(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 963 503**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **11 56919**

(51) Int Cl[8] : ***H 02 K 11/00*** *(2006.01)*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 28.07.11.

(30) **Priorité :** 30.07.10 DE 102010038703.7.

(43) **Date de mise à la disposition du public de la demande :** 03.02.12 Bulletin 12/05.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *ROBERT BOSCH GMBH* — DE.

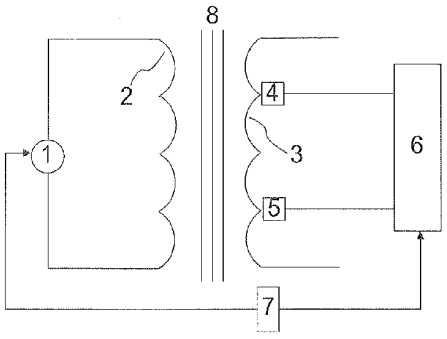
(72) **Inventeur(s) :** SHOKROLLAHI JAMSHID et KRAMER SIMON.

(73) **Titulaire(s) :** ROBERT BOSCH GMBH.

(74) **Mandataire(s) :** CABINET HERRBURGER.

(54) PROCEDE POUR GENERER UNE PAIRE REQUETE/REPONSE DANS UNE MACHINE ELECTRIQUE ET MACHINE ELECTRIQUE METTANT EN OEUVRE LE PROCEDE.

(57) Procédé pour générer une paire requête/réponse dans une machine électrique (1) comme base d'une authentification. La machine électrique comporte au moins un stator (2) et un rotor (3). La requête est un signal de tension ou d'intensité qui produit une induction entre le rotor et le stator et la réponse à la requête est une grandeur dépendant de l'induction produite.



FR 2 963 503 - A1

Domaine de l'invention

La présente invention se rapporte à un procédé pour générer une paire requête/réponse d'une machine électrique comme élément de base d'une authentification, la machine électrique ayant au moins un stator et au moins un rotor.

L'invention se rapporte également à une machine électrique comportant au moins un stator et un rotor et mettant en œuvre un tel procédé.

Etat de la technique

Pour se protéger contre les imitations ou les modules techniques contrefaits, les clients ne peuvent, par exemple, souhaiter pouvoir authentifier en toute sécurité un module ou un élément pour vérifier qu'il s'agit d'un produit d'origine. Un procédé relativement récent utilisé pour garantir l'authenticité est fondé sur l'utilisation de fonctions physiques dites « non clonables ». Ces fonctions sont désignées par leur abréviation de fonction PUF.

Le document US 2009/0083833 décrit comment implémenter les fonctions par un module PUF supplémentaire pour une notification d'une série de composants électroniques tels que des composants FPGA, RFID, ASIC. Le document US 7,681,103 décrit comment générer de manière fiable une valeur spécifique d'un composant en utilisant les fonctions PUF.

Exposé et avantages de l'invention

La présente invention a pour but de développer un procédé du type défini ci-dessus et a ainsi pour objet un tel procédé caractérisé en ce qu'on génère comme requête un signal de tension ou d'intensité qui produit une induction entre le rotor et le stator, et on définit comme réponse, une grandeur dépendant de l'induction produite.

L'invention a également pour objet une machine électrique comportant au moins un stator et au moins un rotor, caractérisée en ce qu'elle comporte des moyens pour générer comme requête, un signal de tension ou d'intensité produisant une induction entre le rotor et le stator et des moyens pour déterminer, comme réponse, une grandeur dépendant de l'induction produite.

La présente invention permet ainsi une authentification, d'une manière particulièrement simple et économique, d'une machine électrique ou d'un appareil comportant une machine électrique ou encore d'un appareil relié à une machine électrique et cela sur le fondement de l'induction dans la machine électrique. Par comparaison à d'autres procédés d'authentification, cela permet d'éviter l'utilisation de composants de circuit, supplémentaires, coûteux notamment d'un module PUF supplémentaire. Pour certains développements de l'invention, il suffit de composants économiques et qui peuvent s'intégrer simplement dans les systèmes existants. Les méthodes et les procédés pour contourner de telles solutions, par exemple en recueillant les signaux ou en interposant des circuits sont des moyens compliqués, coûteux et les manipulations sont fréquemment décelables.

Le procédé selon l'invention peut s'appliquer d'une manière particulièrement simple et économique si la réponse est une grandeur dépendant de la tension dans le rotor ou le stator de la machine électrique. Pour cela, selon un développement préférentiel, on détecte, par exemple, la tension entre deux points d'une bobine du rotor ou d'une bobine du stator par l'intermédiaire de deux contacts et on traite la tension obtenue.

D'une manière particulièrement avantageuse car cela permet d'utiliser des informations supplémentaires et d'avoir ainsi un procédé plus résistant, on utilise non seulement une valeur de tension, c'est-à-dire par exemple l'amplitude de la tension mais aussi l'évolution chronologique de la tension. Sous forme de circuit, se développement avantageux peut se réaliser par exemple par une unité de mesure supplémentaire qui mesure la tension (son amplitude et le cas échéant son évolution dans le temps) et traite ce signal.

Le signal de requête peut être généré, de préférence, par un générateur spécial de signal équipant la machine électrique. Ce générateur de signal peut ainsi se réaliser d'une manière économique et le procédé être optimisé.

Selon le développement avantageux, on détermine la position du rotor en exécutant le procédé, par exemple, à l'aide d'un capteur de position. Cela permet de définir de manière optimale les

conditions pour générer la paire (ou binôme) requête/réponse et de minimiser l'influence de la positon actuelle du rotor sur le résultat.

Selon un développement particulièrement sûr, on génère la requête et on détermine la réponse de manière déclenchée par les signaux du capteur de position de façon que le rotor se trouve dans une position déterminée.

En plus ou en variante du capteur de position, on peut également déclencher manuellement, par exemple pour économiser le coût d'un capteur prévu le cas échéant spécialement à cet effet.

Pour cela, on prévoit par exemple deux points sur le rotor et le stator avec des repères. Un opérateur pourra alors juxtaposer les marques (points) et avoir une position définie du rotor puis déclencher le procédé de mesure.

De manière avantageuse, on détermine la réponse pour une authentification en ce qu'avec une réponse déterminée et une clé publique on vérifie une réponse préalablement signée avec une clé secrète. On a ainsi un procédé simple à réaliser et cela de manière économique. Il en est de même de l'appareil ou du véhicule équipé de la machine électrique ou de la machine électrique elle-même qui pourrait être authentifiée, par exemple par un client, en ce qu'il disposera d'une clé publique et une réponse signée avec la clé secrète fournie avec la machine électrique ou avec l'appareil ou le véhicule.

Selon un autre développement avantageux, on génère une clé secrète avec la paire requête/réponse (pour cela on peut utiliser l'ensemble de la paire requête/réponse ou seulement la réponse) et on pourra vérifier avec un message d'authentification. On peut ainsi réaliser avec des moyens relativement réduits, un chemin de communication sécurisé entre la machine électrique et un appareil relié à celle-ci.

Dessins

La présente invention sera décrite ci-après de manière plus détaillée pour un procédé générant une paire requête/réponse dans une machine électrique en vue de son authentification ainsi qu'une machine électrique appliquant ce procédé et représentée dans les dessins annexés dans lesquels :

- la figure 1 montre un exemple de réalisation d'une machine électrique équipée d'un dispositif pour générer ou déterminer une paire requête/réponse,
- la figure 2 montre la courbe de tension schématique (fonction V(t), tension V en fonction du temps t),
- la figure 3 montre schématiquement un procédé pour déterminer ou pour traiter une courbe de tension,
- la figure 4 montre schématiquement l'exécution d'un procédé d'authentification d'une machine électrique,
- la figure 5 montre une machine électrique avec un chemin de communication garanti vers un appareil relié, et
- la figure 6 montre la structure schématique d'un procédé pour réaliser un chemin de communication sécurisé entre une machine électrique et un appareil relié à celle-ci.

Description de mode de réalisation de l'invention

Les développeurs et les fabricants de produits de qualité très élevée rencontrent souvent le problème de la piraterie et de la contrefaçon des produits. Souvent des sommes considérables sont investies dans la recherche et le développement de tels produits mais qui pourront toutefois être copiés illégalement d'une manière relativement simple. Le problème ne se limite pas aux fabricants des produits mais concerne souvent les acheteurs de ces produits à cause de la très mauvaise qualité des produits. Pour les fabricants et les clients il est de ce fait souhaitable de pouvoir authentifier les produits en toute sécurité. La description suivante concerne une machine électrique permettant de générer une paire ou binôme requête/réponse utilisée pour authentifier une machine électrique ou un appareil équipée d'une telle machine électrique. On utilise pour cela l'effet inductif dans la machine électrique comme fondement d'une fonction physique non clonable (fonction PUF). L'expression « machine électrique » désigne, en particulier, les moteurs électriques et les génératrices. L'invention sera, en partie, décrite à l'aide de moteurs électriques mais s'applique en principe tout aussi bien à d'autres machines électriques rotatives.

Pour protéger des ensembles techniques contre la copie ou l'imitation, le client peut par exemple souhaiter d'authentifier en

toute sécurité un module ou produit comme produit original. Un procédé utilisable pour garantir l'authentification peut se faire en utilisant des fonctions physiques non clonables (fonctions PUF).

Une fonction PUF s'appuie sur la structure physique d'une pièce ou d'un composant utilisant de nombreux paramètres aléatoires définis par la fabrication exacte des différents composants. Pour utiliser les fonctions PUF pour une authentification, on utilise le fait que la variation par exemple de paramètres géométriques et/ou spécifiques aux matériaux dans un système physique, au moment de sa fabrication, donne des réponses déterminées à un stimulus physique déterminé c'est-à-dire une paire ou un binôme requête/réponse (encore appelée binôme CRP) caractéristique d'un certain produit dans une ligne de fabrication. Le stimulus est appelé requête et la réaction de la fonction PUF est appelée réponse. Pour utiliser une fonction PUF pour l'authentification, on utilise des procédés cryptographiques décrits de manière explicite dans la documentation par exemple dans les documents US 2009/0083833 et US 7.681.103.

La présente invention est fondée sur une grandeur dépendant de l'induction d'une machine électrique pour la fonction PUF. Les paramètres aléatoires nécessaires à l'authentification à l'aide de la fonction PUF pour la fabrication d'une machine électrique sont par exemple la variation de propriétés géométriques (disposition, dimension) du stator et du rotor, par exemple la répartition spatiale des enroulements des bobines ou une légère asymétrie du rotor et du stator.

La figure 1 montre un exemple de réalisation pour générer une paire requête/réponse d'une machine électrique. La structure présentée permet de déclencher la fonction PUF (requête) et de l'exploiter (réponse). Dans cette réalisation pratique une bobine de la machine électrique (ici la bobine du stator 2) est reliée à une source de signal 1. En appliquant un signal fixe de tension ou d'intensité par la source de signal 1 comme requête, on crée un effet inductif entre la bobine de stator 2 et la bobine de rotor 3. Cet effet est mesuré à la figure 1 en prenant la tension entre deux points 4 et 5 de la bobine de rotor 3. La différence de tension (par exemple l'amplitude et la répartition dans le temps) est reçue par une unité de mesure 6 qui traite cette informa-

tion. L'unité de mesure 6 fournit la réponse à la requête définie par le générateur de signal 1. Comme les conditions pour générer une paire requête/réponse sont parfaitement définies, la position de la bobine 3 du rotor (ou la position du rotor en rotation) est enregistrée par un capteur de position 7 qui fournit, à la fois, au générateur de signal 1 et à l'unité de mesure 6 pour une position prédéfinie, déterminée du rotor, un signal et peut ainsi générer le signal ou déclencher la mesure. En plus ou en variante du capteur de position 7, on peut également produire manuellement ce déclenchement, par exemple, pour faire l'économie d'un capteur prévu, le cas échéant à cet effet. Pour cela, on peut définir des repères, par exemple deux points du rotor et du stator. Un opérateur peut placer alors les deux repères (points) l'un à côté de l'autre et avoir une position définie du rotor pour déclencher ensuite le procédé de mesure. La référence 8 à la figure 1 désigne schématiquement les lignes du champ magnétique.

On peut modifier la structure de principe de la figure 1 en intervertissant le rôle du stator et du rotor ou encore en ce qu'on utilise les deux bobines présentées du rotor ou en variante celles du stator. On peut également envisager de mesurer la courbe de tension dans la bobine reliée au générateur de signal.

Les points 4 et 5 entre lesquels on mesure la différence de tension comme base de la valeur de la réponse sont des points aléatoires (mais fixés pour cette machine électrique) sur une bobine. Pour disposer d'un nombre plus grand de paires requête/réponse, on peut augmenter le nombre des paires de points. La réponse d'une certaine paire à une certaine requête par le générateur de signal 1 définit à chaque fois la paire requête/réponse.

La source de signal 1 est, de préférence, une source de tension qui peut, par exemple, générer des impulsions de tension de longueur variable et d'amplitude fixe. En déclenchant par l'information du capteur de position ou, selon une variante de réalisation, par l'actionnement manuel pour que le rotor soit dans la position correcte, le générateur de signal 1 génère un signal par exemple un pic delta de tension. Le signal est formé de préférence spécialement pour générer la paire requête/réponse et le procédé s'applique, de préférence, en dehors

du mode de fonctionnement normal. La source de signal 1 est prévue, de préférence, spécialement pour le procédé d'authentification. Il en est de même pour l'appareil de mesure 6. Si du fait d'autres applications disposent de ressources appropriées, on pourra naturellement les utiliser. Il faut éventuellement prévoir, en plus, un capteur de position 7 ; si les capteurs correspondants existent déjà, on pourra les utiliser.

La figure 2 montre schématiquement le chronogramme V(t) de la différence de tension V, mesurée entre les points 4 et 5 sur la bobine 3 du rotor après une impulsion de tension appliquée par le générateur de signal 1 à la bobine de stator 2. La référence V désigne l'axe des tensions et la référence (t) l'axe du temps dans le diagramme. La fonction V(t) à décroissance par exemple exponentielle donne l'amplitude et son évolution en fonction de l'action de l'induction entre le rotor et le stator (suivant la figure 1, entre les bobines 2 et 3 – y compris les noyaux des bobines) ainsi que leurs caractéristiques de résistance, ce qui dépend des particularités de fabrication décrites (géométrie, dimensions, matières). Comme décrits, ces paramètres varient entre les différents appareils de construction par ailleurs identiques et ainsi la fonction V(t) peut servir de base à une identification univoque.

La fonction V(t) de la figure 2 permet de transformer le signal de mesure reçu par l'unité de mesure 6 de la figure 1 en une chaîne numérique. Un ordinogramme donné à titre d'exemple et qui peut s'appliquer pour mesurer ou donner une image des propriétés de cette fonction dépendant du temps est présenté à la figure 3. On suppose pour cela que le système comporte un tableau de mémoire (c'est-à-dire dans la machine électrique ou de manière associée à la machine électrique) pour N entrée possible ainsi qu'un compteur. On a également enregistré des valeurs de seuil (i) pour tous les états possibles de valeurs de seuil i=0...N.

Dans l'étape 31, on lance le compteur de temps.

Dans l'étape 32, on met la valeur de départ de i à 0.

Dans l'étape 33, on vérifie que (i) est inférieur à N. Dans l'affirmative, on passe à l'étape 34, dans la négative, on passe à l'étape 38.

Dans l'étape 34, on lit la valeur de mesure actuelle V(t) pour (i) inférieur à N.

Dans l'étape 35, on vérifie si la valeur de V(t) est inférieure au seuil du paramètre actuel (i). Si cela est le cas, on passe à l'étape 36. Dans la négative, le procédé passe à l'étape 34 et de celle-ci à l'étape 35 et cela jusqu'à ce que la condition V(t) inférieure à valeur de seuil (i) est remplie puis on passe à l'étape 36.

Dans l'étape 36, on inscrit la valeur du compteur de temps dans la position (i) parmi les N positions de la mémoire.

Dans l'étape 37, on incrémente la valeur (i) d'une unité. Dans l'étape 37, le procédé passe à l'étape 33.

Dans l'étape 38, on assemble les N valeurs de temps de la mémoire (concaténation) et on émet ces valeurs.

Le signal mesuré est comparé en permanence à l'entrée actuelle c'est-à-dire la valeur de seuil (i). Si la valeur descend en dessous du seuil, on enregistre l'instant actuel dans un réseau « temps » et la variable « i » indique l'entrée suivante du tableau avec les valeurs de seuil. Lorsque toutes les entrées sont traitées (i=N) on émet la chaîne (concaténation) des entrées du tableau « temps » et on utilise la chaîne de signes qui caractérise la machine électrique comme réponse de la fonction PUF à la requête.

Pour diminuer les effets négatifs du bruit et augmenter la sécurité du procédé, on peut traiter le signal de réponse en utilisant un extracteur en logique flou. Des exemples d'extracteurs flous se trouvent, par exemple dans le document : Yevgeniy Dodis, Jonathan Katz, Leonid Reyzin : « Robust fuzzy extractors and authenticated key agreement from close secrets », Advances in Cryptology-CRYPTO '06, volume 4117 Lecture Notes, Computer Science, pages 232-250, Springer Verlag, 2006.

Dans un mode de réalisation particulier à partir des propriétés de la fonction PUF, la machine électrique peut appliquer elle-même les fonctions d'induction pour l'identification. Si, dans cet exemple de réalisation, on veut, par exemple, vérifier si la machine électrique provient d'un certain constructeur. La figure 4 montre un schéma correspondant.

Dans la première étape 41, on génère le stimulus physique (tension, intensité) comme requête, comme par exemple à la figure 1.

La réponse de la fonction PUF à l'effet inductif de ce stimulus est reçue dans l'étape 42 pour être traitée, par exemple, sous la forme d'une chaîne numérique, comme cela a été décrit à la figure 2. On a ainsi une paire requête/réponse CRP dans les étapes 41 et 42.

Dans la troisième étape 43, on signe la réponse avec la clé privée (clé secrète) du constructeur. Cela peut se faire de façon interne dans l'appareil dans la mesure où l'on dispose des ressources de calcul appropriées. Cela peut également se faire de manière externe. La signature ainsi obtenue est appliquée dans ou à la machine électrique ou dans ou sur l'appareil équipé de la machine électrique. Cela peut se faire par exemple dans une mémoire spéciale ou sous la forme d'un code à barres, appliqué à la machine électrique ou à l'appareil qu'elle équipe. Comme exemple pratique, on a par exemple un moteur électrique installé dans un outil électrique et la signature peut être appliquée sur l'outil électrique. Selon un autre exemple, le moteur électrique est installé dans un véhicule et la signature sera enregistrée dans la mémoire du véhicule. Avant de signer la réponse, on peut, selon un développement particulier, l'adapter dans un code approprié de correction d'erreur (code ECC).

Les étapes 41-43 peuvent être appliquées de préférence chez le constructeur des machines électriques ou par exemple dans un atelier autorisé, avec un nombre limité de personnes autorisées.

Dans les étapes 44-46, on effectue l'authentification proprement dite de la machine électrique, par exemple par le client ou la douane pour contrôler l'appareil ou la machine électrique, tant à l'identité correcte du constructeur. Pour cela, le contrôleur applique dans l'étape 44, la requête, c'est-à-dire le stimulus physique. Cela peut se faire, par exemple, en ce qu'il utilise un élément d'actionnement approprié ou qu'il applique à l'entrée de signal, le signal approprié pour déclencher le stimulus ou qu'il applique directement le stimulus à la machine électrique. Le signal correct du stimulus sera déclenché auto-

matiquement où la valeur a été fixée dans l'étape 41, par exemple en étant enregistrée en mémoire ou fournie avec la signature.

La requête de l'étape 44 génère une réponse dans la machine électrique. Cette réponse est déterminée dans l'étape 45 par le contrôleur. Le traitement de la réponse se fait, par exemple, comme dans l'étape 42. Avec cette réponse et la clé publique du fabricant de la machine électrique, on peut vérifier la signature que l'on obtient lors (par exemple la signature appliquée ou enregistrée en mémoire) et vérifier l'origine de la machine électrique dans l'étape 46.

Globalement, selon cet exemple de réalisation, on pourra ainsi authentifier une machine électrique. Cela peut également s'utiliser pour authentifier un véhicule entraîné au moins en partie par des moyens électriques ou encore un outil électrique. Les étapes 44-46 peut être appliquées le cas échéant aussi souvent que possible pour les authentifications, ce qui est indiqué par un trait en pointillés avec une flèche allant de l'étape 46 à l'étape 44.

La figure 5 montre une construction donnée à titre d'exemple pour utiliser l'induction dans une machine électrique avec des fonctions non clonables reposant sur une caractéristique physique pour établir un chemin de communication en sécurité entre une machine électrique et un appareil relié à celle-ci, par exemple entre un moteur électrique installé dans un véhicule et un appareil de commande relié à celui-ci.

La figure 5 montre la machine électrique 51, par exemple un moteur électrique, installée dans un véhicule et un appareil 52 relié électriquement, par exemple un appareil de commande.

La machine électrique est associée à un extracteur flou 53 et une unité de calcul et de vérification MAC 54. Des exemples d'extracteurs flous sont connus selon la documentation évoquée précédemment. Les unités 53 et 54 peuvent être intégrées par exemple dans un circuit électrique, le cas échéant avec d'autres fonctions cryptographiques. Les unités 53 et 54 peuvent faire partie de la machine électrique ou être associées de manière externe à celle-ci.

Une liaison de communication permet à l'appareil 52 équipé de la machine électrique 51 d'émettre des informations (55).

Comme décrite à l'aide de la figure 1, la machine électrique 51 de la figure 5 est équipée de moyens non présentés de manière explicite (par exemple associés schématiquement à l'unité 53 permettant de définir une paire requête/réponse fondée sur une induction dans la machine électrique 51. Pour cela, on génère une requête (portant schématiquement la référence 56 à la figure 5 et on produit ainsi une induction. La réponse de la machine électrique 51 est indiquée schématiquement sous la référence 57. En fonction de la paire requête/réponse (ou en fonction de la réponse) l'extracteur flou 53 génère une clé secrète comme cela est précisé à la figure 6 et envoie 58 cette clé à l'unité de calcul et de vérification MAC 54. Une information sécurisée (complément d'authentification) avec la même clé secrète dans l'appareil 52 et qui a été reçue 55 par la machine électrique 51 pourra alors être vérifiée. Le résultat de la vérification se poursuit, par exemple, par le traitement de l'information par la machine électrique 59 ou le rejet de l'information.

Si la machine électrique 51 de la figure 5 utilise le chemin sécurisé décrit pour communiquer avec l'appareil relié 52, on est ainsi confirmé avec une sécurité élevée que les signaux reçus proviennent effectivement de l'appareil et n'ont pas été manipulés entretemps.

La figure 6 montre schématiquement le déroulement d'un procédé d'établissement d'un chemin de communication sécurisé entre une machine électrique et un appareil relié à celle-ci.

Dans l'étape 61, on détermine la fonction PUF et la paire CRP (paire requête/réponse) comme cela par exemple a été décrit à la figure 1 pour générer à partir de là une clé secrète. La génération de la clé peut se faire de manière interne, par exemple, dans l'appareil ou dans la machine électrique ou encore de manière externe. Pour l'exemple d'un moteur électrique équipant un véhicule relié à un appareil de commande, on peut avantageusement générer la clé directement à l'aide de l'appareil de commande car les appareils de commande ont habituellement et de façon normale les circuits nécessaires. La façon d'utiliser la fonction PUF pour générer à partir de là, par exemple avec un extracteur flou, une clé cryptographique, sont des procédés décrits par exemple dans le document : Yevgeniy Dodis, Jonathan Katz, Leonid

Reyzin, Robust fuzzy extractors and authenticated key agreement from close secrets, Advances in Cryptology-CRYPTO '06, volume 4117 Lecture Notes, Computer Science, pages 232-250, Springer Verlag, 2006 ou US 2009/0083833 A1.

La clé secrète ainsi générée est enregistrée selon l'étape 62 dans l'appareil ou dans une mémoire associée à celui-ci, de préférence dans une zone de mémoire cryptographique, protégée par des circuits spéciaux et dans lesquels on ne peut simplement lire la clé.

Les étapes 61 et 62 constituent, en quelque sorte, l'initialisation du procédé et sont exécutées, par exemple dans l'atelier du constructeur. L'authentification, c'est-à-dire la communication sécurisée, se fait par un chemin de communication sécurisé entre les machines électriques et un appareil relié à celles-ci. Cette opération se fait dans les étapes 63-67.

Pour authentifier l'appareil, celui-ci envoie une information à la machine électrique (étape 63). L'information est codée avec la clé secrète ou elle est, de préférence, munie d'une étiquette d'identité qui ne peut être obtenue qu'avec la clé secrète. Une telle étiquette d'identité peut être réalisée de manière cryptographique avec des procédés connus en utilisant, par exemple, le code d'authentification de message (code MAC). L'étiquette d'identification est générée également par l'appareil relié à la machine électrique, c'est-à-dire que l'information a été codée par celui-ci ; pour cela, l'appareil comporte les moyens cryptographiques et les ressources de circuits appropriés.

Dans un exemple de réalisation préférentielle (machine électrique = moteur électrique équipant un véhicule, appareil = appareil de commande) l'authentification de l'appareil de commande (faite par exemple par l'envoi d'une information avec l'étiquette d'identification) peut se faire lors de la mise en œuvre ou de l'opération inverse de l'appareil de commande, par exemple au démarrage du moteur ou dans l'appareil de commande et/ou en fin de course du moteur.

Dans l'étape 64, la machine électrique génère d'elle-même la réponse prévue liée à l'application du signal de requête (comme cela a été décrit à la figure 5 pour générer à partir de là, par exemple à l'aide d'un extracteur flou (figure 5) la clé secrète comme à l'étape 61. Cette

clé secrète est ainsi la même que celle qui a été enregistrée dans l'étape 62.

Par l'unité de vérification MAC, la machine électrique vérifie dans l'étape 65 que l'étiquette d'identité est correcte (c'est-à-dire qu'elle décode l'information codée) et elle vérifie ainsi l'identité de l'appareil. Suivant le résultat de ce contrôle, on passe à l'étape 66 (fausse identité) ou à l'étape 67 (identité correcte).

Comme décrit, en cas de vérification donnant une information fausse dans l'étape 65 on passe à l'étape 66. Dans cette étape, on pourra prévoir les différentes réactions à l'échec d'une authentification. On pourra par exemple ignorer l'ordre ou l'information et émettre un message d'erreur, désactiver la machine électrique et/ou l'appareil ou passer en mode de sécurité ou encore prendre d'autres mesures. Dans le cas d'un appareil de commande relié à un moteur électrique équipant un véhicule, par exemple dans le cas d'une authentification ayant échouée, on pourra activer un blocage de fonctionnement. Le cas échéant, le procédé présenté à la figure 6 avec l'étape 66 pourra être terminé par anticipation mais le cas échéant (s'il n'y a eu qu'un message de défaut) on pourra repasser sur l'étape 63 et poursuivre le procédé avec l'information suivante reçue par l'appareil.

Dans le cas d'une vérification ou d'une authentification correcte, on accepte et on traite l'information dans l'étape 67 par exemple en exécutant l'ordre. L'étape 67 passe ensuite à l'étape 63 dès que l'information suivante a été reçue par l'appareil par le chemin de communication sécurisé et cette nouvelle information sera vérifiée.

Une éventuelle difficulté liée à l'identification ou à l'authentification de machines électriques (en particulier de machines anciennes) ou d'appareils reliés à celles-ci sur le fondement de fonctions PUF peut se rencontrer à cause de la dégradation des paramètres par vieillissement qui sont critiques pour les fonctions PUF choisies. Cela peut être contourné dans certains cas si la réponse vieillie est actualisée à des instants fixes ou par des évènements déterminés pour être remplacés par une valeur actuelle pour la paire requête/réponse.

C'est ainsi qu'en s'appuyant sur l'exemple de réalisation des figures 5 et 6, la machine électrique pourrait générer une nouvelle

paire requête/réponse CRP et, à partir de là, envoyer automatiquement une clé secrète à l'autre appareil. La clé y est ensuite enregistrée pour être utilisée pour la suite du procédé servant à créer un chemin de communication sécurisé entre l'appareil et la machine électrique. Pour la clé secrète servant la communication, la machine électrique et l'appareil associé pourront le cas échéant utiliser encore l'ancienne clé secrète pour la protection dans la mesure où celle-ci se trouve dans les deux appareils (à l'étape enregistré en mémoire). Une telle actualisation de la fonction PUF et de la paire requête/réponse CRP peut se faire à intervalles réguliers ou selon des périodes définies ou encore selon des paramètres traduisant un vieillissement. L'actualisation peut se faire par exemple sur un moteur ou un appareil de commande à la fin de l'actionnement dans un véhicule électrique si la machine électrique est un moteur électrique équipant le véhicule relié à l'appareil par un appareil de commande associé.

NOMENCLATURE

1	source de signal de bobine de stator
3	bobine de rotor
4, 5	points d'application d'une tension
6	unité de mesure
7	capteur de position
8	lignes de champ électrique
31-38	étapes de procédé
41-46	étapes de procédé
51	machine électrique
52	appareil relié à la machine électrique
53	extracteur flou
54	unité de calcul et de vérification
55	ligne de communication/transmission d'information de l'appareil 52 à la machine 51
56	envoi d'une requête
57	réponse de la machine électrique
58	émission de la clé
59	traitement de l'information par la machine électrique
61-67	étapes de procédé

REVENDICATIONS

1°) Procédé pour générer une paire requête/réponse d'une machine électrique comme élément de base d'une authentification,
la machine électrique ayant au moins un stator et au moins un rotor
procédé caractérisé en ce que
on génère comme requête, un signal de tension ou d'intensité qui produit une induction entre le rotor et le stator, et
on définit comme réponse une grandeur dépendant de l'induction produite.

2°) Procédé selon la revendication 1,
caractérisé en ce que
la réponse est définie en fonction de la tension entre deux points fixe (4, 5) d'une bobine (3) du rotor ou du stator.

3°) Procédé selon la revendication 2,
caractérisé en ce que
la réponse dépend de l'évolution chronologique et de l'amplitude de la tension entre les points fixes (4, 5) de la bobine (3).

4°) Procédé son la revendication 1,
caractérisé en ce qu'
on définit une position du rotor.

5°) Procédé selon la revendication 4,
caractérisé en ce qu'
on déclenche la génération de la requête et la détermination de la réponse lorsqu'on constate que le rotor se trouve dans une position fixée.

6°) Procédé selon la revendication 5,
caractérisé en ce que
la position fixée du rotor est fixée par un capteur de position (7).

7°) Procédé selon la revendication 1,
caractérisé en ce qu'

on vérifie une réponse signée préalablement par une clé secrète avec la réponse déterminée et une clé publique.

8°) Procédé selon la revendication 1,
caractérisé en ce qu'
on génère une clé secrète à partir de la paire requête/réponse et on vérifie un message d'authentification avec la clé secrète.

9°) Machine électrique comportant au moins un stator et au moins un rotor,
caractérisée en ce qu'
elle comporte des moyens (1) pour générer comme requête, un signal de tension ou d'intensité produisant une induction entre le rotor et le stator, et
des moyens (6) pour déterminer, comme réponse, une grandeur dépendant de l'induction produite.

10°) Machine électrique selon la revendication 9,
caractérisée en ce qu'
elle comporte un capteur de position (7) qui détermine une position du rotor.

11°) Machine électrique selon la revendication 9,
caractérisée en ce qu'
elle comporte une unité de mesure (6) pour déterminer une tension,
l'unité de mesure (6) étant reliée à au moins deux points (4, 5) d'une bobine (3) du rotor ou du stator.

12°) Machine électrique selon la revendication 9,
caractérisée en ce qu'
elle comporte un générateur de signal (1) qui génère un signal fixe de tension ou d'intensité.

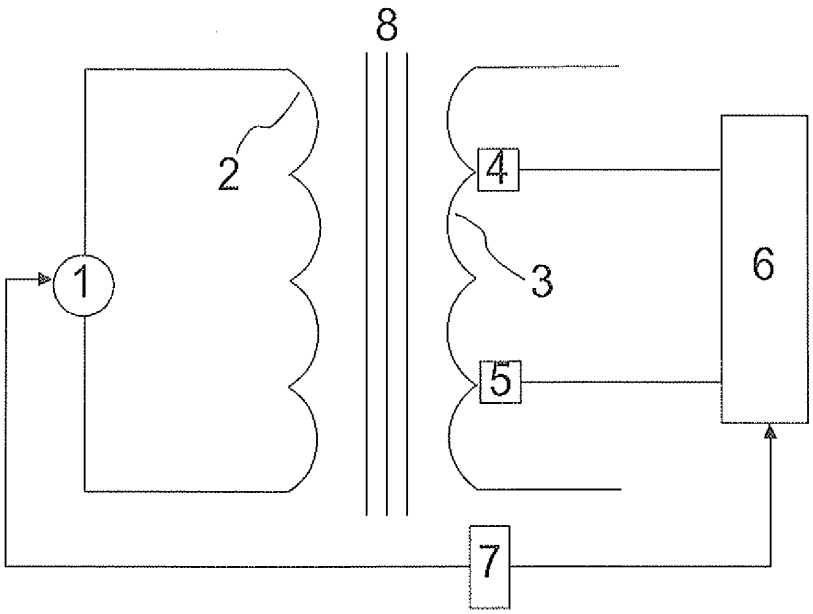


FIG. 1

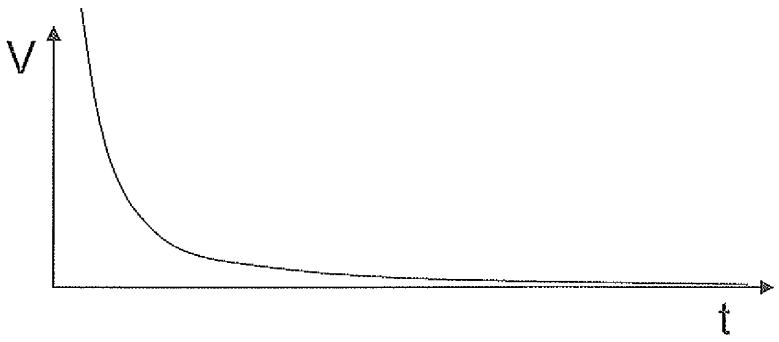


FIG. 2

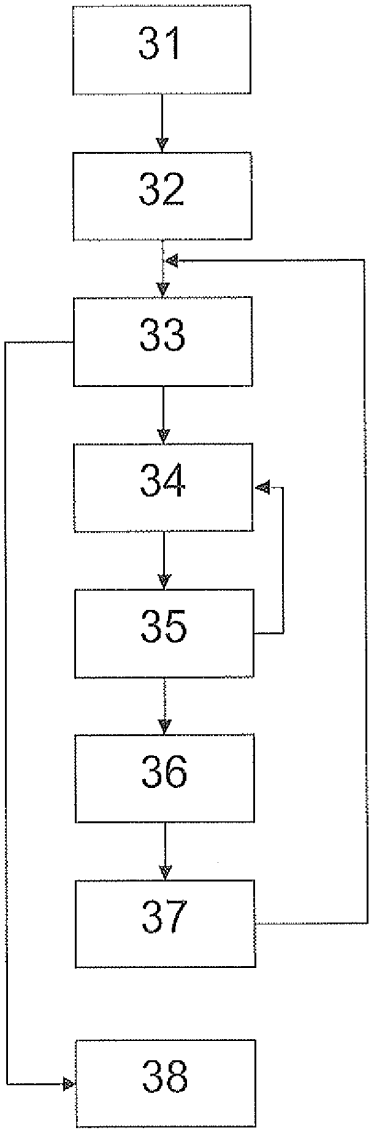


FIG. 3

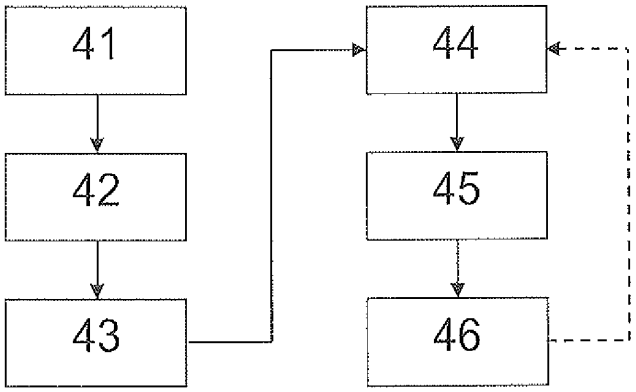


FIG. 4

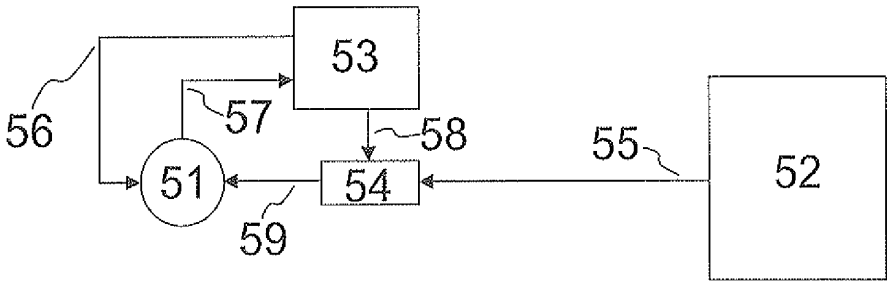


FIG. 5

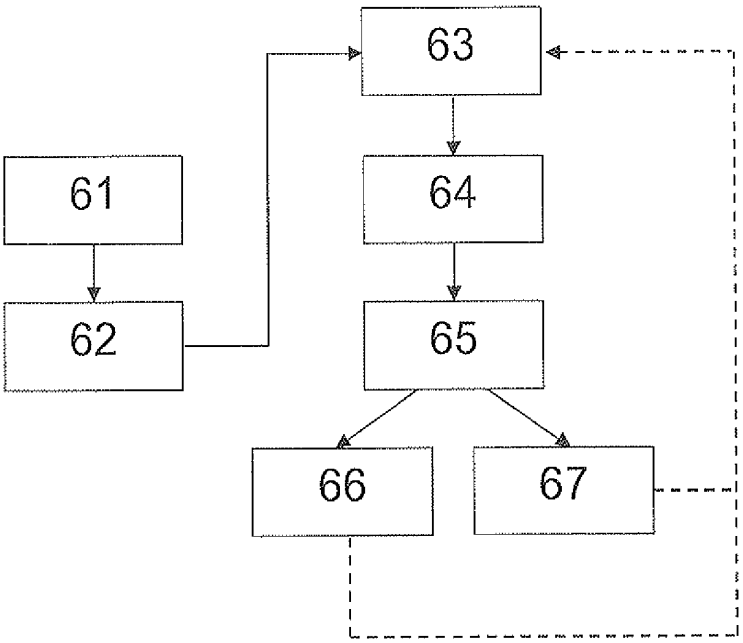


FIG. 6