(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
10. September 2020 (10.09.2020)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2020/177806 A1

(51) Internationale Patentklassifikation:
H04L 9/30 (2006.01) *H04L 9/08* (2006.01)

(21) Internationales Aktenzeichen: PCT/DE2020/100063

(22) Internationales Anmeldedatum:
31. Januar 2020 (31.01.2020)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2019 105 297.1
01. März 2019 (01.03.2019) DE

(71) Anmelder: **BAYERISCHE MOTOREN WERKE AKTIENGESELLSCHAFT** [DE/DE]; Petuelring 130, 80809 München (DE).

(72) Erfinder: **WAGENHUBER, Josef**; Riederner Äcker 10 a, 85302 Gerolsbach (DE). **HOFMANN, Sven**; Therese-Studer-Strasse 23, 80797 München (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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:** CONTROL OF A MOTOR VEHICLE

(54) **Bezeichnung:** STEUERUNG EINES KRAFTFAHRZEUGS

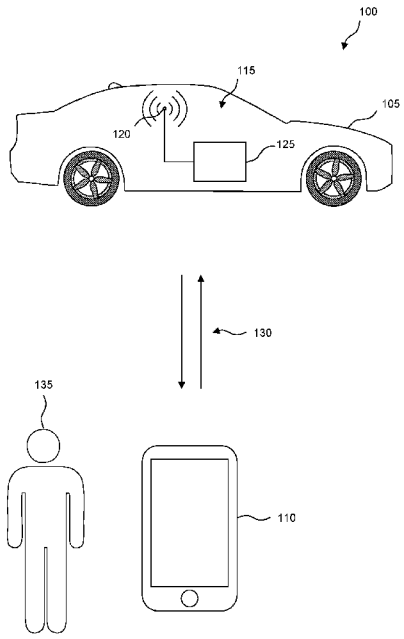


Fig. 1

(57) **Abstract:** A motor vehicle stores a first one-way hash x of a password p and an encrypted value V from the second one-way hash y of the password p. A method for authenticating a device with respect to the vehicle comprises the steps: a PACE procedure is carried out so that the device and the motor vehicle determine the same session key; the motor vehicle generates a communication key on the basis of the session key and the encrypted one-way hash V; and the device generates the communication key on the basis of the session key and the second one-way hash y.

(57) **Zusammenfassung:** Seitens eines Kraftfahrzeugs sind ein erster Einweg-Hash x eines Passworts p, und ein verschlüsselter Wert V aus dem zweiten Einweg-Hash y des Passworts p abgelegt. Ein Verfahren zum Authentifizieren eines Geräts gegenüber dem Kraftfahrzeug, umfasst Schritte des Durchführens eines PACE-Verfahrens, um seitens des Geräts und des Kraftfahrzeugs den gleichen Sitzungsschlüssel zu bestimmen; des Erzeugens eines Kommunikationsschlüssels seitens des Kraftfahrzeugs auf der Basis des Sitzungsschlüssels und des verschlüsselten Einweg-Hashs V; und des Erzeugens des Kommunikationsschlüssels seitens des Geräts auf der Basis des Sitzungsschlüssels und des zweiten Einweg-Hashs y.

WO 2020/177806 A1

Steuerung eines Kraftfahrzeugs

Die Erfindung betrifft eine verschlüsselte Kommunikation zwischen einem Gerät und einer Vorrichtung. Dabei befindet sich die Vorrichtung insbesondere an Bord eines Kraftfahrzeugs.

Zur Herstellung einer verschlüsselten Kommunikationsverbindung zwischen einem ersten und einem zweiten Kommunikationspartner sind unterschiedliche Verfahren bekannt, von denen einige auch eine Authentifizierung des ersten Partners gegenüber dem zweiten unterstützen. Hierbei kann zumindest der zweite Partner die Identität des ersten verifizieren, sodass die Verbindung nicht mit beliebigen, sondern mit ausgewählten Partnern hergestellt werden kann.

Hierzu muss üblicherweise seitens des ersten Partners eine Information vorliegen, die den zweiten Partner kennzeichnet. Ein solches Verfahren ist als PACE bekannt und kann beispielsweise verwendet werden, um eine gesicherte Kommunikation zwischen einem in einem Personalausweis angebrachten RFID und einem entfernten Rechner zu etablieren.

Solche Verfahren sind zum Einsatz an Bord eines Kraftfahrzeugs jedoch nur bedingt geeignet. Anders als der entfernte Rechner ist ein physischer Zugang zu einer an Bord eines Kraftfahrzeugs angebrachten Vorrichtung relativ leicht zu erhalten. Die Kommunikation kann abgehört werden oder die Vorrichtung kann manipuliert oder analysiert werden. Ein in der Vorrichtung hinterlegter Hinweis auf einen Kommunikationspartner kann zur Nachbildung der Identität oder eines Kommunikationsschlüssels des zweiten Partners verwendet werden.

Eine der Erfindung zu Grunde liegende Aufgabe besteht darin, ein verbessertes Verfahren zum Authentifizieren eines Geräts gegenüber einem Kraftfahrzeug anzugeben. Die Erfindung löst die Aufgabe mittels der Gegenstände der unabhängigen Ansprüche. Unteransprüche geben bevorzugte Ausführungsformen wieder.

Seitens eines Kraftfahrzeugs sind ein erster Einweg-Hash x eines Passworts p, und ein verschlüsselter Wert V aus dem zweiten Einweg-Hash y des Passworts p abgelegt.

Nach einem ersten Aspekt der Erfindung umfasst ein Verfahren zum Authentifizieren eines Geräts gegenüber dem Kraftfahrzeug Schritte des Durchführens eines PACE-Verfahrens, um seitens des Geräts und des Kraftfahrzeugs den gleichen Sitzungsschlüssel zu bestimmen; des Erzeugens eines Kommunikationsschlüssels seitens des Kraftfahrzeugs auf der Basis des Sitzungsschlüssels und des verschlüsselten Einweg-Hashs V; und des Erzeugens des Kommunikationsschlüssels seitens des Geräts auf der Basis des Sitzungsschlüssels und des zweiten Einweg-Hashs y.

Durch die beschriebene Bestimmung des Sitzungsschlüssels kann das zur Familie symmetrischen der PAKE (Password Authenticated Key Exchange) Verfahren zählende PACE zu einem asymmetrischen PAKE verbessert (augmented) werden. Das erweiterte Verfahren wird hierin auch PACE+ genannt.

Mittels des PACE+ Verfahrens kann eine sichere Kommunikation zwischen dem Gerät und dem Kraftfahrzeug etabliert werden. Dabei können Informationen, die seitens des Kraftfahrzeugs zur Identifikation des Geräts abgelegt sind, so gestaltet, dass aus ihnen das empfängerseitig verwendete Passwort nicht abgeleitet werden kann. Das Hinterlegen von kryptographischen Informationen seitens des Kraftfahrzeugs wird auch Provisionieren genannt. Ein Diebstahl der Informationen nach dem Provisionieren durch einen Angreifer kann ungefährlich sein.

Auf der Basis des bestimmten Sitzungsschlüssels kann ein beliebiger Austausch von Informationen erfolgen. Beispielsweise kann das Kraftfahrzeug über ausgetauschte Informationen gesteuert werden. Insbesondere können ein Schließsystem oder eine Wegfahrsperre auf diese Weise deaktiviert werden.

Bevorzugt ist der zweite Einweg-Hash y des Passworts bezüglich eines vorbestimmten Basispunkts eines Verschlüsselungssystems verschlüsselt. Der Basispunkt kann beispielsweise seitens des Geräts gewählt sein.

Das Gerät kann mit dem Kraftfahrzeug verknüpft werden, falls eine verschlüsselte Kommunikation auf der Basis des Kommunikationsschlüssels möglich ist. Im Folgenden können praktisch beliebige Informationen zwischen

dem Gerät und der Vorrichtung an Bord des Kraftfahrzeugs ausgetauscht werden.

Weiter bevorzugt wird eine Verschlüsselung auf der Basis elliptischer Kurven durchgeführt wird. Dies kann sowohl das PACE-Verfahren als auch die Bestimmung von V im Rahmen des Provisionierens betreffen.

Es ist weiter bevorzugt, dass das Gerät ein mobiles Gerät umfasst. Das Gerät kann insbesondere einem Benutzer zugeordnet sein, dem die Nutzung einer vorbestimmten Funktion des Kraftfahrzeugs erlaubt ist. Durch das Austauschen von Informationen über die geschilderte Kommunikationsverbindung kann der Benutzer authentifiziert sein, sodass die Funktion ermöglicht werden kann. Die Funktion kann insbesondere einen üblichen Betrieb bzw. eine Verwendung des Kraftfahrzeugs umfassen.

Es ist weiterhin bevorzugt, dass das Gerät ein einem vorbestimmten Benutzer zugeordnetes persönliches Gerät umfasst. Das Gerät kann insbesondere ein Mobiltelefon (Smartphone) umfassen, das üblicherweise nur durch den Benutzer verwendet wird.

Nach einem weiteren Aspekt der Erfindung ist eine Vorrichtung an Bord eines Kraftfahrzeugs dazu eingerichtet, einen ersten Einweg-Hash x eines Passworts p, und einen verschlüsselten Wert V aus dem zweiten Einweg-Hash y des Passworts p zu speichern; ferner ein PACE-Verfahren mit einem Gerät durchzuführen, um einen Sitzungsschlüssel zu bestimmen; einen Kommunikationsschlüssel auf der Basis des Sitzungsschlüssels und des verschlüsselten Einweg-Hashs V zu erzeugen und eine auf der Basis des Kommunikationsschlüssels verschlüsselte Kommunikation mit dem Gerät zu führen.

Nach noch einem weiteren Aspekt der Erfindung umfasst ein Kraftfahrzeug eine hierin beschriebene Vorrichtung.

Ein zu der hierin beschriebenen Vorrichtung an Bord des Kraftfahrzeugs korrespondierendes Gerät ist dazu eingerichtet, ein PACE-Verfahren mit der Vorrichtung durchzuführen, um einen Sitzungsschlüssel zu bestimmen; und

einen Kommunikationsschlüssel auf der Basis des Sitzungsschlüssels und eines Einweg-Hashs y eines für das PACE-Verfahren verwendeten Passworts p zu bestimmen.

Auf der Basis des Kommunikationsschlüssels können das Gerät und die Vorrichtung an Bord des Kraftfahrzeugs eine verschlüsselte Kommunikation führen.

Zur Durchführung wenigstens eines Teils eines hierin beschriebenen Verfahrens können das Gerät und/oder die Vorrichtung jeweils eine Verarbeitungsvorrichtung kann einen programmierbaren Mikrocomputer oder Mikrocontroller umfassen und das Verfahren kann in Form eines Computerprogrammprodukts mit Programmcodemitteln vorliegen. Das Computerprogrammprodukt kann auch auf einem computerlesbaren Datenträger abgespeichert sein. Merkmale oder Vorteile des Verfahrens können auf die Vorrichtung oder das Gerät übertragen werden oder umgekehrt.

Die Erfindung wird nun mit Bezug auf die beigefügten Zeichnungen genauer beschrieben, in denen:

Figur 1 ein System; und
Figur 2 ein Ablaufdiagramm eines Verfahrens

illustriert.

Figur 1 zeigt ein System 100, das ein Kraftfahrzeug 105 und ein Gerät 110 umfasst. An Bord des Kraftfahrzeugs 105 ist eine Vorrichtung 115 angebracht, die bevorzugt eine Übertragungsvorrichtung 120 und eine Verarbeitungsvorrichtung 125 umfasst.

Die Vorrichtung 115 und das Gerät 110 sind dazu eingerichtet, über eine bevorzugt drahtlose Schnittstelle 130 miteinander zu kommunizieren, wozu die Vorrichtung 115 insbesondere die Übertragungsvorrichtung 120 einsetzen kann. Die Schnittstelle 130 kann zur Übertragung in einem vorbestimmten Nahbereich eingeschränkt sein, beispielsweise in einem Abstand von typisch ca. 10 Meter zwischen dem Kraftfahrzeug 105 und dem Gerät 110. In einer weiteren Variante

kann die Schnittstelle zur Kommunikation mit dem Gerät 110 in einem Innenraum des Kraftfahrzeugs 105 eingerichtet sein.

Das Gerät 110 ist bevorzugt einem Benutzer 135 zugeordnet und kann weiter bevorzugt ein Mobilgerät umfassen, das zur mobilen Verwendung eingerichtet ist, beispielsweise als Mobiltelefon, Smartphone, Tablet Computer oder Laptop Computer. Der Benutzer 135 kann dem Kraftfahrzeug 105 zugeordnet sein, beispielsweise als Fahrer, Fahrgast, Eigentümer, Mieter oder Leasingnehmer.

Eine Kommunikation zwischen dem Gerät 110 und der Vorrichtung 115 soll verschlüsselt erfolgen, wobei die Verschlüsselung von einem Passwort abhängen soll, das seitens des Geräts 110 – insbesondere seitens des Benutzers 135 – bekannt ist. Weiter ist bevorzugt, dass Informationen über das Passwort in keiner Form in der Vorrichtung 115 abgelegt sind, dass ein Angreifer daraus das Passwort algorithmisch rekonstruieren könnte.

Ein hierin beschriebenes Verfahren kann zur Herstellung einer verschlüsselten Kommunikation genutzt werden. In einer Ausführungsform kann dadurch das Gerät 110 gegenüber der Vorrichtung 115, oder der Benutzer 135 gegenüber dem Kraftfahrzeug 105 authentifiziert werden. Die Nutzung einer Funktion kann erst nach erfolgter Authentifizierung ermöglicht sein.

Figur 2 zeigt ein Ablaufdiagramm eines Verfahrens 200 zur verschlüsselten Kommunikation zwischen einem Gerät 110 und einer Vorrichtung 115, die bevorzugt an Bord eines Kraftfahrzeugs 105 angebracht ist. Das Verfahren 200 kann insbesondere mittels Elementen des Systems 100 durchgeführt werden.

Im Folgenden wird eine Formelschreibweise verwendet, in der ein kleiner lateinischer Buchstabe einer Zahl und ein großer lateinischer Buchstabe einem Punkt auf einer elliptischen Kurve entspricht, der zur Verschlüsselung oder Entschlüsselung verwendet wird. Eine zufällig gewählte Zeichenfolge zur Entropieerhöhung bei der Bildung eines Einweg-Hashes wird auch Salt genannt und hier mit s abgekürzt.

In Figur 2 sind exemplarisch Schritte, die bevorzugt seitens des Kraftfahrzeugs 105 bzw. der Vorrichtung 115 durchgeführt werden, links dargestellt und Schritte,

die bevorzugt seitens des Geräts 110 bzw. des Benutzers 135 durchgeführt werden, rechts dargestellt. Ein in der Mitte dargestellter Schritt kann beide Seiten betreffen.

Ein erster Abschnitt 205 des Verfahrens 200 betrifft das Provisionieren, also das Hinterlegen von Informationen, die für eine spätere Authentifizierung zwischen den Kommunikationspartnern 110 und 115 erforderlich sind. Ein zweiter Abschnitt 210 betrifft das Aushandeln oder Erstellen einer verschlüsselten Kommunikationsverbindung zwischen dem Gerät 110 und der Vorrichtung 115. Beide Abschnitte 205, 210 können auch als eigenständige Verfahren aufgefasst werden.

Bezug nehmend auf den ersten Abschnitt 205 kann in einem Schritt 215 ein Passwort p bestimmt werden, das der Benutzer 135 später zur Authentifizierung verwenden soll. Der Benutzer 135 kann ein beliebiges Passwort p wählen oder es kann ein Passwort p vorgeschlagen werden, das der Benutzer 135 akzeptieren kann. Bevorzugt umfasst das Passwort p eine Kette insbesondere alphanumerischer Zeichen, die sich der Benutzer 135 merken und mittels einer realen oder virtuellen Tastatur in das Gerät 110 eingeben kann. Eine Operation $\star$ steht für eine Multiplikation einer Zahl mit einem Punkt einer elliptischen Kurve, eine Operation $\cdot$ für eine Multiplikation zweier Zahlen. $\oplus$ bezeichnet eine Addition, $\ominus$ eine Subtraktion auf elliptischen Kurven.

In einem Schritt 220 können auf der Basis des Passworts mittels einer ersten Einweg-Hashfunktion H ein erster Einweg-Hash x=H(s,p) und mittels einer zweiten Einweg-Hashfunktion G ein zweiter Einweg-Hash y=G(s,p) bestimmt werden. Der zweite Einweg-Hash y wird bevorzugt mittels eines gewählten Generator- oder Basispunkts G verschlüsselt: $V = y \star G$. Diese Operationen können seitens des Geräts 110 oder seitens einer externen Stelle durchgeführt werden, die sich bevorzugt nicht an Bord des Kraftfahrzeugs 105 befindet. In einem Schritt 225 werden bevorzugt x und V, das Salt s, sowie eine Identifikation I des Benutzers 135 in der Vorrichtung 115 hinterlegt.

Bezug nehmend auf den zweiten Abschnitt 210 wird zunächst in Schritten 230 bis 260 ein an sich bekanntes PACE-Verfahren (Password Authenticated Connection

Establishment) durchgeführt, das eine Authentisierung und einen sicheren Schlüsselaustausch zur Herstellung einer kryptographisch abgesicherten Kommunikationsverbindung umfasst. Das PACE-Verfahren ist in der Technischen Richtlinie TR-03110 des Deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) genau beschrieben. PACE zählt zur Familie der Password Authenticated Key Exchange (PAKE) Protokolle. Durch nachfolgende Schritte 265 bis 275 des zweiten Abschnitts 210 entsteht insgesamt ein Verbessertes (Augmented) PAKE-Verfahren, das hierin auch PACE+ genannt wird.

In einer genaueren Betrachtung kann in einem Schritt 230 seitens des Geräts 110 eine Zufallszahl a gewählt und verschlüsselt werden: $A = a \star G$. Die verschlüsselte Zufallszahl A wird bevorzugt zusammen mit einem Salt s an die Vorrichtung 115 übermittelt. In umgekehrter Richtung kann seitens der Vorrichtung 115 eine Zufallszahl b gewählt und verschlüsselt werden: $B = b \star G$. Die verschlüsselte Zufallszahl B wird bevorzugt zusammen mit einem Salt s an das Gerät 110 übermittelt. Auf beiden Seiten kann die empfangene Information auf einen Erzeuger der verwendeten mathematischen Gruppe abgebildet werden: $T = a \star B = (a \cdot b) \star G = (b \cdot a) \star G = b \star A$.

In einem Schritt 250 erfolgt bevorzugt der tatsächliche Schlüsselaustausch. Dazu kann der Benutzer 135 das Passwort p in das Gerät 110 eingeben und der Einweg-Hash $x = H(s, p)$ kann bestimmt werden. Eine gewählte Zufallszahl c kann auf der Basis von x verschlüsselt werden: $C = \mathrm{Enc}_x(c)$. Die verschlüsselte Zufallszahl C kann dann an die Vorrichtung 115 an Bord des Kraftfahrzeugs 105 übermittelt werden.

Die Vorrichtung 115 kann die empfangene Zufallszahl entschlüsseln: $c = \mathrm{Dec}_x(C)$. Dabei wird eine Entschlüsselung Dec_x verwendet, die zur Verschlüsselung Enc_x korrespondiert und auf dem Einweg-Hash x basiert. Die Vorrichtung 115 und das Gerät 110 können dann jeweils einen vorübergehenden Generatorpunkt D bestimmen: $D = c \star G \oplus T$. Auf der Basis von D kann dann eine Diffie-Hellmann Vereinbarung getroffen werden.

Seitens des Geräts 110 kann eine weitere Zufallszahl e bestimmt werden, die mit D verschlüsselt werden kann: $E = e \star D$. Seitens der Vorrichtung 115 kann eine weitere Zufallszahl f bestimmt werden, die mit D verschlüsselt werden kann: $F = f \star D$. Die bestimmten verschlüsselten Zufallszahlen E und F werden dann bevorzugt an den jeweils anderen Kommunikationspartner übermittelt, also E vom Gerät 110 an die Vorrichtung 115 und F von der Vorrichtung 115 an das Gerät 110. Die Vorrichtung 115 kann dann einen ersten Kommunikationsschlüssel $K_H = e \star F = (e \cdot f) \star D$ bestimmen und das Gerät 110 kann einen zweiten Kommunikationsschlüssel $K_U = f \star E = (f \cdot e) \star D$ bestimmen. Dabei gilt: $K = K_U = K_H$.

Sollte die Entschlüsselung einer mittels K verschlüsselten und zwischen den Kommunikationspartnern 110, 115 übermittelten Nachricht empfängerseitig nicht möglich sein, so gilt der zweite Abschnitt 210 des Verfahrens 200 allgemein als gescheitert und kann abgebrochen oder neu begonnen werden.

Im Anschluss an das PACE-Verfahren der Schritte 230 bis 260 kann in einem Schritt 265 seitens der Vorrichtung 115 ein Kommunikationsschlüssel $\mathrm{sk} = \mathrm{H}(\mathrm{x}, \mathrm{T}, \mathrm{D}, \mathrm{K}, \mathrm{b} \star \mathrm{V})$ gebildet werden. Dies ist möglich, weil im ersten Abschnitt 205 b und V in der Vorrichtung 115 hinterlegt wurden. Seitens des Geräts 110 kann ein Kommunikationsschlüssel $\mathrm{sk} = \mathrm{H}(\mathrm{x}, \mathrm{T}, \mathrm{D}, \mathrm{K}, \mathrm{y} \star \mathrm{B})$ gebildet werden. Dazu kann das Gerät 110 die verschlüsselte Zufallszahl B aus dem Diffie-Hellmann-Schlüsselaustausch verwenden.

Die beiden gebildeten Kommunikationsschlüssel *sk* sind identisch, da gilt: $\mathrm{y} \star \mathrm{B} = \mathrm{y} \star (\mathrm{b} \star \mathrm{G}) = (\mathrm{y} \cdot \mathrm{b}) \star \mathrm{G} = (\mathrm{b} \cdot \mathrm{y}) \star \mathrm{G} = \mathrm{b} \star (\mathrm{y} \star \mathrm{G}) = \mathrm{b} \star \mathrm{V}$.

Diese zusätzlichen Operationen verwandeln das bekannte PACE-Verfahren in ein verbessertes PAKE-Protokoll, da auf Seiten der Vorrichtung 115 nur V verwendet wird, während auf Seiten des Geräts 110 der unverschlüsselte Wert y erforderlich ist, der auf der Basis des Schlüssels p gebildet werden muss.

In einem folgenden Schritt 275 kann eine Kommunikation zwischen der Vorrichtung 115 und dem Gerät 110 auf der Basis des Kommunikationsschlüssels *sk* durchgeführt werden. Ist dies nicht möglich, so

kann der zweite Abschnitt 210 des Verfahrens 200 als gescheitert angesehen werden. Die Kommunikation kann die Herstellung einer Verbindung umfassen, die auch Sitzung genannt wird, wobei der Vorgang des Verbindens auch Paarung (Pairing) genannt werden kann.

Die Komplexität des vorgeschlagenen zweiten Abschnitts 210 des Verfahrens 200 ist überschaubar. Seitens der Vorrichtung 115 sind zur Bestimmung des Kommunikationsschlüssels *sk* sechs Skalarmultiplikationen oder vier Skalarmultiplikationen und eine bilineare Skalarmultiplikation durchzuführen. Der Aufwand seitens des Geräts 110 ist gleich groß.

Bezugszeichen

100	System
105	Kraftfahrzeug
110	Gerät, Mobilgerät
115	Vorrichtung
120	Übertragungsvorrichtung
125	Verarbeitungsvorrichtung
130	Schnittstelle
200	Verfahren
205	erster Abschnitt
210	zweiter Abschnitt
215	Passwort bestimmen
220	Hashes bestimmen
225	Hashes hinterlegen
230	Nonce bestimmen, verschlüsseln, übermitteln
235	entschlüsseln
240	Nonce auf Erzeuger abbilden
245	Nonce auf Erzeuger abbilden
250	Diffie-Hellmann-Schlüsselaustausch
255	Sitzungsschlüssel ableiten
260	Sitzungsschlüssel ableiten
265	Kommunikationsschlüssel ableiten
270	Kommunikationsschlüssel ableiten
275	Kommunikation / Pairing

Ansprüche

1. Verfahren (200) zum Authentifizieren eines Geräts (110) gegenüber einem Kraftfahrzeug (105), wobei seitens des Kraftfahrzeugs (105) ein erster Einweg-Hash x eines Passworts p, und ein verschlüsselter Wert V aus dem zweiten Einweg-Hash y des Passworts p abgelegt sind, wobei das Verfahren (200) folgende Schritte umfasst:
   - Durchführen (230-260) eines PACE-Verfahrens (200), um seitens des Geräts (110) und des Kraftfahrzeugs (105) den gleichen Sitzungsschlüssel zu bestimmen;
   - Erzeugen (265) eines Kommunikationsschlüssels seitens des Kraftfahrzeugs (105) auf der Basis des Sitzungsschlüssels und des verschlüsselten Einweg-Hashs V; und
   - Erzeugen (270) des Kommunikationsschlüssels seitens des Geräts (110) auf der Basis des Sitzungsschlüssels und des zweiten Einweg-Hashs y.

2. Verfahren (200) nach Anspruch 1, wobei der zweite Einweg-Hash y des Passworts p bezüglich eines vorbestimmten Basispunkts eines Verschlüsselungssystems verschlüsselt ist.

3. Verfahren (200) nach Anspruch 1 oder 2, wobei das Gerät (110) mit dem Kraftfahrzeug (105) verknüpft (275) wird, falls eine verschlüsselte Kommunikation auf der Basis des Kommunikationsschlüssels möglich ist.

4. Verfahren (200) nach einem der vorangehenden Ansprüche, wobei eine Verschlüsselung auf der Basis elliptischer Kurven durchgeführt wird.

5. Verfahren (200) nach einem der vorangehenden Ansprüche, wobei das Gerät (110) ein mobiles Gerät (110) umfasst.

6. Verfahren (200) nach einem der vorangehenden Ansprüche, wobei das Gerät (110) ein einem vorbestimmten Benutzer zugeordnetes persönliches

Gerät (110) umfasst

7. Vorrichtung (115) an Bord eines Kraftfahrzeugs (105), wobei die Vorrichtung (115) dazu eingerichtet ist, einen ersten Einweg-Hash x eines Passworts p, und einen verschlüsselten Wert V aus dem zweiten Einweg-Hash y des Passworts p zu speichern; ein PACE-Verfahren (200) mit einem Gerät (110) durchzuführen, um einen Sitzungsschlüssel zu bestimmen; einen Kommunikationsschlüssel auf der Basis des Sitzungsschlüssels und des verschlüsselten Einweg-Hashs V zu erzeugen; und eine auf der Basis des Kommunikationsschlüssels verschlüsselte Kommunikation mit dem Gerät (110) zu führen.

8. Kraftfahrzeug (105), umfassend eine Vorrichtung (115) nach Anspruch 7.

9. Gerät (110), das dazu eingerichtet ist, ein PACE-Verfahren (200) mit einer Vorrichtung (115) an Bord eines Kraftfahrzeugs (105) durchzuführen, um einen Sitzungsschlüssel zu bestimmen; und einen Kommunikationsschlüssel auf der Basis des Sitzungsschlüssels und eines Einweg-Hashs y eines für das PACE-Verfahren (200) verwendeten Passworts p zu bestimmen.

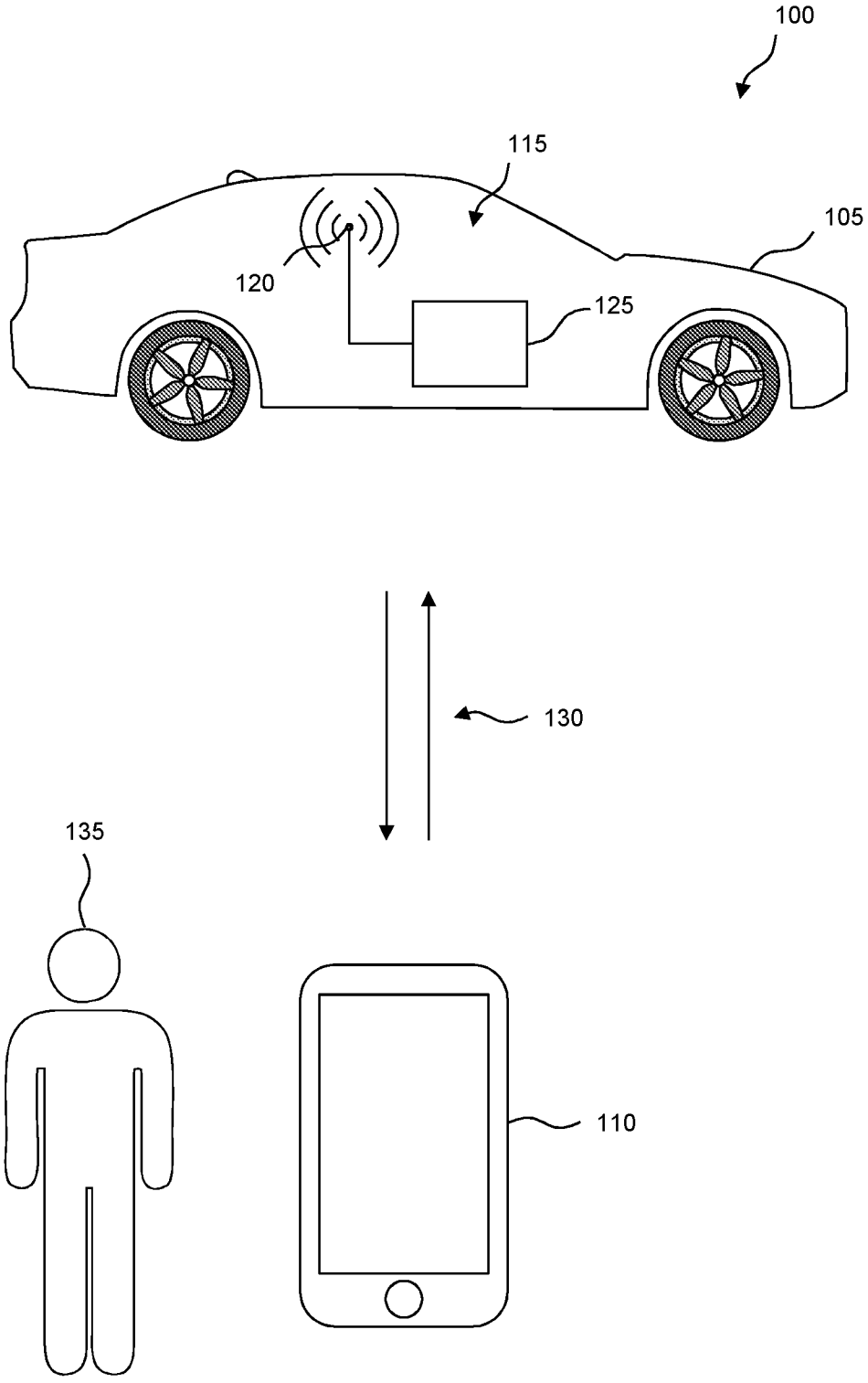


Fig. 1

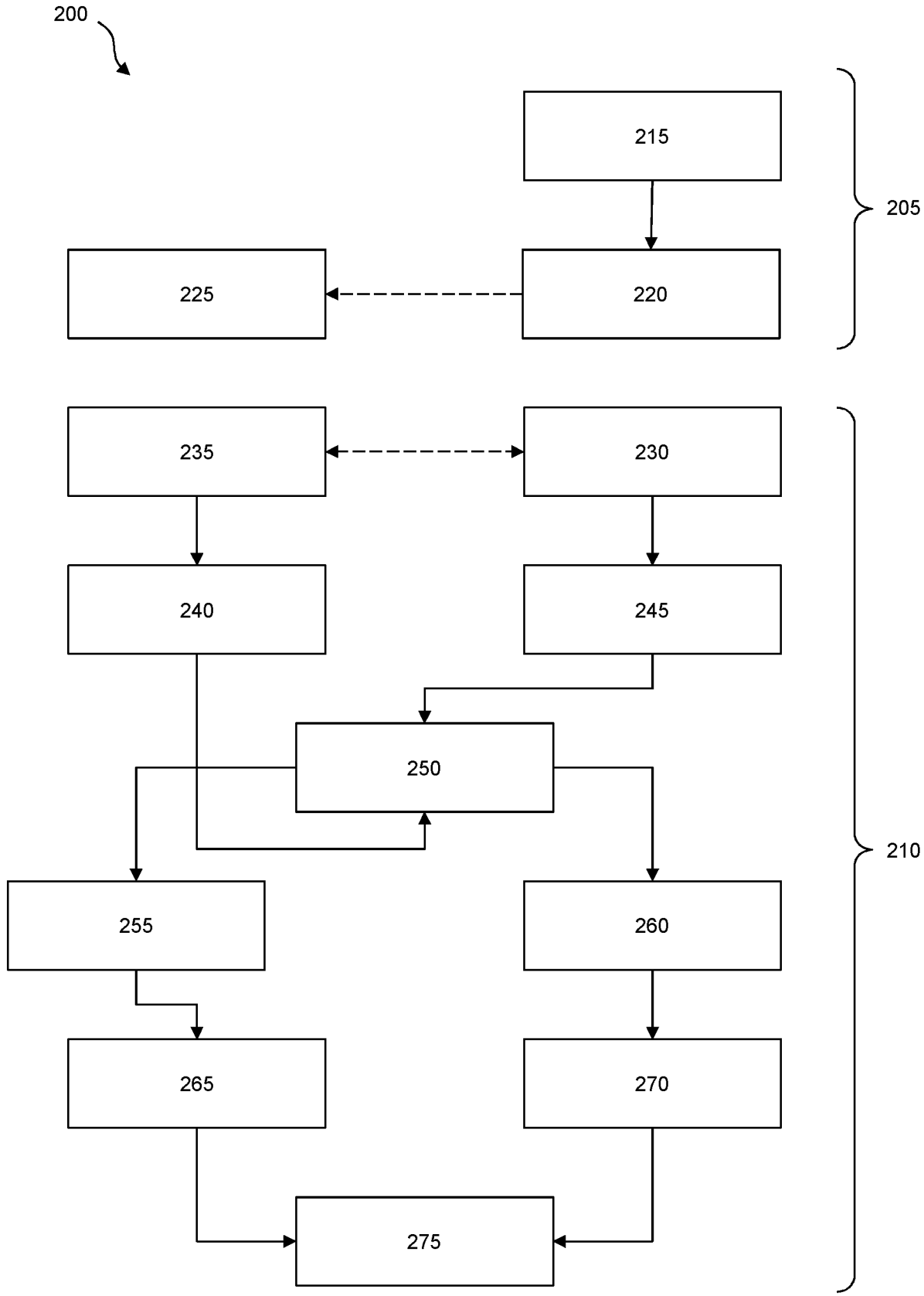


Fig. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/DE2020/100063

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/30(2006.01)i; ***H04L 9/08***(2006.01)i

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)

H04L

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2518932 A2 (BRANDENBURGISCHE TECH UNI COTTBUS [DE]) 31 October 2012 (2012-10-31) paragraph [0028] - paragraph [0041]	1-9
X	US 2008165955 A1 (IBRAHIM MOHAMMAD K [GB]) 10 July 2008 (2008-07-10) paragraph [0079] paragraph [0230] - paragraph [0242]	1-9
A	TEO J C M ET AL. "An Anonymous DoS-Resistant Password-Based Authentication, Key Exchange and Pseudonym Delivery Protocol for Vehicular Networks" *ADVANCED INFORMATION NETWORKING AND APPLICATIONS, 2009. AINA '09. INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA,* 26 May 2009 (2009-05-26), pages 675-682 ISBN: 978-1-4244-4000-9. XP031476166 the whole document	1-9

☑ 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	Date of mailing of the international search report
05 May 2020	**13 May 2020**

Name and mailing address of the ISA/EP	Authorized officer
European Patent Office **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	**Apostolescu, Radu** Telephone No.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	STANISLAW JARECKI ET AL. "OPAQUE: An Asymmetric PAKE Protocol Secure Against Pre-Computation Attacks" , Vol. 20190107:165837, 07 January 2019 (2019-01-07), pages 1-39, IACR, INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH, Retrieved from the Internet: http://eprint.iacr.org/2018/163.pdf [retrieved on 2019-01-07] XP061027458 the whole document	1-9

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/DE2020/100063

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
EP 2518932 A2	31 October 2012	EP 2518932 A2	31 October 2012
		US 2012082312 A1	05 April 2012
US 2008165955 A1	10 July 2008	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE2020/100063

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L9/30 H04L9/08
ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L

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

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

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 2 518 932 A2 (BRANDENBURGISCHE TECH UNI COTTBUS [DE]) 31. Oktober 2012 (2012-10-31) Absatz [0028] - Absatz [0041]	1-9
X	US 2008/165955 A1 (IBRAHIM MOHAMMAD K [GB]) 10. Juli 2008 (2008-07-10) Absatz [0079] Absatz [0230] - Absatz [0242]	1-9

-/--

[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 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	Absendedatum des internationalen Recherchenberichts
5. Mai 2020	13/05/2020

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	Apostolescu, Radu

1

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	TEO J C M ET AL: "An Anonymous DoS-Resistant Password-Based Authentication, Key Exchange and Pseudonym Delivery Protocol for Vehicular Networks", ADVANCED INFORMATION NETWORKING AND APPLICATIONS, 2009. AINA '09. INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 26. Mai 2009 (2009-05-26), Seiten 675-682, XP031476166, ISBN: 978-1-4244-4000-9 das ganze Dokument -----	1-9
A	STANISLAW JARECKI ET AL: "OPAQUE: An Asymmetric PAKE Protocol Secure Against Pre-Computation Attacks", IACR, INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH , Bd. 20190107:165837 7. Januar 2019 (2019-01-07), Seiten 1-39, XP061027458, Gefunden im Internet: URL:http://eprint.iacr.org/2018/163.pdf [gefunden am 2019-01-07] das ganze Dokument -----	1-9

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE2020/100063

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 2518932 A2	31-10-2012	EP 2518932 A2	31-10-2012
		US 2012082312 A1	05-04-2012
US 2008165955 A1	10-07-2008	KEINE	