



DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

(51) Classification internationale des brevets ⁷ : H04L 9/22	A1	(11) Numéro de publication internationale: WO 00/10284 (43) Date de publication internationale: 24 février 2000 (24.02.00)
(21) Numéro de la demande internationale: PCT/FR99/01996 (22) Date de dépôt international: 16 août 1999 (16.08.99) (30) Données relatives à la priorité: 98/10592 17 août 1998 (17.08.98) FR (71) Déposant (pour tous les Etats désignés sauf US): GEMPLUS S.C.A. [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 Gémenos Cedex (FR). (72) Inventeurs; et (75) Inventeurs/Déposants (US seulement): CORON, Jean-Sébastien [FR/FR]; 4, rue Léon de Lagrange, F-75015 Paris (FR). NACCACHE, David [FR/FR]; 7, rue Chaptal, F-75009 Paris (FR). (74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 Gémenos Cedex (FR).		(81) Etats désignés: AU, CA, CN, IN, JP, MX, SG, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Publiée <i>Avec rapport de recherche internationale.</i>
(54) Title: METHOD FOR TESTING A RANDOM NUMBER SOURCE AND ELECTRONIC DEVICES COMPRISING SAID METHOD (54) Titre: PROCEDE DE TEST DE SOURCE DE NOMBRE ALEATOIRE ET DISPOSITIFS ELECTRONIQUES COMPRENANT CE PROCEDE (57) Abstract The invention concerns a method for testing sources generating random numbers, particularly sources set up in the context of cryptographic systems such as random number generators incorporated in chip cards. The invention is particularly designed to be used for testing and validating electronic devices such as chip cards, PCMCIA, badges, contactless cards or any other similar portable apparatus. (57) Abrégé La présente invention concerne un procédé de test de sources générant des nombres aléatoires, en particulier des sources mises au point dans le cadre de systèmes cryptographiques tels que les générateurs de nombres aléatoires embarqués à bord de cartes à puce. Elle est particulièrement destinée à être mise en oeuvre dans le test et la validation de dispositifs électroniques du type carte à puce, PCMCIA, badges, cartes sans contact ou tout autre appareil portable.		