernnebensprechübertragungsf unkt ion von Alice zu Bob gemäß der Gleichung

$$F(j\omega) \approx \hat{F}(j\omega) = F_1(j\omega)H_2(j\omega) + F_2(j\omega)H_1(j\omega) \qquad (1)$$

berechnet werden kann. Hierbei steht j für die komplexe Einheit, ω für die Kreisfrequenz. $\hat{F}$ steht für eine Schätzung oder einen Näherungswert. Diese Annahme könnte aufgrund der Zweiteilung der kabelbasierten Kommunikation gerechtfertigt sein. Die gesamte Fernnebensprech-übertragungsfunktion könnte näherungsweise die Summe aus den beiden Beiträgen sein.

Zum einen wird das Signal direkt von Alice zu Eve übertragen, dies entspricht H1 und von Eve zu Bob ist der Beitrag zur Fernnebensprechübertragungsfunktion gleich F2. Um den Anteil zur Fernnebensprechübertragungsfunktion des ersten Beitrags zu berechnen, muss somit H1 mit F2 multipliziert werden.

Der zweite Beitrag setzt sich entsprechend aus der Fernnebensprechübertragungsfunktion von Alice zu Eve - dies entspricht F1 - und der direkten Übertragungsfunktion von Eve zu Bob - dies entspricht H2 - zusammen.

Der Fachmann könnte ferner annehmen, dass sich die direkte Übertragungsfunktion von Alice zu Bob - H genannt - einfach aus dem Produkt der Teilübertragungsfunktionen H1 und H2 ergibt.

Praktische Messungen zeigen jedoch, dass die beiden obenstehenden Annahmen überraschenderweise nicht korrekt sind. Es wird bestenfalls der Trend teilweise korrekt wiedergegeben, nicht jedoch der komplette und exakte Verlauf. Ausführungsbeispiele hierzu sind in den übrigen Figuren zu sehen.

Bei Verwendung der Fernnebensprechubertragungsf unkt ion liegt die Abweichung zwischen Schätzung und der tatsächlichen Gesamtf ernnebensprechübertragungsf unktion in der Vernachlässigung von Kopplungseffekten über die Schnittstelle, d.h. an der Position von Eve, hinaus. Bei Net zSegmenten und Zugang über Steckdosen, liegt die Abweichung an der teilweisen Nutzung verschiedener Kabel oder an den unterschiedlichen Netzstrukturen wie z.B. Stichleitungen mit oder ohne Verbraucher, die an den verschiedenen Steckdosen anzutreffen sind.

Die „Übertragungsfunktion" kann insbesondere eine einheitenlose, komplexwert ige Funktion oder komplexwert iger Wert sein, welche oder welcher in der Regel frequenzabhängig ist, jedoch auch noch von weiteren Größen abhängig sein kann. Die Übertragungsfunktion ist definiert als das Verhältnis der komplexen Ausgangsspannung zur komplexen Eingangsspannung.

Eine „aus der gemessenen Übertragungsfunktion abgeleiteten Größe" ist beispielsweise ein komplexer Wert welcher anhand der Übertragungsfunktion ermittelt wird. So können beispielsweise beim Messen der Übertragungsfunktion an einigen Frequenzen Werteeinbrüche oder lokale Wertemaxima entstehen, welche wiederum Basis für das Bitmuster dienen.

Für den Fall, dass die Übertragungsfunktion zwischen dem ersten und dem zweiten Benutzer symmetrisch ist, ist es bevorzugt, dass die Übertragungsfunktion zwischen dem ersten und dem zweiten Benutzer durch den ersten oder den zweiten Benutzer gemessen wird.

Quantisieren ist insbesondere eine klassische Technik der Signalverarbeitung, bei der die Werte einer gegebenen Funktion bestimmten, nichtkontinuierlichen, also quantisierten, Werten derselben Funktion zugeordnet werden. Diese Technik kann insbesondere zur Datenkompression verwendet werden. Falls die Quantisierung als Funktion eine skalare Funktion verwendet, spricht man insbesondere von einer skalaren Quantisierung. Falls die Quantisierung als Funktion vektorwertige Funktionen verwendet, handelt es sich um eine Vektorquantisierung.

Eine Vektorquantisierung kann insbesondere zwei Schritte aufweisen. Im ersten Schritt, dem sogenannten Training, wird die Tabelle, welche auch Codebuch genannt wird, mit häufig vorkommenden Merkmalsvektoren erstellt. Im zweiten Schritt wird für weitere Vektoren jeweils der Codebuchvektor mit dem geringsten Abstand bestimmt. Durch diese Quantisierung der z.B. zweidimensionalen Vektoren ergeben sich, falls die Übertragungsfunktion als zweidimensionale Funktion des Real- und Imaginärteils oder dargestellt wird, sogenannten Voronoi-Regionen, welche in einem Voronoi-Diagramm darstellbar sind.

Nach dem Quantisieren der Übertragungsfunktion weist die quantisierte Übertragungsfunktion lediglich quantisierte Werte als Funktionswerte auf.

Den quantisieren Werten wird ein Bitmuster zugeordnet. Falls Voronoi-Regionen verwendet werden, werden bevorzugt den Voronoi-Regionen Bitmuster zugeordnet.

Die Kabel können bevorzugt in ihren Eigenschaften durch zusätzliche Maßnahmen verändert werden, z.B. durch

veränderliche Stichleitungen oder veränderlichen Kopplungsfunktionen, zusätzlich zu Änderungen, die sich durch An-/Abschalten von Verbrauchern in Stromnetz ergeben. Damit können neue unabhängige Bitmuster erzeugt werden, die dann zur Bildung eines Schlüssels zusammengefügt werden. Somit kann die zu messende Übertragungsfunktion zufallsbasiert aktiv verändert werden. Dies ist beispielsweise auch durch einstellbar veränderliche Abschlusswiderstände realisierbar, welchen per Zufallsgenerator ein Abschlusswiderstandswert aufgeprägt wird. Die Übertragungsfunktion ändert sich insbesondere dadurch, dass sich die physikalischen Eigenschaften des Kabels ändern.

Einfache stark vereinfachte Realisierung der Erfindung erfolgt somit wie folgt. Alice sendet Bob ein Sinussignal mit veränderlicher Frequenz. Die Parameter dieser Funktion seien Bob bekannt. Nun misst Bob (vereinfacht) die Übertragungsfunktion für eine bestimmte Frequenz und ermittelt einen zugehörigen komplexen Übertragungsf unkt ionswert . Dieser Übertragungsf unkt ionswert wird in einer komplexen Ebene mit 4 Quadranten (z.B. durch Koordinatenachsen getrennt) eingefügt. Jeder Quadrant entspricht einem Bitmuster. Somit sei der erste Quadrant 00, der zweite Quadrant 01, der dritte Quadrant 10 und der letzte Quadrant 11. Liegt nun der komplexe Übertragungsf unkt ionswert im dritten Quadranten lautet der kryptographische Teilschlüssel (binär) 10, entsprechend der Bezeichnung des dritten Quadranten. Dies kann nun für weitere (vorher abgesprochene) Frequenzen erfolgen, wobei durch ein Aneinanderreihen der kryptographische

Teilschlüssel der kryptographische (Gesamt-)Schlüssel erzeugt wird.

Gemäß einer Ausführungsform ist die Übertragungsfunktion eine direkte Übertragungsfunktion oder eine Fernnebensprechübertragungsf unkt ion . Das Fernnebensprechen wird auch Fernübersprechen genannt. Die Fernnebensprech–übertragungsf unkt ion wird auch FEXT-Übertragungsf unkt ion genannt, wobei FEXT für Far-End Crosstalk steht. Der Vorteil der Benutzung der direkten Übertragungsfunktion ist, dass diese sehr einfach gemessen werden kann. Der Vorteil der Benutzung der Fernnebensprechübertragungsf unkt ion ist, dass es ein Dritter, der die beiden Benutzer abhören will, in diesem Fall wesentlich schwerer hat, die Fernneben–sprechübertragungsf unkt ion zu schätzen oder zu ermitteln.

Für den Fall, dass die Übertragungsfunktion zwischen dem ersten und dem zweiten Benutzer asymmetrisch, insbesondere nicht perfekt symmetrisch, ist, ist es gemäß einer Ausführungsform vorgesehen, dass die Übertragungsfunktion zwischen dem ersten und dem zweiten Benutzer durch den ersten und den zweiten Benutzer gemessen wird. Falls nun jeder Benutzer gemäß dem oben beschriebenen Verfahren jeweils einen Schlüssel erzeugt, so kann es vorkommen, dass die beiden erhaltenen Schlüssel nicht vollkommen identisch sind. Für diesen Fall können die Abweichungen zwischen den beiden Schlüsseln durch sogenannte Key-Reconciliat ion-Verfahren vermieden oder korrigiert werden.

Falls nur bestimmte Übertragungsfunktionen die nötige annähernde Symmetrie ausweisen, z.B. nur die direkte

Übertragungsfunktion, ist es bevorzugt, die besser symmetrische Übertragungsfunktion zu benutzen. -

Asymmetrien und Schlüsselabweichungen können von nicht-idealen Eigenschaften der Bauteile oder unkorreliertem Rauschen bei Alice und Bob herrühren. Als Key-Reconciliation-Verfahren kommen beispielsweise Schutzintervalle bei der Vektorquantisierung oder Code-basierte Verfahren, z.B. das Slepian-Wolf Coding in Frage. Diese Verfahren sind z.B. in den folgenden Veröffentlichungen beschrieben:

[1] Islam, N., Graur, O., Henkel, W., Filip, A.: LDPC Code Design Aspects for Physical-Layer Key Reconciliation, IEEE International Global Communications Conference, San Diego, California, 2015

[2] Filip, A., Henkel, W.: Variable Guard Band Construction to Support Key Reconciliation, IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2014), Florence, Italy, 2014

[3] Filip, A., Mehmood, R., Wallace, J., Henkel, W.: Physical-Layer Key Generation Supported by RECAP Antenna Structures, 9th International ITG Conference on Source and Channel Coding (SCC), Munich, Germany, 2013

[4] Etesami, J., Henkel, W.: LDPC Code Construction for Wireless Physical-Layer Key Reconciliation, First IEEE International Conference on Communications in China (ICCC 12), Beijing, China, 2012

Gemäß einer Ausführungsform weist der Informationskanal mindestens ein Kabel auf, in dem zwei Adernpaare verlaufen. Mit dieser Ausführungsform können sowohl die direkte Übertragungsfunktion als auch die Fernnebensprechübertragungsfunktion gemessen werden. Im Falle der Benutzung der Fernnebensprechübertragungsfunktion wird eine erhöhte Sicherheit gegenüber Abhörangriffen Dritter erzielt.

Gemäß einer weiteren Ausführungsform weist der Informationskanal mindestens ein Dreileiterkabel auf. Das Dreileitersystem kann so wie ein Doppeladerpaar verwendet werden. Hierzu wird die erste und die zweite Ader als das erste Paar und die zweite und die dritte Ader als das zweite Paar verwendet.

Um vorteilhafterweise auch mehrdimensionale Funktionen quantisieren zu können, ist die Quantisierung eine Vektorquantisierung. Im Fall von skalaren Funktionen kann eine skalare Quantisierung verwendet werden.

Gemäß einer Ausführungsform wird die Vektorquantisierung auf eine Größe angewendet, welche durch Real- und Imaginärteil oder Betrag und Phase charakterisiert ist. Eine komplexe Größe kann durch den Real- und Imaginärteil oder den Betrag und die dazugehörige Phase vollständig beschrieben werden. Eine zweidimensionale Vektorgröße kann ebenfalls durch Betrag und die dazugehörige Phase vollständig beschrieben werden.

Um vorteilhafterweise eine Mindestkonfiguration zu erreichen, wird die Übertragungsfunktion bei mindestens einer Frequenz verwendet.

Gemäß einer weiteren Ausführungsform wird die Übertragungsfunktion bei einer Vielzahl von Frequenzen verwendet. Dies hat den Vorteil, dass eine Vielzahl von Bitmustern zur Schlüsselerzeugung benutzt werden können. Ferner kann die Information, welche Frequenzen benutzt werden, auch einen möglichen Angriff von einem Dritten abwehren, wenn der Dritte nicht weiß, welche Frequenzen zur Schlüsselerzeugung benutzt werden.

Um vorteilhafterweise standardisierte Modulationsverfahren zur Datenübertragung verwenden zu können, ist die oben genannten mindestens eine Frequenz eine Frequenz eines Mehrträger Systems , insbesondere ein Orthogonales Frequenzmultiplexverfahren OFDM (engl. Orthogonal Frequency-Division Mult iplexing) oder Discrete Multitone Transmission (DMT) .

Gemäß einer Ausführungsform wird die Übertragungsfunktion in einer Zeitbasis, einer Frequenzbasis oder einer anderen geeigneten Basis dargestellt und die Quantisierung erfolgt in dieser Darstellung. Durch eine geeignete Transformation der Übertragungsfunktion geeignete Basis, die das System in einer einfachen Form beschreibt, kann erreicht werden, dass sich das Quantisieren einfach berechnen lässt.

In einer anderen Ausführungsform können auch Frequenzen von lokalen Minima oder lokalen Maxima der Übertragungsfunktion oder entsprechend der FEXT-Übertragungsf unkt ion zur Schlüsselgenerierung herangezogen werden.

Weiterhin kann die Aufgabe gelöst werden durch einen Rechner, welcher derart eingerichtet ist, dass ein zuvor beschriebenes Verfahren durchführbar ist.

Damit kann vorteilhafterweise erreicht werden, dass das zuvor beschriebene Verfahren auf einen Rechner oder Computer ausgeführt wird.

Im Weiteren wird die Erfindung anhand von Ausführungsbeispielen näher erläutert. Es zeigen

Figur 2 zeigt die Amplitude $|F|$ der gesamten Fernnebensprechübertragungsfunktion zwischen den beiden kommunizierenden Benutzern Alice und Bob im Vergleich zur Amplitude des Berechnungsergebnisses $|\hat{F}|$, das dem Dritten, auch Eve genannt, bestenfalls zur Verfügung stände, in Abhängigkeit der Frequenz .

Figur 3 zeigt eine schematische Darstellung eines Energieversorgungskabels mit drei Adern.

Figur 4 zeigt Messungen von direkten Übertragungsfunktionen zwischen Alice und Bob und Alice und Eve für ein in Figur 3 dargestelltes Energieversorgungskabel, an dem Steckdosen mit noch nicht perfekt gestalteten Endeinrichtungen angeschlossen sind. Figur 4 zeigt ebenso die jeweiligen entgegengesetzten Messungen zwischen Bob und Alice und Eve und Alice, wobei geringe Abweichungen zwischen den entgegengesetzten Messungen auf die nichtperfekten Eigenschaften der Messeinrichtung zurückzuführen sind.

Figur 5 zeigt den Betrag der Fernnebensprech-übertragungsfunktionen, die in einem Dreiadersystem innerhalb eines fünfadrigen Kabels zwischen Alice und Bob gemessen wurden.

Figur 2 zeigt die Amplitude \F\ der gesamten Fernnebensprechubertragungsf unkt ion zwischen den beiden kommunizierenden Benutzern Alice und Bob im Vergleich zur Amplitude des Berechnungsergebnisses $|\hat{F}|$, das dem Dritten, auch Eve genannt, bestenfalls zur Verfügung stände, in Abhängigkeit der Frequenz. In Figur 2 sind ebenfalls die beiden Amplituden \F\ und $|\hat{F}|$ für die Übertragung von Bob zu Alice dargestellt. Diese sind jedoch kaum unterscheidbar von der Übertragung von Alice zu Bob.

Für diesen Fall belegt dies, dass der Angreifer Eve nicht in der Lage ist, die Fernnebensprechübertragungsf unkt ion zu rekonstruieren. Somit ist er auch nicht in der Lage, den einen korrekten kryptographischen Schlüssel zu erhalten.

Figur 3 zeigt eine schematische Darstellung eines Energieversorgungskabels mit drei Adern. Die drei Adern weisen den Leiter L, den Nullleiter N und den Schutzleiter PE auf. Bei Anwendung in Energieversorgungskabeln stehen oft keine zwei getrennten Doppeladern zur Verfügung. Die Fernnebensprechübertragungsf unkt ion kann hierbei gemäß Figur 3 zwischen den Paaren L-N und N-PE oder vergleichbaren Paarungen gemessen werden. Hierzu kommt, dass Eve ü nur zu anderen Steckdosen im Netzsegment Zugang hat. Damit ist eine Rückberechnung oder auch nur Schätzung der Übertragungsfunktion ausgeschlossen.

Bei Verwendung der Übertragungsfunktion und gleichzeitigem Einsatz von Bit-Loading würde jedoch die Übertragungsfunktion indirekt zu einem gewissen Maße durch Mitteilung der Bit-Belegung kommuniziert, was dann näherungsweise Rückschlüsse auf die Übertragungsfunktion

zuließe. Allerdings geht in das Bit-Loading auch das Rauschen auf beiden Seiten ein, was in die Schlüsselgenerierung nicht einbezogen würde, bestenfalls als Störung, deren Einfluss durch Key-Reconciliation reduziert wird.

Bei Telefonleitungen oder Datenkabeln wäre die Schätzung der Übertragungsfunktion möglich, insbesondere, wenn keine zusätzlichen Abgänge, sogenannte Bridge Taps, vorhanden sind, was in Europa üblicherweise nicht der Fall ist. Fernnebensprechübertragungsfunktion bieten sich dann besonders an, da sie keine solche Möglichkeit der Schätzung bieten .

Figur 4 zeigt Messungen von direkten Übertragungsfunktionen zwischen Alice und Bob und Alice und Eve für ein in Figur 3 dargestellte Energieversorgungskabelverbindung, an dem Steckdosen mit noch nicht perfekt gestalteten Endeinrichtungen beschaltet sind. Figur 4 zeigt ebenso die jeweiligen entgegengesetzten Messungen zwischen Bob und Alice und Eve und Alice, wobei geringe Abweichungen zwischen den entgegengesetzten Messungen auf die nichtperfekten Eigenschaften der verwendeten Messeinrichtung zurückzuführen sind.

Diese Messung zeigt, dass ein Angreifer praktisch trotz Zugang zum Kabel oder anderen Steckdosen im Falle von Energienetzen eine direkte Übertragungsfunktion nicht exakt rekonstruieren kann.

Figur 5 zeigt den Betrag der Fernnebensprechübertragungsfunktionen, die in einem Dreiadersystem innerhalb eines fünfadrigen Kabels zwischen Alice und Bob

gemessen wurden. Da die Messungen in beide Richtungen völlig überlappend sind, wurde eine Kurve gestrichelt dargestellt, um die zweit Kurve dahinter sichtbar zu machen.

Hieran erkennt man, dass Kopplungsfunktionen bei Energiekabeln deutlich stärker als bei symmetrischen Telefonleitungen oder Datenkabeln sind. Energieverbraucher führen allerdings auch zu stärkeren Störungen, die bei der Quantisierung durch geeignete Key-Reconciliation zu berücksichtigen sind. Ein Wechsel von Verbrauchern führt zu wechselnden Abschlüssen und damit zu Änderungen in den Übertragungsfunktionen, was neue Schlüsselzuweisungen zur Folge hat.

Zum Erzeugen eines kryptographischen Schlüssels sowohl für den ersten Benutzer Alice als auch für den zweiten Benutzer Bob kann gemäß einem Ausführungsbeispiel wie folgt vorgegangen werden.

Alice und Bob sind durch zwei Adernpaare API, AP2 verbunden. An einer Stelle zwischen Alice und Bob hat ein Dritter Zugriff auf das Hierbei wird ein passiver „Man-in-the-Middle-Angrif f" angenommen, d.h. Eve kann alle zwischen Alice und Bob ausgetauschten Signale an dieser Stelle abhören.

Die kabelbasierte Kommunikation zwischen Alice und Bob verwendet in diesem Ausführungsbeispiel vier unterschiedliche Frequenzen.

Für diese vier unterschiedlichen Frequenzen wird die Übertragungsfunktion zwischen Alice und Bob gemessen.

Die hier verwendete Übertragungsfunktion ist die FEXT-Übertragungsf unkt ion . Diese wird jeweils für die vier verwendeten Frequenzen zwischen Alice und Bob gemessen. Hierzu wird eine Funktion in das erste Adernpaar API bei Alice eingespeist und an dem zweiten Adernpaar AP2 bei Bob gemessen. Die gemessenen FEXT- Übertragungsfunktion ist eine komplexwert ige Funktion.

Daraufhin werden die gemessenen Übertragungsfunktionen jeweils für die vier unterschiedlichen Frequenzen quantisiert. Vorliegend wird für jede Frequenz eine einer Vektorquantisierung der FEXT-Übertragungsf unkt ion durch–geführt .

Hierzu wird in einem ersten Schritt, dem sogenannten Training, eine Tabelle, auch Codebuch genannt, mit häufig vorkommenden Merkmalsvektoren erstellt. Im zweiten Schritt wird für weitere Vektoren jeweils der Codebuchvektor mit dem geringsten Abstand bestimmt. Durch diese Quantisierung ergeben sich für jede der vier Frequenzen unterschiedliche Voronoi-Regionen, welche jeweils in einem Voronoi-Diagramm darstellbar sind.

Jeder Voronoi-Region wird ein Bitmuster zugewiesen.

Im letzten Schritt der kryptographische Schlüssel aus den Bitmustern gebildet.

Patentansprüche

1. Verfahren zum Erzeugen eines kryptographischen Schlüssels für eine elektronische, kabelbasierte Kommunikation für einen ersten Benutzer als auch einen zweiten Benutzer,
wobei das Verfahren folgende Schritte aufweist:
- Messen einer Übertragungsfunktion oder Bestimmen einer aus der gemessenen Übertragungsfunktion abgeleiteten Größe zwischen dem ersten und dem zweiten Benutzer durch den ersten oder den zweiten Benutzer,
- Quantisieren der Übertragungsfunktion oder der daraus abgeleiteten Größe, sodass quantisierte Werte der Übertragungsfunktion oder der abgeleiteten Größe vorliegen, und
- Zuweisen eines Bitmusters zu den quantisierten Werten der Übertragungsfunktion oder der abgeleiteten Größe, wobei das Bitmuster zumindest einen Teil des kryptographischen Schlüssels bildet.

2. Verfahren gemäß Anspruch 1, dadurch gekennzeichnet, dass die Übertragungsfunktion eine direkte Übertragungsfunktion oder eine Fernnebensprechübertragungsfunktion ist.

3. Verfahren gemäß Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Übertragungsfunktion zwischen dem ersten und dem zweiten Benutzer sowohl durch den ersten als auch durch den zweiten Benutzer gemessen wird.

4. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass die Übertragungsfunktion zufallsbasiert aktiv verändert wird.

5. Verfahren einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die kabelbasierte Kommunikation wenigstens mittels eines Kabels erfolgt, welches mindestens ein Adernpaar, insbesondere mindestens zwei Adernpaare, aufweist.

6. Verfahren einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die kabelbasierte Kommunikation mindestens ein Dreileiterkabel verwendet.

7. Verfahren gemäß einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Quantisierung eine skalare Quantisierung oder eine Vektorquantisierung ist.

8. Verfahren gemäß Anspruch 7, dadurch gekennzeichnet, dass die Vektorquantisierung auf eine Größe angewendet wird, welche durch Real- und Imaginärteil oder Betrag und Phase charakterisiert ist.

9. Verfahren gemäß einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Übertragungsfunktion oder die Fernnebensprechübertragungsf unkt ion bei mindestens einer Frequenz verwendet wird.

10. Verfahren gemäß Anspruch 8, dadurch gekennzeichnet, dass die mindestens eine Frequenz eine Frequenz eines Mehrträger Systems, insbesondere OFDM oder DMT, ist.

11. Verfahren gemäß einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Übertragungsfunktion in einer Zeitbasis, einer Frequenzbasis oder einer anderen geeigneten Basis dargestellt wird und die Quantisierung in dieser Darstellung erfolgt.

12. Verfahren gemäß einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die aus der gemessenen Übertragungsf unt ion abgeleiteten Größe die Frequenzen von lokalen Minima oder lokalen Maxima der Übertragungsfunktion umfassen.

13. Rechner, welcher derart eingerichtet ist, dass ein Verfahren gemäß einem der Ansprüche 1 bis 12 durchführbar ist.

Figuren

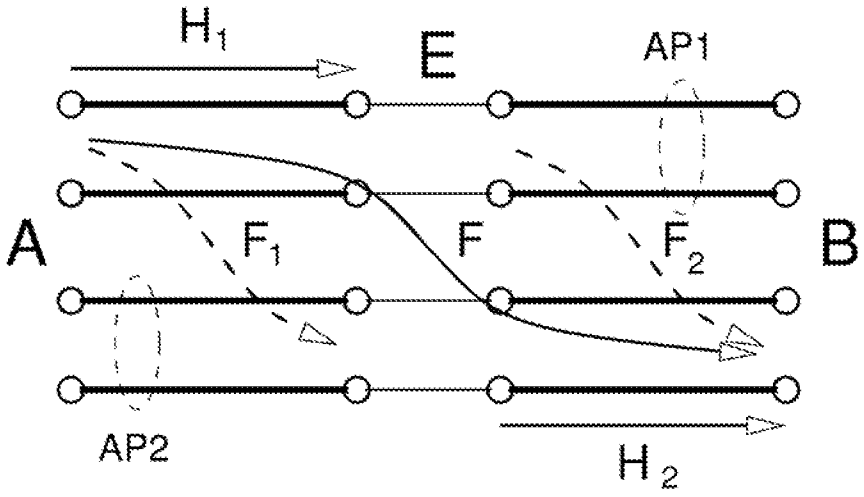

Fig. 1

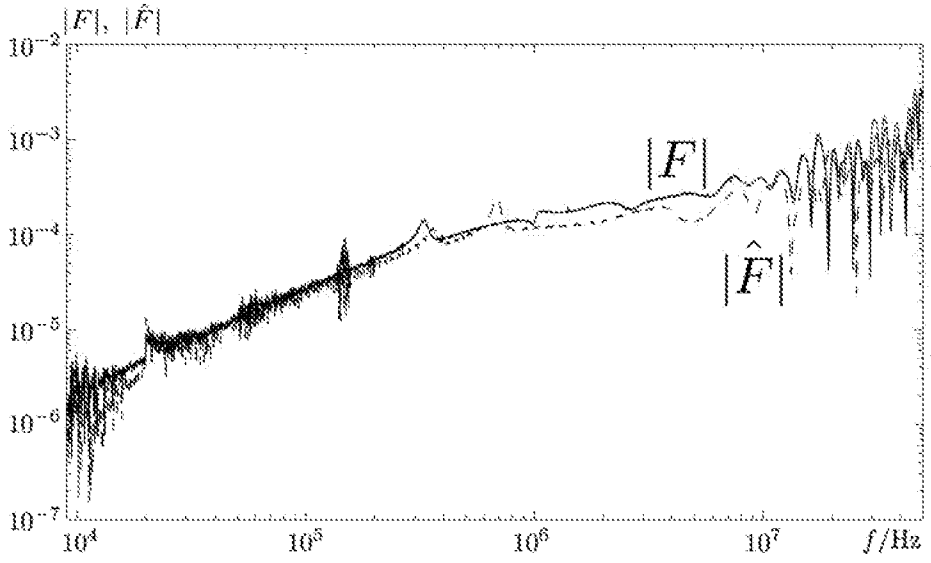

Fig. 2

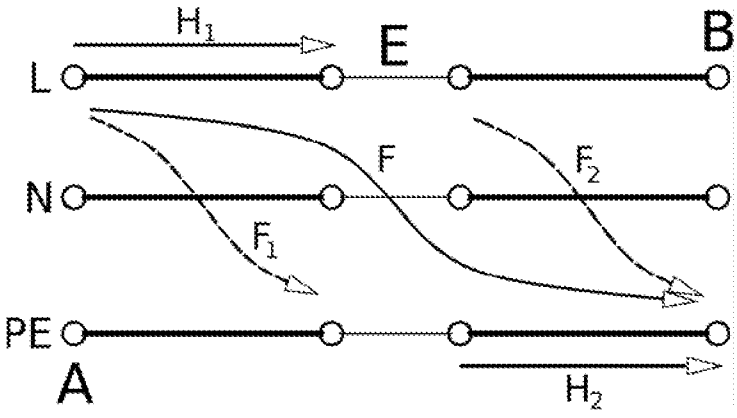

Fig. 3

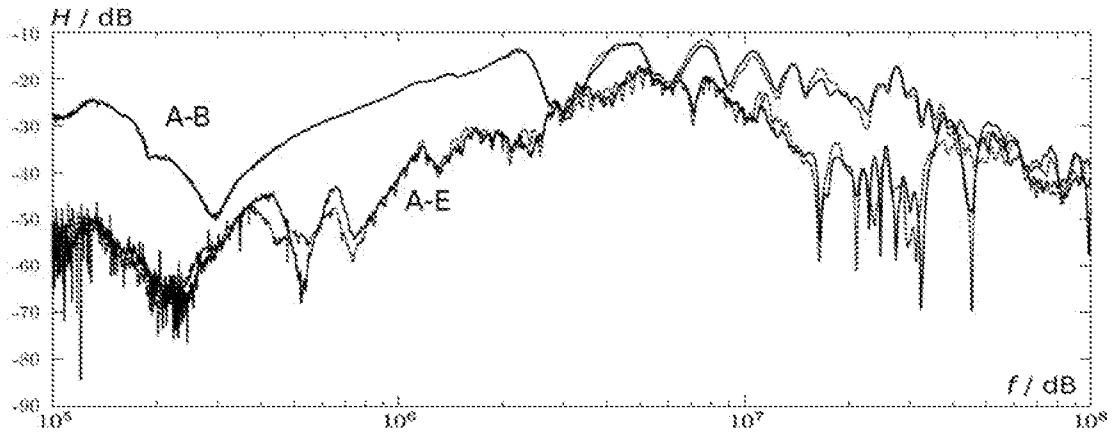

Fig. 4

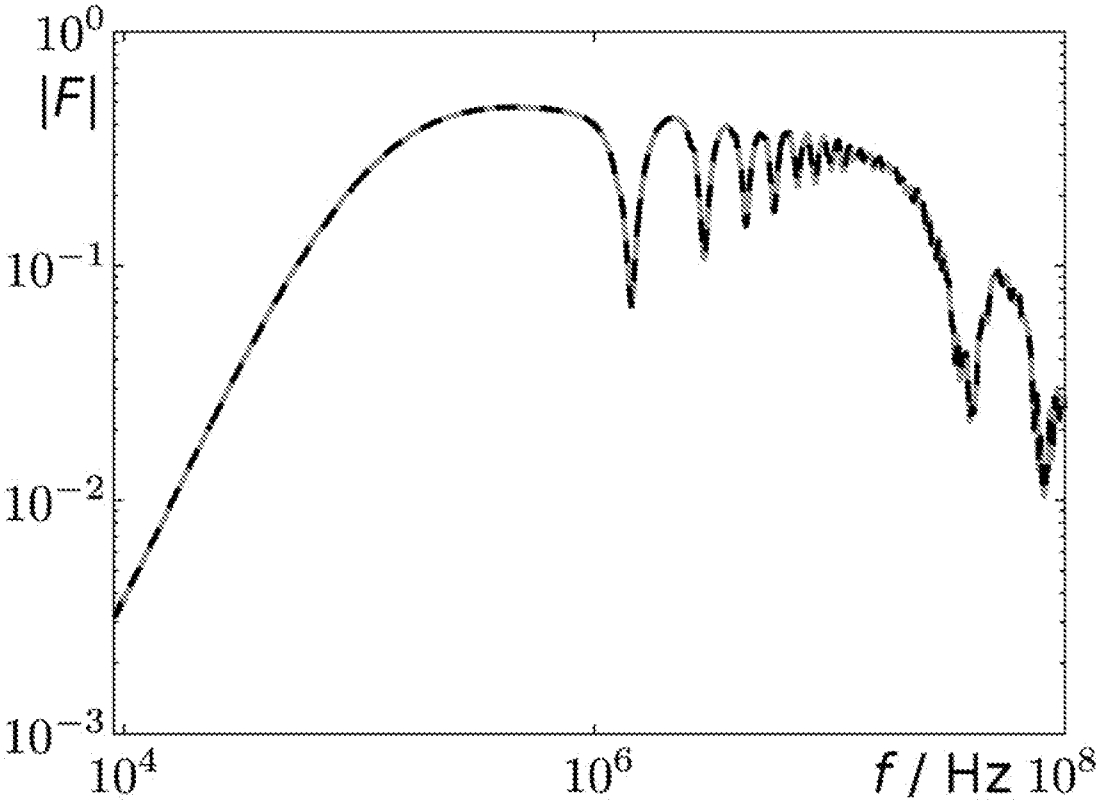

Fig. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/DE2016/100338

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08 H04L29/06
ADD.

According to International Patent Classification (IPC) orto both national Classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (Classification System followed by Classification Symbols)
H04L G06F

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, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to Claim No.
X	US 2011/087897 AI (NELSON PATRICK A [US] ET AL) 14 Apri l 2011 (2011-04-14) abstract paragraphs [0001] - [0017] , [0034] - [0083] f i gures la-3c -----	1-13
X	MAS0UD GHOREISHI MADISEH ET AL: "Secret Key Generati on wi thi n Peer-to-Peer Network Overl ays" , P2P, PARALLEL, GRID, CL0UD AND INTERNET COMPUTING (3PGCIC) , 2012 SEVENTH INTERNATIONAL CONFERENCE 0N, I EEE, 12 November 2012 (2012-11-12) , pages 156-163 , XP032274954, D0I : 10. 1109/3PGCIC.2012 .62 ISBN : 978-1-4673-2991-0 the whol e document ----- -/- ·	1-13

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

X I 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" documentwhich may throw doubts on priority claim(s) orwhich 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 ortheory underlying the invention

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 November 2016	01/12/2016

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

2

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to Claim No.
A	FI LI P ALEXANDRA ET AL: "Vari abl e guard band constructi on t o support key reconci 1i ati on" , 2014 I EEE INTERNATIONAL CONFERENCE 0 N ACOUSTICS, SPEECH AND SIGNAL PROCESSING (ICASSP) , I EEE, 4 May 2014 (2014-05-04) , pages 8173-8177 , XP032618026, D0I : 10. 1109/ICASSP. 2014. 6855194 [retri eved on 2014-07-11] the whol e document -----	1-13

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/DE2016/100338

Patent document cited in search report	Publioation date	Patent family member(s)	Publioation date
US 2011087897 AI	14-04-2011	CA 2777363 AI	21-04-2011
		EP 2488988 A2	22-08-2012
		US 2011087897 AI	14-04-2011
		US 2012198244 AI	02-08-2012
		WO 2011046817 A2	21-04-2011

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE2016/100338

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

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

B. RECHERCHIERTE GEBIETE

Recherchierter MindestprUfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L G06F

Recherchierte, aber nicht zum MindestprUfstoff 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, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2011/087897 AI (NELSON PATRICK A [US] ET AL) 14. Apri l 2011 (2011-04-14) Zusammenfassung Absätze [0001] - [0017] , [0034] - [0083] Abbi l dungen la-3c -----	1-13
X	MAS0UD GHOREISHI MADISEH ET AL: "Secret Key Generati on wi thi n Peer-to-Peer Network Overl ays" , P2P, PARALLEL, GRID, CL0UD AND INTERNET COMPUTING (3PGCIC) , 2012 SEVENTH INTERNATIONAL CONFERENCE 0N, I EEE, 12. November 2012 (2012-11-12) , Sei ten 156-163 , XP032274954, D0I : 10. 1109/3PGCIC.2012 .62 ISBN : 978-1-4673-2991-0 das ganze Dokument ----- -/- ·	1-13

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

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" 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 er¬scheinen 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	Absendedatum des internationalen Recherchenberichts
23. November 2016	01/12/2016

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

2

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	FI LI P ALEXANDRA ET AL: "Vari abl e guard band constructi on t o support key reconci 1i ati on" , 2014 I EEE INTERNATIONAL CONFERENCE 0 N ACOUSTICS, SPEECH AND SIGNAL PROCESSING (ICASSP) , I EEE, 4 . Mai 2014 (2014-05-04) , Sei ten 8173-8177 , XP032618026, D0I : 10. 1109/ICASSP. 2014. 6855194 [gefunden am 2014-07-11] das ganze Dokument -----	1-13

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE2016/100338

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2011087897 A1	14-04-2011	CA 2777363 A1	21-04-2011
		EP 2488988 A2	22-08-2012
		US 2011087897 A1	14-04-2011
		US 2012198244 A1	02-08-2012
		WO 2011046817 A2	21-04-2011