(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** ***2 823 580***
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **01 04954**

(51) Int Cl[7] : **G 06 F 19/00,** G 06 F 7/38 // G 06 F 161:00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 11.04.01.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 18.10.02 Bulletin 02/42.

(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) :** *PELE LAURENT FRANCOIS ERNEST* — FR.

(72) **Inventeur(s) :** PELE LAURENT FRANCOIS ERNEST.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** PELE LAURENT.

(54) PROCEDE CRYPTOGRAPHIQUE DE SELECTION ET D'ECHANGE DE CARTES POUR UN JEU DE CARTES A DISTANCE SANS INTERMEDIAIRE.

(57) L'invention consiste en un procédé de sélection en aveugle de X cartes à distance parmi un jeu de K cartes représentées par les nombres C_1 , C_2 à C_K . 2 moyens « Joueur A » et « Joueur B » partagent un nombre N premier.

Le " joueur A " tire au hasard un nombre A1 tel que A1 soit premier avec N-1.

Le " joueur A " calcule pour tout i de 1 à K, Vi tel que Vi = Ci^ A1 modulo N, mélange les cartes et les envoie au « joueur B ».

Le " Joueur B " tire au hasard 2 nombres B1 et B2 tels que B1 et B2 soit premiers avec N-1.

Le " Joueur B " sélectionne au hasard X cartes différentes parmi les K cartes reçues et calcule pour chacune JB_i; V_i^ B1 modulo N qu'il renvoie au « joueur A ».

Le « joueur A » calcule A1prime tel que A1prime * A1 = 1 modulo N-1

A calcule Vi = JB_i ^ A1prime modulo N pour les X cartes et les renvoie à B.

Le « joueur B » calcule B1prime tel que B 1prime * B1 = 1 modulo N-1.

B calcule pour les Vi = JB_i ^ B1prime modulo N pour les X cartes et voit donc des cartes correspondant à des nombres C_j en clair et peut choisir les cartes qu'il conserve et remet les autres dans le tas.

FR 2 823 580 - A1

Domaine technique :

Lorsque des personnes jouent aux cartes, ils ont habituellement recours à un tas de cartes mélangées, un joueur tire une carte dans le tas, il ne la voit pas, mais il sait que la carte dans le tas ne se trouve pas dans son jeu ou dans celui des autres joueurs, pourtant il n'a pas vu les cartes des autres joueurs. Quand un joueur n'est pas satisfait d'une carte et en veut une autre, il la remet dans le tas.

Certains jeux de cartes ne sont pas ouverts à tout public, par exemple, le jeu de poker, même sans argent, est interdit en France sauf dans le cadre du cercle de famille En effet, il est possible pour des membres d'une même famille de jouer de l'argent au poker.

Or du fait de l'éclatement des familles, il peut être difficile pour certaines personnes isolées de s'adonner à leur jeu favori à moins de trouver un système de jeu par correspondance.

Dans d'autres cas, certaines personnes doivent se connecter sur Internet pour trouver des partenaires compréhensifs pour jouer au jeu de cartes qui les intéresse.

Il n'était pas possible jusqu'à présent de jouer aux cartes par correspondance à cause des caractéristiques techniques insoupçonnées du tas que l'on vient d'évoquer sauf à recourir à un tiers. Mais ce tiers peut être corrompu, complice de collusion ou non protégé contre les indiscrétions de tiers, surtout si des gens misent de l'argent sur le résultat du jeu. En l'absence d'enjeu pour l'intermédiaire, il peut ne pas prendre les mesures de protection nécessaires.

Comme on n'est bien servi que par soi-même et pour éviter les risques, la présente invention présente la solution technique avec un système de sélection de cartes pour un jeu par correspondance sans intermédiaire.

Dans les jeux d'argent, certains croupiers se sont mêmes enrichis en pratiquant de faux mélanges imperceptibles profitant à des complices.

Un bon mélange fait par plusieurs personnes indépendantes permet d'éviter ce risque de fraude, le système de sélection de cartes sous forme électronique permet d'éviter ce risque car tous les joueurs mélangent les cartes.

Le procédé de sélection de cartes repose sur des méthodes cryptographiques permettant au joueur adverse de choisir une carte dans un tas chiffré sans connaître les cartes dans ce tas ni choisir de carte déjà en sa possession ni en possession de l'adversaire.

Les cartes sont mélangées à chaque tour pour empêcher les joueurs de trouver quelle carte est sélectionnée.

Le principe est le suivant : le joueur A chiffre les cartes du tas, le joueur B choisit des cartes de ce tas et les chiffre, les envoie au joueur A qui les déchiffre avec sa clé (mais le joueur A ne peut voir les cartes choisies car elles restent chiffrées avec la clé du joueur B) ensuite le joueur

B déchiffre à son tour les cartes qu'il a sélectionnées avec sa clé pour les voir en clair.

Le procédé s'appuie sur les particularités mathématiques de la fonction puissance sur des nombres entiers modulo un nombre fixé. La fonction puissance est commutative (X puissance A puissance B est égal à X puissance A puissance B lui même égal à X puissance (A*B)) et très difficilement inversible (connaissant X et X^A, il est très difficile de retrouver A).

Il est possible d'étendre le procédé au cas de jeu avec plus de 2 joueurs, avec rejet de cartes, repioche et plusieurs phases de jeu en combinant les principes de mélanges de cartes et de clés différentes par groupe.

Etat de la technique antérieure :

Aucun des procédés cryptographiques connus jusqu'à présent (notamment cryptographie à clé publique, cryptographie symétrique), ne permettait de résoudre le problème de tirage au sort d'une carte par un tiers parmi des valeurs différentes, sans la révéler.

Exposé de l'invention :

Procédé de sélection de X cartes pour un jeu de cartes par correspondance entre 2 ou plusieurs joueurs impliquant le tirage au sort de cartes dans un tas sans que l'une quelconque des joueurs ne connaisse le contenu du tas et sans que 2 personnes jouant au jeu n'aient les mêmes cartes à l'aide de :

- un nombre N entier strictement positif
- un jeu de K cartes représentées par des nombres C_1, C_2 à C_K avec K entier strictement supérieur à 1 et strictement inférieur à N et les nombres C_1, C_2 à C_K entiers compris entre 2 et N-1
- un nombre PhiN égal à l'indicatrice d'Euler du nombre N
- 2 supports dits "Joueur A" et "Joueur B" dotés de capacité de mémoire et de calcul de stockage de nombres

Etape 1

Le "joueur A" stocke dans des mémoires représentant le Tas T_1, T_2 à T_K les valeurs respectivement C_1, C_2 à C_K

Le "Joueur A" mélange les K mémoires T_1, T_2 à T_K (par exemple en faisant plusieurs changes de mémoire Ti et Tj étant tiré au hasard)

Le "joueur A" tire au hasard un nombre A1 tel que A1 soit premier avec PhiN

Le "joueur A" calcule pour tout i de 1 à K, Vi tel que Vi = Ti ^A1 modulo N (le signe ^ représente l'élévation à la puissance) et affecte les valeurs Vi dans les Ti

Le "Joueur A" mélange les K mémoires T_1, T_2 à T_K

Le "Joueur A" envoie au "joueur B" les K valeurs T_1, T_2 à T_K

Etape 2

Le "Joueur B" reçoit K valeurs et les affecte dans des mémoires T_1, T_2 à T_K

Le "Joueur B" mélange les K mémoires T_1, T_2 à T_K

Le "Joueur B" sélectionne au hasard X cartes différentes parmi les T_1, T_2 à T_K et affecte leurs valeurs dans JB_1, JB_2 à JB_X, les cartes non sélectionnées sont donc stockées dans T_1, T_2 à T_{K-X}

Le "Joueur B" tire au hasard 2 nombres B1 et B2 tels que B1 et B2 soit premiers avec PhiN

Le "joueur B" calcule pour tout i de 1 à K-X, Vi tel que Vi = Ti ^B2 modulo N et affecte les valeurs Vi dans les Ti

Le "Joueur B" mélange les K-X mémoires T_1, T_2 à T_{K-X}

Le "joueur B" calcule pour tout i de 1 à X, Vi tel que Vi = JB_i ^B1 modulo N et affecte les valeurs Vi dans les JB_i

Le "Joueur B" mélange les X mémoires JB_1, JB_2 à JB_X

Le "Joueur B" envoie au "joueur A" les valeurs T_1, T_2 à T_{K-X} dans un groupe et les valeurs JB_1, JB_2 à JB_X dans un autre groupe

Etape 3

Le "Joueur A" affecte le premier groupe de valeurs dans les mémoires T_1, T_2 à T_{K-X} et le deuxième de valeurs dans les mémoires JB_1, JB_2 à JB_X

Le "Joueur A" mélange les K-X mémoires T_1, T_2 à T_{K-X}

Le "Joueur A" mélange les X mémoires JB_1, JB_2 à JB_X

Le "joueur A" calcule A1prime tel que A1prime * A1 = 1 modulo PhiN

Le "joueur A" calcule pour tout i de 1 à X, Vi tel que Vi = JB_i ^A1prime modulo N et affecte les valeurs Vi dans les JB_i

Le "Joueur A" tire au hasard 2 nombres A2 et A3 tels que A2 et A3 soit premiers avec PhiN

Le "Joueur A" sélectionne au hasard X cartes différentes parmi les T_1, T_2 à T_K et affecte leurs valeurs dans JA_1, JA_2 à JA_X, les cartes non sélectionnées sont donc stockées dans T_1, T_2 à T_{K-2*X}

Le "Joueur A" mélange les X mémoires JA_1, JA_2 à JA_X

Le "joueur A" calcule pour tout i de 1 à X, Vi tel que Vi = JA_i ^(A1prime*A2) modulo N et affecte les valeurs Vi dans les JA_i

Le "Joueur A" mélange les X mémoires JA_1, JA_2 à JA_X

Le "joueur A" calcule pour tout i de 1 à K-2*X, Vi tel que Vi = Ti ^(A1prime*A3) modulo N et affecte les valeurs Vi dans les Ti

Le "Joueur A" mélange les K-2*X mémoires T_1, T_2 à T_{K-2*X}

Le "Joueur A" envoie au "joueur B" les valeurs T_1, T_2 à T_{K-2*X} dans un groupe, les valeurs JB_1, JB_2 à JB_X dans un $2^{ème}$ groupe et les valeurs JB_1, JB_2 à JB_X dans un $3^{ème}$ groupe

Etape 4

Le "Joueur B" affecte le premier groupe de valeurs dans les mémoires T_1, T_2 à T_{K-2*X} , le deuxième groupe de valeurs dans les mémoires JB_1, JB_2 à JB_X , le deuxième groupe de valeurs dans les mémoires JA_1, JA_2 à JA_X

Le "Joueur B" mélange les K-2*X mémoires T_1, T_2 à T_{K-2*X}

Le "Joueur B" mélange les X mémoires JB_1, JB_2 à JB_X

Le "joueur B" calcule B1prime tel que B1prime * B1 = 1 modulo PhiN

Le "joueur B" calcule pour tout i de 1 à X, Vi tel que Vi = JB_i ^B1prime modulo N et affecte les valeurs Vi dans les JB_i

Le "joueur B" voit donc en clair ses cartes car les JB_i doivent correspondre à des C_1, C_2 à C_K puisque C_i ^(A1*B1*A1prime*B1prime) modulo N est égal à C_i

Le "joueur B" calcule B2prime tel que B2prime * B2 = 1 modulo PhiN

Le "joueur B" calcule pour tout i de 1 à X, Vi tel que Vi = JA_i ^B2prime modulo N et affecte les valeurs Vi dans les JA_i

Le "Joueur B" mélange les X mémoires JA_1, JA_2 à JA_X

Le "Joueur B" envoie au "joueur A" les valeurs T_1, T_2 à T_{K-2*X} dans un groupe, les valeurs JA_1, JA_2 à JA_X dans un $2^{ème}$ groupe

Etape 5

Le "Joueur A" affecte le premier groupe de valeurs dans les mémoires T_1, T_2 à T_{K-2*X} , le deuxième groupe de valeurs dans mémoires JA_1, JA_2 à JA_X

Le "joueur A" calcule A2prime tel que A2prime * A2 = 1 modulo PhiN

Le "joueur A" calcule pour tout i de 1 à X, Vi tel que Vi = JA_i ^A2prime modulo N et affecte les valeurs Vi dans les JA_i

Le "joueur A" voit donc en clair ses cartes car les JA_i doivent correspondre à des C_1, C_2 à C_K puisque C_i ^(A1*B1*A1prime*A2*B1prime*A2prime) modulo N est égal à C_i

Indication de la manière dont l'invention est susceptible d'application industrielle :

Les calculs et les stockages peuvent être effectués par des cartes à microprocesseur ou un micro-ordinateur.

L'invention est particulièrement adaptée pour des tirages au sort impartiaux et confidentiels à distance ou pour mettre en place des systèmes de sélection de cartes à distance. Il peut être également mis en place pour des validations d'expérience par tirage au sort en double aveugle.

Le système d’échange et de sélection peut servir pour d’autres jeux que les cartes tels que le jeu de domino.

En effet, le système de sélection de cartes est indépendant de la règle du jeu proprement dit.

REVENDICATIONS

1) Procédé de sélection par tirage au sort impartial, confidentiel et par correspondance de X identifiants numériques parmi K dans un tas entre 2 intervenants distants et indépendants sans que l'un quelconque des intervenants ne connaisse le contenu du tas et sans que les 2 intervenants participant au tirage n'aient sélectionné les mêmes identifiants numériques caractérisé par

Ces intervenants, appelés « Intervenant A » et « Intervenant B », disposant chacun de moyens indépendants de calcul, de stockage et d'échange de données appropriés possèdent en commun

- un nombre N entier premier strictement positif
- un jeu de K identifiants numériques représentées par des nombres C_1, C_2 à C_K avec K entier strictement supérieur à 1 et strictement inférieur à N et les nombres C_1, C_2 à C_K entiers compris entre 2 et N-1
- un nombre PhiN égal à l'indicatrice d'Euler du nombre N soit PhiN = N-1

Ces moyens de calcul, de stockage et d'échange de données sont utilisés pour les étapes successives suivantes :

Etape 1

L' "Intervenant A" stocke dans des mémoires représentant le Tas T_1, T_2 à T_K les valeurs respectivement C_1, C_2 à C_K

L'" Intervenant A" mélange les K mémoires T_1, T_2 à T_K (par exemple en faisant plusieurs échanges de mémoire Ti et Tj étant tiré au hasard)

L'" Intervenant A" tire au hasard un nombre A1 tel que A1 soit premier avec PhiN

L'" Intervenant A" calcule pour tout i de 1 à K, Vi tel que Vi = Ti ^A1 modulo N (le signe ^ représente l'élévation à la puissance) et affecte les valeurs Vi dans les Ti

L'" Intervenant A" mélange les K mémoires T_1, T_2 à T_K

L'" Intervenant A" envoie à l'" Intervenant B" les K valeurs T_1, T_2 à T_K

Etape 2

L'" Intervenant B" reçoit K valeurs et les affecte dans des mémoires T_1, T_2 à T_K

L'" Intervenant B" mélange les K mémoires T_1, T_2 à T_K

L'" Intervenant B" sélectionne au hasard X identifiants numériques différents parmi les T_1, T_2 à T_K et affecte leurs valeurs dans JB_1, JB_2 à JB_X, les identifiants numériques non sélectionnées sont donc stockées dans T_1, T_2 à T_{K-X}

L'" Intervenant B" tire au hasard 2 nombres B1 et B2 tels que B1 et B2 soit premiers avec

PhiN

L'" Intervenant B" calcule pour tout i de 1 à K-X, Vi tel que Vi = Ti ^B2 modulo N et affecte les valeurs Vi dans les Ti

L'" Intervenant B" mélange les K-X mémoires T_1, T_2 à T_{K-X}

L'" Intervenant B" calcule pour tout i de 1 à X, Vi tel que Vi = JB_i ^B1 modulo N et affecte les valeurs Vi dans les JB_i

L'" Intervenant B" mélange les X mémoires JB_1, JB_2 à JB_X

L'" Intervenant B" envoie à l'"Intervenant A" les valeurs T_1, T_2 à T_{K-X} dans un groupe et les valeurs JB_1, JB_2 à JB_X dans un autre groupe

Etape 3

L'" Intervenant A" affecte le premier groupe de valeurs dans les mémoires T_1, T_2 à T_{K-X} et le deuxième groupede valeurs dans les mémoires JB_1, JB_2 à JB_X

L'" Intervenant A" mélange les K-X mémoires T_1, T_2 à T_{K-X}

L'" Intervenant A" mélange les X mémoires JB_1, JB_2 à JB_X

L'" Intervenant A" calcule A1prime tel que A1prime * A1 = 1 modulo PhiN

L'" Intervenant A" calcule pour tout i de 1 à X, Vi tel que Vi = JB_i ^A1prime modulo N et affecte les valeurs Vi dans les JB_i

L'" Intervenant A" tire au hasard 2 nombres A2 et A3 tels que A2 et A3 soit premiers avec PhiN

L'" Intervenant A" sélectionne au hasard X identifiants numériques différents parmi les T_1, T_2 à T_{K-X} et affecte leurs valeurs dans JA_1, JA_2 à JA_X, les cartes non sélectionnées sont donc stockées dans T_1, T_2 à T_{K-2*X}

L'" Intervenant A" mélange les X mémoires JA_1, JA_2 à JA_X

L'" Intervenant A" calcule pour tout i de 1 à X, Vi tel que Vi = JA_i ^(A1prime*A2) modulo N et affecte les valeurs Vi dans les JA_i

L'" Intervenant A" mélange les X mémoires JA_1, JA_2 à JA_X

L'" Intervenant A" calcule pour tout i de 1 à K-2*X, Vi tel que Vi = Ti ^(A1prime*A3) modulo N et affecte les valeurs Vi dans les Ti

L'" Intervenant A" mélange les K-2*X mémoires T_1, T_2 à T_{K-2*X}

L'" Intervenant A" envoie à l'" Intervenant B" les valeurs T_1, T_2 à T_{K-2*X} dans un groupe, les valeurs JB_1, JB_2 à JB_X dans un $2^{ème}$ groupe et les valeurs JB_1, JB_2 à JB_X dans un $3^{ème}$ groupe

Etape 4

L'" Intervenant B" affecte le premier groupe de valeurs dans les mémoires T_1, T_2 à T_{K-2*X} , le deuxième groupe de valeurs dans les mémoires JB_1, JB_2 à JB_X , le deuxième groupe de valeurs dans les mémoires JA_1, JA_2 à JA_X

L'" Intervenant B" mélange les K-2*X mémoires T_1, T_2 à T_{K-2*X}

L'" Intervenant B" mélange les X mémoires JB_1, JB_2 à JB_X

L'" Intervenant B" calcule B1prime tel que B1prime * B1 = 1 modulo PhiN

L'" Intervenant B" calcule pour tout i de 1 à X, Vi tel que Vi = JB_i ^B1prime modulo N et affecte les valeurs Vi dans les JB_i

L'" Intervenant B" voit donc en clair ses identifiants numériques car les JB_i doivent correspondre à des C_1, C_2 à C_K puisque C_i ^(A1*B1*A1prime*B1prime) modulo N est égal à C_i

L'" Intervenant B" calcule B2prime tel que B2prime * B2 = 1 modulo PhiN

L'" Intervenant B" calcule pour tout i de 1 à X, Vi tel que Vi = JA_i ^B2prime modulo N et affecte les valeurs Vi dans les JA_i

L'" Intervenant B" mélange les X mémoires JA_1, JA_2 à JA_X

L'" Intervenant B" envoie à l'" Intervenant A" les valeurs T_1, T_2 à T_{K-2*X} dans un groupe, les valeurs JA_1, JA_2 à JA_X dans un 2ème groupe

Etape 5

L'" Intervenant A" affecte le premier groupe de valeurs dans les mémoires T_1, T_2 à T_{K-2*X} , le deuxième groupe de valeurs dans mémoires JA_1, JA_2 à JA_X

L'" Intervenant A" calcule A2prime tel que A2prime * A2 = 1 modulo PhiN

L'" Intervenant A" calcule pour tout i de 1 à X, Vi tel que Vi = JA_i ^A2prime modulo N et affecte les valeurs Vi dans les JA_i

L'" Intervenant A" voit donc en clair ses identifiants numériques car les JA_i doivent correspondre à des C_1, C_2 à C_K puisque C_i ^(A1*B1*A1prime*A2*B1prime*A2prime) modulo N est égal à C_i

2) Procédé selon la revendication 1 où l'un des moyens est une carte à microprocesseur

3) Procédé selon l'une quelconque des revendications n°1 ou 2 dans le cas où l'un des moyens est un micro ordinateur

4) Procédé selon l'une quelconque des revendications n°1 à 3 pour lequel le procédé est adapté à la validation d'expérience par tirage au sort en double aveugle, caractérisé en cela que les identifiants numériques tirées au sort (C_1, C_2 à C_K) représentent des numéros d'expérience et les intervenants sont les institutions préparant ou conduisant les expériences

5) Procédé selon l'une quelconque des revendications n°1 à 3 pour lequel le procédé est adapté à une sélection de cartes ou de dominos pour un jeu par correspondance caractérisé en cela que les identifiants numériques sélectionnées par tirage au sort (C_1, C_2 à C_K) représentent des éléments de jeu (cartes ou dominos) et les intervenants sont des joueurs