(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
12 janvier 2023 (12.01.2023)

WIPO | PCT

(10) Numéro de publication internationale
WO 2023/280699 A1

(51) Classification internationale des brevets :
G06F 13/42 (2006.01) *H04L 12/40* (2006.01)
H04L 12/413 (2006.01) *H04L 9/40* (2022.01)

(21) Numéro de la demande internationale :
PCT/EP2022/068242

(22) Date de dépôt international :
01 juillet 2022 (01.07.2022)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
FR2107276 06 juillet 2021 (06.07.2021) FR

(71) Déposant : **CONTINENTAL AUTOMOTIVE GMBH** [DE/DE] ; Vahrenwalder Strasse 9, 30165 HANOVRE (DE).

(72) Inventeurs : **BOISSET, Jean-Philippe** ; CONTINENTAL AUTOMOTIVE FRANCE - Service Intellectual Property, 1, avenue Paul Ourliac, 31100 TOULOUSE (FR). **ELORCH, Mounir** ; CONTINENTAL AUTOMOTIVE FRANCE - Service Intellectual Property, 1, avenue Paul Ourliac, 31100 TOULOUSE (FR). **BOUROUNIA, Abir** ; CONTINENTAL AUTOMOTIVE FRANCE - Service Intellectual Property, 1, avenue Paul Ourliac, 31100 TOULOUSE (FR).

(74) Mandataire : **KAABOUNI, Fatima** ; CONTINENTAL AUTOMOTIVE FRANCE - Service Intellectual Property, 1, avenue Paul Ourliac, 31100 TOULOUSE (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : 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, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN,

WO 2023/280699 A1

(54) **Title:** ANTI-IDENTITY THEFT METHOD FOR A SPECIFIC ELECTRONIC CONTROL UNIT OF A MOTOR VEHICLE

(54) **Titre :** PROCÉDÉ POUR PRÉVENIR L'USURPATION D'IDENTITÉ D'UNE UNITÉ DE COMMANDE ÉLECTRONIQUE PARTICULIÈRE D'UN VÉHICULE AUTOMOBILE

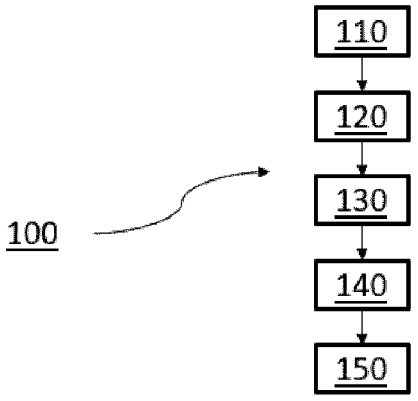

FIG. 1

(57) Abstract: The invention relates to an anti-identity theft method for a specific electronic control unit of a motor vehicle, which method is used when the specific electronic control unit sends a plaintext message (M) containing measurement data to a central electronic control unit of the motor vehicle. The method of the invention comprises the steps of: - generating (110) an identifier for selecting a hashing algorithm (hi), - obtaining (120) at least one parameter (K) shared by the central electronic control unit and the specific electronic control unit, - generating (130) a first digital hash fingerprint (E) of the combination of the plaintext message (M) and the common parameter (K) from the identifier for selecting a hashing algorithm (hi), - forming (140) a data frame (T) which includes the plaintext message (M), the identifier for selecting a hashing algorithm (hi) and the first digital hash fingerprint (E), and - sending (150) the data frame (T) to the central electronic control unit.

(57) Abrégé : L'invention concerne un procédé pour prévenir l'usurpation d'identité d'une unité de commande électronique particulière d'un véhicule automobile, lorsque l'unité de commande électronique particulière envoie un message en clair (M), qui contient des données de mesure, à une unité de commande électronique centrale du véhicule automobile. Dans l'invention, on : - génère (110) un identifiant de sélection d'un algorithme de hachage (hi), - obtient (120) au moins un paramètre commun (K) à l'unité de commande électronique centrale et l'unité de commande électronique particulière, - générer (130) une première empreinte numérique de hachage (E) de la combinaison du message en clair (M) et du paramètre commun (K), à partir de l'identifiant de sélection d'un algorithme de hachage (hi), - forme (140) une trame de données (T) qui inclut le message en clair (M), l'identifiant de sélection d'un algorithme de hachage (hi) et la première empreinte numérique de hachage (E), et - envoie (150) la trame de données (T) à l'unité de commande électronique centrale.

[Suite sur la page suivante]

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) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (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).

Publiée:

— *avec rapport de recherche internationale (Art. 21(3))*

— *en noir et blanc ; la demande internationale telle que déposée était en couleur ou en échelle de gris et est disponible sur PATENTSCOPE pour téléchargement.*

DESCRIPTION

TITRE : PROCÉDÉ POUR PRÉVENIR L'USURPATION D'IDENTITÉ D'UNE UNITÉ DE COMMANDE ÉLECTRONIQUE PARTICULIÈRE D'UN VÉHICULE AUTOMOBILE

[Domaine technique]

[0001] L'invention concerne les techniques de prévention de l'usurpation d'identité dans les systèmes automobiles. Plus particulièrement, l'invention concerne un procédé pour prévenir l'usurpation d'identité d'une unité de commande électronique particulière d'un véhicule automobile, lorsque l'unité de commande électronique particulière envoie un message en clair, qui contient des données de mesure, à une unité de commande électronique centrale du véhicule automobile.

[Etat de la technique antérieure]

[0002] Les capteurs de pression de pneu agencés sur la jante d'un véhicule automobile, dits capteurs TPMS (pour tire pressure monitoring system, en anglais) transmettent régulièrement des données de mesure à une unité centrale du véhicule automobile par un lien radiofréquence sur une porteuse de fréquence déterminée (par ex. 433 MHz ou 2.4 GHz). Ces données sont envoyées dans un message en clair, et il n'est pas possible de vérifier l'authenticité de l'émetteur, c'est-à-dire l'origine du message.

[0003] Ainsi, un tiers malveillant (ou attaquant) pourrait se faire passer pour un tel capteur et envoyer de faux messages que l'unité centrale du véhicule automobile interprèterait comme valides et compréhensibles.

[0004] Or, une telle possibilité peut être dangereuse pour les passagers du véhicule automobile.

[0005] En effet, ces faux messages permettraient de simuler une anomalie de pression pour forcer l'arrêt du véhicule automobile et déboucher, par exemple, sur un méfait de type « car jacking ».

[0006] Par ailleurs, ces faux messages peuvent masquer une réelle anomalie de pression et ainsi porter atteinte à la sécurité des passagers du véhicule automobile.

[0007] On a proposé des solutions qui consistent à crypter les données de mesure grâce à une clé privée ou symétrique fournie par l'unité centrale du véhicule automobile au capteur, lors de l'appairage par exemple, en sorte que le cryptage des données est possible uniquement par le capteur autorisé. Dans ce cas, des données de mesures ainsi cryptées sont décodables par toute entité les recevant qui possède la clé publique ou symétrique.

[0008] Toutefois, cette solution présente l'inconvénient de nécessiter un rafraichissement périodique de la clé pour éviter que l'information éventuellement apprise pendant les périodes passées n'aide un attaquant pendant les périodes ultérieures.

[0009] En résumé, il est nécessaire de s'assurer de l'authenticité des messages émis.

[0010] Il est également nécessaire de vérifier l'intégrité des messages émis.

[0011] Enfin, il est aussi nécessaire d'empêcher l'usurpation d'identité d'un capteur d'un véhicule automobile.

[Exposé de l'invention]

[0012] L'invention vise à pallier ces inconvénients.

[0013] A cet effet, il est proposé un procédé pour prévenir l'usurpation d'identité d'une unité de commande électronique particulière d'un véhicule automobile, lorsque l'unité de commande électronique particulière envoie un message en clair, qui contient des données de mesure, à une unité de commande électronique centrale du véhicule automobile, l'unité de commande électronique centrale comprenant au moins une base de données qui stocke au moins un tuple de valeurs, formé d'un identifiant de sélection d'un algorithme de hachage et d'un algorithme de hachage. Le procédé comprend les étapes suivantes, mises en œuvre au niveau de l'unité de commande électronique particulière :

- générer un identifiant de sélection d'un algorithme de hachage,

- obtenir au moins un paramètre évolutif commun à l'unité de commande électronique centrale et l'unité de commande électronique particulière,

- générer une première empreinte numérique de hachage de la combinaison du message en clair et du paramètre commun, à partir de l'identifiant de sélection d'un algorithme de hachage,

- former une trame de données qui inclut le message en clair, l'identifiant de sélection d'un algorithme de hachage (hi) et la première empreinte numérique de hachage, et

- envoyer la trame de données à l'unité de commande électronique centrale.

[0014] Dans un mode de mise en œuvre, le procédé peut comprendre en outre les étapes suivantes, mises en œuvre au niveau de l'unité de commande électronique centrale, en réponse à la réception de la trame de données :

- extraire le message en clair et l'identifiant de sélection d'un algorithme de hachage de la trame de données,

- obtenir le paramètre évolutif commun à l'unité de commande électronique centrale et l'unité de commande électronique particulière,

- générer une deuxième empreinte numérique de hachage de la combinaison du message en clair et du paramètre commun, à partir de l'identifiant de sélection d'un algorithme de hachage,

- comparer la première empreinte numérique et la deuxième empreinte numérique, et

- utiliser les données de mesure du message en clair en fonction de la comparaison.

[0015] Dans une mise en œuvre, le procédé peut comprendre en outre les étapes suivantes :

- crypter, par l'unité de commande électronique particulière, la première empreinte numérique de hachage avec une clé privée secrète l'unité de commande électronique particulière, avant de former la trame de données, et

- décrypter, par l'unité de commande électronique particulière, la première empreinte numérique de hachage avec une clé publique de l'unité de commande électronique particulière qui est associée à la clé privée secrète l'unité de commande électronique particulière, avant de comparer la première empreinte numérique et la deuxième empreinte numérique.

[0016] Par exemple :

- on utilise la clé privée secrète d'une paire clé publique/clé privée secrète, en fonction d'un paramètre de sélection de clé asymétrique de cryptage que l'on insère dans la trame de données, et

- on utilise la clé publique de la paire clé publique/clé privée secrète, en fonction du paramètre de sélection de clé asymétrique de cryptage que l'on extrait de la trame de données.

[0017] Dans un exemple, le procédé peut comprendre en outre l'étape suivante :

- supprimer, par l'unité de commande électronique particulière, un champ CRC du message en clair qui contient une séquence CRC, avant de former la trame de données.

[0018] Le procédé peut aussi comprendre, en outre, l'étape suivante :

- chercher, par l'unité de commande électronique centrale, dans la base de données, l'algorithme de hachage associé à l'identifiant de sélection d'un algorithme de hachage, avant de générer la deuxième empreinte numérique de hachage.

[0019] Dans un mode de mise en œuvre, on peut prévoir que, au niveau de l'unité de commande électronique particulière, l'identifiant de sélection d'un algorithme de hachage est un index aléatoire qui est associé à une position spécifique dans une liste prédéterminée d'algorithmes de hachage, la liste étant stockée dans une mémoire de l'unité de commande électronique particulière.

[0020] Par exemple on peut générer l'index aléatoire avant l'envoi de chaque trame de données.

[0021] Dans un mode de mise en œuvre, on choisit le paramètre commun parmi : un compteur, un générateur pseudo-aléatoire et une horloge.

[0022] Par exemple, au niveau l'unité de commande électronique particulière et au niveau de l'unité de commande électronique centrale, on renouvelle la valeur du paramètre commun selon une périodicité prédéterminée.

[Description des dessins]

[0023] D'autres caractéristiques et avantages de l'invention apparaîtront encore à la lecture de la description qui va suivre. Celle-ci est purement illustrative et doit être lue en regard des dessins annexés sur lesquels :

[Fig. 1] La figure 1 représente un procédé selon l'invention lorsqu'il est mis en œuvre au niveau d'une unité de commande électronique particulière.

[Fig. 2] La figure 2 représente un procédé selon l'invention lorsqu'il est mis en œuvre au niveau d'une unité de commande électronique centrale.

[Fig. 3] La figure 3 représente une trame de données selon l'invention.

[0024] Les figures ne respectent pas nécessairement les échelles, notamment en épaisseur, et ce à des fins d'illustration.

[Description des modes de réalisation]

[0025] La figure 1 illustre un procédé 100 pour prévenir l'usurpation d'identité d'une unité de commande électronique particulière d'un véhicule automobile. En particulier, lorsque l'unité de commande électronique particulière envoie un message en clair M, qui contient des données de mesure, à une unité de commande électronique centrale du véhicule automobile.

[0026] On entend par unité de commande électronique, un microprocesseur, un automate programmable ou un contrôleur qui est adapté pour contrôler le fonctionnement des systèmes du véhicule automobile, tels que le groupe motopropulseur, le système de

climatisation, le système d'info-divertissement, les systèmes de carrosserie, les systèmes de châssis, le système des unités TPMS (mis pour « Tire Pressure Monitoring System », en anglais) et autres.

[0027] Dans l'invention, une unité de commande électrique centrale contrôle le fonctionnement global du véhicule automobile, tandis qu'une unité de commande électronique particulière contrôle le fonctionnement d'au moins un des systèmes du véhicule automobile.

[0028] Dans l'invention, l'unité de commande électronique centrale comprend au moins une base de données qui stocke au moins un tuple de valeurs, formé d'un identifiant de sélection d'un algorithme de hachage hi et d'un algorithme de hachage.

[0029] En d'autres termes, la base de données permet d'associer un identifiant de sélection d'un algorithme de hachage hi avec un algorithme de hachage stocké.

[0030] Dans un exemple, on choisit l'algorithme de hachage parmi : l'algorithme SHA, l'algorithme MD5, l'algorithme AES et l'algorithme TDES. Toutefois, on peut utiliser d'autres algorithmes de hachage sans nécessiter de modifications substantielles de l'invention.

[0031] Dans l'étape 110, on utilise l'unité de commande électronique particulière pour générer un identifiant de sélection d'un algorithme de hachage hi.

[0032] Dans une mise en œuvre particulière de l'étape 110, l'identifiant de sélection d'un algorithme de hachage hi est un index aléatoire qui est associé à une position spécifique dans une liste prédéterminée d'algorithmes de hachage.

[0033] Dans cette mise en œuvre particulière, une mémoire de l'unité de commande électronique particulière stocke la liste.

[0034] Dans l'étape 120, on utilise l'unité de commande électronique particulière pour obtenir au moins un paramètre masqué K qui est commun à l'unité de commande électronique centrale et à l'unité de commande électronique particulière. Ce paramètre K est un paramètre évolutif, à la manière d'un code tournant, qui évolue selon une même loi d'évolution, à la fois dans l'unité de commande électronique particulière et dans l'unité de commande électronique centrale.

[0035] Dans une mise en œuvre particulière de l'étape 120, on choisit le paramètre commun K comme une valeur produite par un dispositif générateur parmi : un compteur, une horloge et un générateur pseudo-aléatoire.

[0036] Le paramètre commun K est connu de l'unité de commande électronique centrale et de l'unité de commande électronique particulière. A cet effet, l'unité de commande électronique centrale et l'unité de commande électronique particulière comprennent chacune un générateur du type précité, qui opèrent parallèlement, de manière indépendante, dans chacune des parties à l'échange de messages.

[0037] Pour cela, on peut prévoir une phase préalable d'initialisation durant laquelle l'unité de commande électronique centrale et de l'unité de commande électronique particulière peuvent synchroniser leur valeur respective du paramètre commun K, par exemple en s'échangeant des messages appropriés. Après cette synchronisation initiale, le paramètre K évolue sur chacune des parties (unité de commande particulière et unité de commande centrale), selon la loi d'évolution (par exemple un incrément de compteur, un temps d'horloge, ou une autre loi plus complexe). On notera que la loi peut aussi être fonction de l'algorithme de hachage hi (qui peut être identifié dans chaque partie par un identifiant ou index, par exemple) et/ou être fonction d'un autre index passé en paramètre dans une trame de données en clair contenue dans un message échangé lors de cette phase de synchronisation.

[0038] Les deux parties font évoluer en interne le paramètre masqué K, par exemple lors de chaque émission du côté de l'unité de commande particulière, et périodiquement du côté de l'unité de commande centrale pour intégrer le fait qu'une trame peut être perdue. L'évolution se fait selon une loi prédéfinie et connue des deux parties. Ceci autorise une ou plusieurs éventuelles pertes de transmission entre l'émetteur, à savoir l'unité de commande électronique particulière et le récepteur, à savoir l'unité de commande électronique centrale. L'homme du métier appréciera que le fait d'avoir le paramètre masqué K qui est un paramètre évolutif permet d'avoir une signature qui change, même si les données passées en clair dans les messages ne changent pas. Dit autrement, la signature est dynamique, ce qui renforce la robustesse des échanges de messages aux attaques, notamment aux attaques par usurpation d'identité.

[0039] Dans d'autres exemples de la mise en œuvre particulière de l'étape 120, on renouvèle la valeur du paramètre commun K, sur l'une et/ou l'autre des parties à l'échange de messages, selon une périodicité prédéterminée ou lors de la survenue d'un contexte particulier.

[0040] De cette manière, l'unité de commande électronique centrale et l'unité de commande électronique particulière connaissent en permanence la valeur du paramètre

commun K, et ce, même à la suite de pertes de messages entre l'unité de commande électronique centrale et l'unité de commande électronique particulière.

[0041] Dans l'étape 130, on utilise l'unité de commande électronique particulière pour générer une empreinte numérique de hachage E de la combinaison du message en clair M et du paramètre commun K, à partir de l'identifiant de sélection d'un algorithme de hachage hi.

[0042] On note que l'unité de commande électronique particulière stocke dans une mémoire l'ensemble des algorithmes de hachage qui sont utilisables, en relation avec un index d'identification de chaque algorithme de hachage.

[0043] On note, par ailleurs, que l'empreinte numérique de hachage E prend en considération le paramètre commun K, alors que ledit paramètre commun K ne fait pas partie du message en clair. Ainsi, on a virtuellement ajouté le paramètre commun K au message en clair M, avant de générer la première empreinte numérique de hachage E.

[0044] Dans une mise en œuvre particulière de l'étape 130, on crypte la première empreinte numérique de hachage E avec une clé privée secrète connue de l'unité de commande électronique particulière.

[0045] Dans un exemple de la mise en œuvre de l'étape 130, on utilise la clé privée secrète d'une paire clé publique/clé privée secrète, en fonction d'un paramètre de sélection de clé asymétrique de cryptage. Dans un autre exemple de mise en œuvre, on assure l'échange de la clé publique contenue dans l'unité de commande particulière, suite à une requête de l'unité de commande centrale vers cette unité de commande particulière.

[0046] En d'autres termes, dans cette mise en œuvre particulière, on utilise un système de chiffrement asymétrique, de type connu en soi, qui utilise deux clés différentes. En particulier, un tel système peut utiliser une paire composée d'une clé privée secrète, qui sert au chiffrement, et d'une clé publique, qui sert à déchiffrer. Toutefois, dans l'invention, on utilise une ou plusieurs paires de clé publique / clé privée.

[0047] Dans l'étape 140, on utilise l'unité de commande électronique particulière pour former une trame de données T qui inclut le message en clair M, l'identifiant de sélection d'un algorithme de hachage hi et la première empreinte numérique de hachage E.

[0048] On note que la trame de données T n'inclut pas le paramètre commun K, alors que la première empreinte numérique de hachage E le prend en considération.

[0049] C'est ce mécanisme de « champ caché » qui permet à la trame de données T de ne pas pouvoir être rejouée par un tiers malveillant qui l'aurait interceptée. En effet, comme le paramètre commun K est différent lors de chaque envoi, il n'est pas possible de rejouer tel quel une trame de données interceptée.

[0050] Dans un exemple de la mise en œuvre particulière de l'étape 130, on insère le paramètre de sélection de clé asymétrique de cryptage dans la trame de données T.

[0051] Dans une mise en œuvre particulière de l'étape 140, on supprime un champ CRC du message en clair M qui contient une séquence CRC (mis pour « check redundancy code », en anglais), avant de former la trame de données T.

[0052] En effet, avec le mécanisme de l'invention, et notamment l'utilisation d'une fonction de hachage, un champ CRC du message en clair, s'il est présent, n'est plus nécessaire, car cette information est redondante.

[0053] Dans l'étape 150, on utilise l'unité de commande électronique particulière pour envoyer la trame de données T à l'unité de commande électronique centrale.

[0054] Dans un exemple de la mise en œuvre particulière de l'étape 110, on génère l'index aléatoire avant l'envoi de chaque trame de données T.

[0055] Dans une mise en œuvre particulière de l'étape 150, on établit une connexion sans fil entre l'unité de commande électronique particulière et l'unité de commande électronique centrale, pour la transmission de la trame de données T. En variante, on peut aussi transmettre la trame de données T en mode non connecté, par exemple en mode de diffusion (« broadcast » en anglais), par exemple dans un message du type connu sous le nom « Advertising » en anglais.

[0056] Dans un exemple, la connexion sans fil est une connexion Bluetooth.

[0057] Dans une autre mise en œuvre particulière, on maintient la connexion sans fil pendant tout ou partie de la mise en œuvre du procédé 100.

[0058] Dans une mise en œuvre, illustrée dans la figure 2, on poursuit le procédé au niveau de l'unité de commande électronique centrale.

[0059] En particulier, dans l'étape 160, on utilise l'unité de commande électronique centrale pour extraire le message en clair M et l'identifiant de sélection d'un algorithme de hachage hi de la trame de données T.

[0060] Dans l'étape 170, on utilise l'unité de commande électronique centrale pour obtenir le paramètre commun K à l'unité de commande électronique centrale et l'unité de

commande électronique particulière, comme il a été dit dans ce qui précède en relation avec l'étape 120 mise en œuvre du côté de l'unité de commande électronique particulière.

[0061] Notamment, le paramètre commun K peut être donné par un compteur, une horloge ou un générateur pseudo-aléatoire. On rappelle que les deux parties, à savoir l'unité de commande électronique centrale et l'unité de commande électronique particulière, font évoluer en interne ce paramètre K selon une loi prédéfinie.

[0062] Dans un exemple de la mise en œuvre particulière de l'étape 170, on renouvelle la valeur du paramètre commun K selon une périodicité prédéterminée ou lors d'un contexte particulier.

[0063] Dans l'étape 180, on utilise l'unité de commande électronique centrale pour générer une empreinte numérique de hachage, ou empreinte de vérification E', de la combinaison du message en clair M et du paramètre commun K, à partir de l'identifiant de sélection d'un algorithme de hachage hi.

[0064] Dans une mise en œuvre particulière de l'étape 180, on cherche dans la base de données, l'algorithme de hachage associé à l'identifiant de sélection d'un algorithme de hachage hi, avant de générer cette empreinte de vérification E'.

[0065] On note que l'unité de commande électronique centrale stocke à cet effet, dans une mémoire l'ensemble des algorithmes de hachage qui sont utilisables, ladite mémoire étant indexée par un index auquel est comparé l'identifiant de sélection d'un algorithme de hachage hi afin de trouver la fonction de hachage à appliquer.

[0066] Dans l'étape 190, on utilise l'unité de commande électronique centrale pour comparer la première empreinte numérique de hachage E reçue de l'unité de commande électronique particulière et l'empreinte numérique de vérification E' calculée dans l'unité de commande électronique centrale.

[0067] Dans une mise en œuvre particulière de l'étape 190, on décrypte l'empreinte numérique de hachage E reçue avec une clé publique de l'unité de commande électronique particulière qui est associée à la clé privée secrète l'unité de commande électronique particulière.

[0068] Dans un exemple de la mise en œuvre particulière de l'étape 190, on utilise la clé publique de la paire clé publique/clé privée secrète, en fonction du paramètre de sélection de clé asymétrique de cryptage que l'on extrait de la trame de données T.

[0069] Dans l'étape 200, l'unité de commande électronique centrale peut ou non utiliser les données de mesure du message en clair M en fonction du résultat de la comparaison.

[0070] Ainsi, si la première empreinte numérique E et la deuxième empreinte numérique E', sont égales, alors on peut garantir que l'identité de l'unité de commande électronique particulière n'a pas été usurpée et que l'unité de commande électronique centrale peut prendre en considération les données de mesures envoyées par l'unité de commande électronique particulière. A défaut, ces données sont ignorées par l'unité de commande électronique centrale.

[0071] L'invention peut faire l'objet de nombreuses variantes et applications autres que celles décrites ci-dessus. En particulier, sauf indication contraire, les différentes caractéristiques structurelles et fonctionnelles de chacune des mises en œuvre décrite ci-dessus ne doivent pas être considérées comme combinées et/ou étroitement et/ou inextricablement liées les unes aux autres, mais au contraire comme de simples juxtapositions. En outre, les caractéristiques structurelles et/ou fonctionnelles des différents modes de réalisation décrits ci-dessus peuvent faire l'objet en tout ou partie de toute juxtaposition différente ou de toute combinaison différente.

Revendications

[Revendication 1] Procédé (100) pour prévenir l'usurpation d'identité d'une unité de commande électronique particulière d'un véhicule automobile, lorsque l'unité de commande électronique particulière envoie un message en clair (M), qui contient des données de mesure, à une unité de commande électronique centrale du véhicule automobile, l'unité de commande électronique centrale comprenant au moins une base de données qui stocke au moins un tuple de valeurs, formé d'un identifiant de sélection d'un algorithme de hachage (hi) et d'un algorithme de hachage, le procédé comprenant les étapes suivantes, mises en œuvre au niveau de l'unité de commande électronique particulière :

- générer (110) un identifiant de sélection d'un algorithme de hachage (hi),
- obtenir (120) au moins un paramètre évolutif (K) commun à l'unité de commande électronique centrale et l'unité de commande électronique particulière,
- générer (130) une première empreinte numérique de hachage (E) de la combinaison du message en clair (M) et du paramètre commun (K), à partir de l'identifiant de sélection d'un algorithme de hachage (hi),
- former (140) une trame de données (T) qui inclut le message en clair (M), l'identifiant de sélection d'un algorithme de hachage (hi) et la première empreinte numérique de hachage (E), et
- envoyer (150) la trame de données (T) à l'unité de commande électronique centrale.

[Revendication 2] Procédé selon la revendication 1, comprenant en outre les étapes suivantes, mises en œuvre au niveau de l'unité de commande électronique centrale, en réponse à la réception de la trame de données (T) :

- extraire (160) le message en clair (M) et l'identifiant de sélection d'un algorithme de hachage (hi) de la trame de données (T),
- obtenir (170) le paramètre évolutif (K) commun à l'unité de commande électronique centrale et l'unité de commande électronique particulière,
- générer (180) une deuxième empreinte numérique de hachage (E') de la combinaison du message en clair (M) et du paramètre commun (K), à partir de l'identifiant de sélection d'un algorithme de hachage (hi),
- comparer (190) la première empreinte numérique et la deuxième empreinte numérique, et

- utiliser (200) les données de mesure du message en clair (M) en fonction de la comparaison.

[Revendication 3] Procédé selon l'une quelconque des revendications 1 à 2, comprenant en outre les étapes suivantes :

- crypter, par l'unité de commande électronique particulière, la première empreinte numérique de hachage (E) avec une clé privée secrète l'unité de commande électronique particulière, avant de former la trame de données (T), et

- décrypter, par l'unité de commande électronique particulière, la première empreinte numérique de hachage (E) avec une clé publique de l'unité de commande électronique particulière qui est associée à la clé privée secrète l'unité de commande électronique particulière, avant de comparer la première empreinte numérique et la deuxième empreinte numérique.

[Revendication 4] Procédé selon la revendication 3, dans lequel :

- on utilise la clé privée secrète d'une paire clé publique/clé privée secrète, en fonction d'un paramètre de sélection de clé asymétrique de cryptage que l'on insère dans la trame de données (T), et

- on utilise la clé publique de la paire clé publique/clé privée secrète, en fonction du paramètre de sélection de clé asymétrique de cryptage que l'on extrait de la trame de données (T).

[Revendication 5] Procédé selon l'une quelconque des revendications 1 à 4, comprenant en outre l'étape suivante :

- supprimer, par l'unité de commande électronique particulière, un champ CRC du message en clair (M) qui contient une séquence CRC, avant de former la trame de données (T).

[Revendication 6] Procédé selon l'une quelconque des revendications 1 à 5, comprenant en outre l'étape suivante :

- chercher, par l'unité de commande électronique centrale, dans la base de données, l'algorithme de hachage associé à l'identifiant de sélection d'un algorithme de hachage (hi), avant de générer la deuxième empreinte numérique de hachage (E).

[Revendication 7] Procédé selon l'une quelconque des revendications 1 à 6, dans lequel, au niveau de l'unité de commande électronique particulière, l'identifiant de sélection d'un algorithme de hachage (hi) est un index aléatoire qui est associé à une position spécifique

dans une liste prédéterminée d'algorithmes de hachage, la liste étant stockée dans une mémoire de l'unité de commande électronique particulière.

[Revendication 8] Procédé selon la revendication 7, dans lequel on génère l'index aléatoire avant l'envoi de chaque trame de données (T).

[Revendication 9] Procédé selon l'une quelconque des revendications 1 à 8, dans lequel on choisit le paramètre commun (K) parmi : un compteur, un générateur pseudo-aléatoire et une horloge.

[Revendication 10] Procédé selon la revendication 9, dans lequel, au niveau l'unité de commande électronique particulière et au niveau de l'unité de commande électronique centrale, on renouvelle la valeur du paramètre commun (K) selon une périodicité prédéterminée.

[Fig. 1]

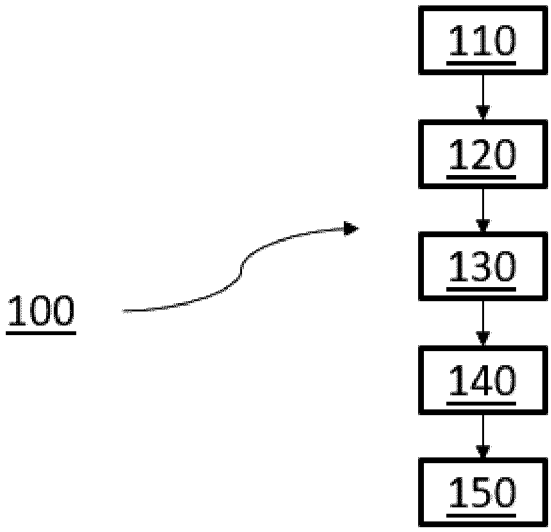

FIG. 1

[Fig. 2]

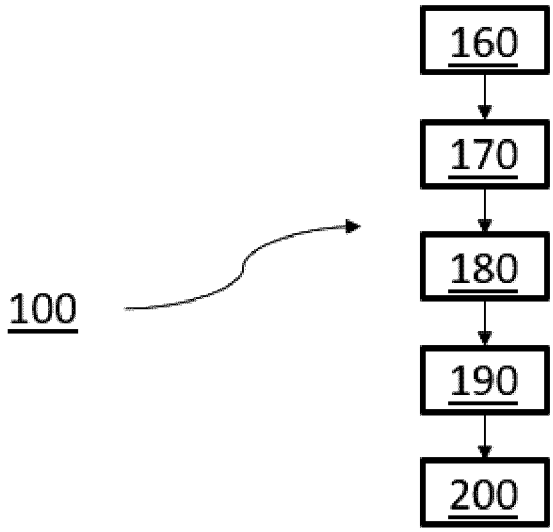

FIG. 2

[Fig. 3]

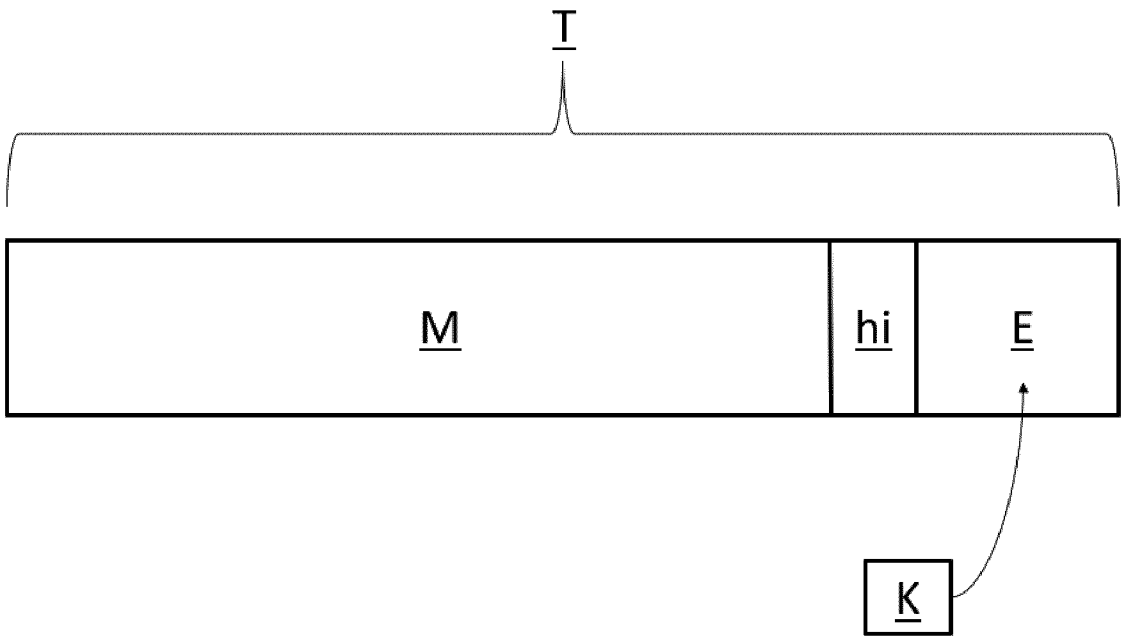

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2022/068242

A. CLASSIFICATION OF SUBJECT MATTER

G06F 13/42(2006.01)i; ***H04L 12/413***(2006.01)i; ***H04L 12/40***(2006.01)i; ***H04L 9/40***(2022.01)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; 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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	"IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture ; IEEE Std 1609.0-2019 (Revision of IEEE Std 1609.0-2013)" *IEEE STANDARD, IEEE, PISCATAWAY, NJ USA,* 10 April 2019 (2019-04-10), pages 1-106, [retrieved on 2019-04-10] DOI: 10.1109/IEEESTD.2019.8686445 XP068150197 section 5.13.5.2	1-10
A	HALABI JOE ET AL. "A Lightweight Synchronous Cryptographic Hash Chain Solution to Securing the Vehicle CAN bus" *2018 IEEE INTERNATIONAL MULTIDISCIPLINARY CONFERENCE ON ENGINEERING TECHNOLOGY (IMCET), IEEE,* 14 November 2018 (2018-11-14), pages 1-6 DOI: 10.1109/IMCET.2018.8603057 XP033493209 abstract abstract, sections I-IV	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	Date of mailing of the international search report
12 October 2022	**24 October 2022**

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

Authorized officer
Bertolissi, Edy
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	PARK CHOL HYUN ET AL. "A Secure Communication Method for CANBus" *2021 IEEE 11TH ANNUAL COMPUTING AND COMMUNICATION WORKSHOP AND CONFERENCE (CCWC), IEEE,* 27 January 2021 (2021-01-27), pages 773-778 DOI: 10.1109/CCWC51732.2021.9376166 XP033887727 abstract section IV	1-10
A	Tobias Islinger. "Autosar SecOC for CAN FD" *CAN Newsletter,* 31 March 2017 (2017-03-31), Retrieved from the Internet: https://can-newsletter.org/uploads/media/raw/d904c 90ba599c668e9758ae558dcb845.pdf [retrieved on 2022-03-11] XP055900301 figures 2, 3	1-10
A	FOUQUE PIERRE-ALAIN ET AL. On the Security of the CCM Encryption Mode and of a Slight Variant, ADVANCES IN DATABASES AND INFORMATION SYSTEMS; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER INTERNATIONAL PUBLISHING, CHAM, PAGE(S) 411 - 428 , 03 June 2008 (2008-06-03), ISBN: 978-3-319-10403-4. XP047503065 abstract section 3	1-10
A	Praneeth Kemparaj ET AL. "Understanding CTR with CBC-MAC Protocol (CCMP) AES-CCMP in depth" 02 May 2020 (2020-05-02), Retrieved from the Internet: https://praneethwifi.in/2020/05/02/ctr-with-cbc-ma c-protocol-ccmp-aes-ccmp/ [retrieved on 2022-06-02] XP055927591 abstract figures 2, 12	1-10

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2022/068242

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

INV. G06F13/42 H04L12/413 H04L12/40 H04L9/40

ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	"IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture ; IEEE Std 1609.0-2019 (Revision of IEEE Std 1609.0-2013)", IEEE STANDARD, IEEE, PISCATAWAY, NJ USA, 10 avril 2019 (2019-04-10), pages 1-106, XP068150197, DOI: 10.1109/IEEESTD.2019.8686445 ISBN: 978-1-5044-5493-3 [extrait le 2019-04-10] Section 5.13.5.2 ----- -/--	1-10

[x] Voir la suite du cadre C pour la fin de la liste des documents

[ ] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent;; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent;; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
12 octobre 2022	24/10/2022

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Bertolissi, Edy

1

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	HALABI JOE ET AL: "A Lightweight Synchronous Cryptographic Hash Chain Solution to Securing the Vehicle CAN bus", 2018 IEEE INTERNATIONAL MULTIDISCIPLINARY CONFERENCE ON ENGINEERING TECHNOLOGY (IMCET), IEEE, 14 novembre 2018 (2018-11-14), pages 1-6, XP033493209, DOI: 10.1109/IMCET.2018.8603057 abrégé Abrege, Section I-IV ----- PARK CHOL HYUN ET AL: "A Secure Communication Method for CANBus", 2021 IEEE 11TH ANNUAL COMPUTING AND COMMUNICATION WORKSHOP AND CONFERENCE (CCWC), IEEE, 27 janvier 2021 (2021-01-27), pages 773-778, XP033887727, DOI: 10.1109/CCWC51732.2021.9376166 abrégé Section IV ----- Tobias Islinger: "Autosar SecOC for CAN FD", CAN Newsletter, 31 mars 2017 (2017-03-31), XP055900301, Extrait de l'Internet: URL:https://can-newsletter.org/uploads/media/raw/d904c90ba599c668e9758ae558dcb845.pdf [extrait le 2022-03-11] figures 2, 3 ----- FOUQUE PIERRE-ALAIN ET AL: "On the Security of the CCM Encryption Mode and of a Slight Variant", 3 juin 2008 (2008-06-03), ADVANCES IN DATABASES AND INFORMATION SYSTEMS; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER INTERNATIONAL PUBLISHING, CHAM, PAGE(S) 411 - 428, XP047503065, ISBN: 978-3-319-10403-4 abrégé Section 3 ----- -/--	1-10 1-10 1-10

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2022/068242

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	Praneeth Kemparaj ET AL: "Understanding CTR with CBC-MAC Protocol (CCMP) AES-CCMP in depth", , 2 mai 2020 (2020-05-02), XP055927591, Extrait de l'Internet: URL:https://praneethwifi.in/2020/05/02/ctr-with-cbc-mac-protocol-ccmp-aes-ccmp/ [extrait le 2022-06-02] abrégé figures 2, 12 -----	1-10

1