(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 853 097**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **03 03521**

(51) Int Cl[7] : **G 06 F 12/14,** G 11 C 8/20

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 24.03.03.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 01.10.04 Bulletin 04/40.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

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

(71) **Demandeur(s) :** *INNOVA CARD Société à responsabilité limitée* — FR.

(72) **Inventeur(s) :** DEHAMEL ARNAUD, BERNARD BRUNO et LHERMET FRANK.

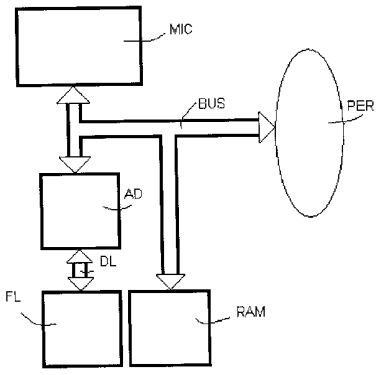
(73) **Titulaire(s) :**

(74) **Mandataire(s) :** RENAUD GOUD CONSEIL.

(54) CIRCUIT PROGRAMMABLE POURVU D'UNE MEMOIRE SECURISEE.

(57) La présente invention concerne un circuit programmable qui comprend un microprocesseur MIC, des périphériques dont une mémoire non volatile FL et une mémoire de travail RAM, un bus d'interconnexion BUS pour relier ces périphériques au microprocesseur MIC.

De plus, ce circuit comprend des moyens de protection AD pour sécuriser la mémoire non volatile FL.



FR 2 853 097 - A1

Circuit programmable pourvu d'une mémoire sécurisée

La présente invention concerne un circuit programmable pourvu d'une mémoire sécurisée.

Le domaine de l'invention est celui des composants électroniques sécurisés, notamment celui des circuits utilisés pour réaliser des transactions confidentielles.

Un tel circuit peut être subdivisé en deux zones, l'une sécurisée, l'autre non. Les informations qui transitent dans la zone sécurisée sont protégées : elles sont brouillées à l'émission et débrouillées à la réception. Dans la zone non sécurisée, les informations transitent en clair.

En tout état de cause, ce circuit intègre un microprocesseur et, souvent, une mémoire cache, un contrôleur de mémoire de cache et / ou une unité de gestion mémoire. De plus, une mémoire non volatile, une ou plusieurs mémoires de travail telles que mémoire à accès aléatoire (« RAM » pour le terme anglais « Random Access Memory ») ou mémoire à lecture seule (« ROM » pour le terme anglais « Read Only Memory ») figurent généralement dans la zone sécurisée. La plupart du temps, d'autres périphériques sont implantés dans la zone non sécurisée.

La mémoire non volatile (dite aussi mémoire « flash ») conserve les données enregistrées lorsque le circuit est hors tension, si bien que ces données sont accessibles à la prochaine mise sous tension. C'est donc dans cette mémoire que sont stockées les données qui doivent être toujours disponibles et, notamment, les clés de chiffrement propre au circuit.

Or une mémoire flash n'est pas totalement protégée. Il est possible de venir lire son contenu de l'extérieur au moyen de deux grands types d'attaques.

En premier lieu, l'attaque logicielle consiste à demander au circuit par une interface externe la lecture de la mémoire flash, ou bien à demander directement au microprocesseur qu'il sorte du circuit les données enregistrées dans cette mémoire. Ce type d'attaque est généralement prévenu par l'utilisation d'une unité de gestion de mémoire couplée au microprocesseur.

En second lieu, l'attaque physique du circuit est réalisée le plus souvent avec un microscope à effet de champ. Celui-ci permet de mesurer les charges stockées sur les grilles flottantes des cellules non volatiles afin de décoder les données contenues dans ces cellules. Cette deuxième attaque est aujourd'hui lente et coûteuse. De plus, certains mécanismes ont été mis en place pour la détecter et vider le contenu complet de la mémoire en cas de détection.

Cependant, ces mécanismes présentent un certain temps de réponse et il peut arriver qu'une partie au moins de la mémoire soit décodée avant que celle-ci ne soit effacée.

Dans certaines applications, il ne faut pas prendre le risque d'une telle attaque qui rend vulnérable les données stockées dans la mémoire flash, données au nombre desquelles peuvent figurer des clés de chiffrement.

La présente invention a ainsi pour objet de renforcer la protection de cette mémoire contre les accès frauduleux.

Selon l'invention, un circuit programmable comprend un microprocesseur, des périphériques dont une mémoire non volatile et une mémoire de travail, un bus d'interconnexion pour relier ces périphériques au microprocesseur ; de plus ce circuit comprend des moyens de protection pour sécuriser la mémoire non volatile.

Avantageusement, ces moyens de protection comportent des moyens de cryptage pour adresser des mots cryptés à la mémoire non volatile.

De préférence, les moyens de cryptage font appel à une clé privée.

Selon un mode de réalisation privilégié du circuit, les moyens de cryptage figurent dans un module d'adaptation raccordé d'une part au bus d'interconnexion et d'autre part à la mémoire non volatile par l'intermédiaire d'une liaison dédiée.

Il est souhaitable que la longueur de la clé de cryptage soit supérieure à la longueur standard des données que traite le microprocesseur, si bien que celui-ci comprend des moyens pour décomposer les mots cryptés en données de longueur standard.

Selon le mode de réalisation privilégié ci-dessus, ces moyens pour décomposer les mots cryptés en données de longueur standard figurent de préférence dans le module d'adaptation.

Ainsi, lorsque le circuit comporte de plus une mémoire cache associé à un contrôleur, la longueur de la clé de cryptage étant supérieure à la longueur standard des données que traite le microprocesseur, le module d'adaptation est prévu pour exploiter les accès consécutifs de ce contrôleur afin de décomposer les mots cryptés en données de longueur standard.

Il est préférable que la clé de cryptage soit stockée dans un registre programmable une seule fois, ce registre pouvant figurer dans la mémoire non volatile.

La présente invention apparaîtra maintenant avec plus de détails dans le cadre de la description qui suit d'un exemple de réalisation donné à titre illustratif en se référant à la figure annexée qui représente un schéma d'un circuit programmable selon l'invention.

En référence à la figure, un circuit programmable comporte un microprocesseur MIC éventuellement associé à une mémoire cache et/ou à un contrôleur de mémoire (non représentés). Les autres éléments du circuit sont :

- une mémoire non volatile FL de type flash,
- une mémoire de travail RAM à accès aléatoire,
- éventuellement un ou plusieurs autres périphériques PER,
- un module d'adaptation AD,
- un bus système BUS pour interconnecter tous les éléments du circuit hormis la mémoire non volatile FL, et
- une liaison dédiée DL pour relier cette mémoire non volatile FL et le module d'adaptation AD.

L'invention propose donc de protéger les données dans la mémoire non volatile FL et une solution avantageuse consiste à recourir à des moyens de cryptage qui sont mis en œuvre de préférence par le module d'adaptation AD.

Ainsi, les données sont cryptées avant d'être enregistrées dans cette mémoire et elles sont décryptées lorsqu'elles sont lues avant d'être traitées.

Il convient donc de chiffrer les données a la volée avant de les stocker dans la mémoire non volatile FL.

Couramment, le microprocesseur traite des données d'une longueur de 8, 16 ou 32 bits (longueur standard), si bien qu'accéder à de telles données de manière sécurisée imposerait un cryptage sur 32 bits. Il s'agirait là d'un cryptage très vulnérable, pratiquement inefficace, si l'on emploie des algorithmes connus.

Il est donc souhaitable de choisir un algorithme travaillant sur des données de 64 bits dans le cas présent, voire même 128 bits dès lors que cela s'avère nécessaire. La sélection d'un algorithme standard permet d'éviter des contraintes supplémentaires, tout en assurant un niveau de sécurité maximal.

On préfèrera un algorithme a clé privée car il nécessite des temps de calcul beaucoup plus courts qu'un algorithme à clé publique.

A titre d'exemple, on retiendra les algorithmes suivants :

- AES (abréviation de l'expression anglaise « Advanced Encryption Standard »), travaillant sur des mots de 128 bits et offrant, à l'heure actuelle, une sécurité maximale,

- DES (abréviation de l'expression anglaise « Data Encryption Standard »), travaillant sur des mots de 64 bits, connu pour son universalité dans les systèmes les moins exigeants en matière de sécurité,
- 3DES (abréviation de l'expression anglaise « Triple Data Encryption Standard »), ou
- XDES (abréviation de l'expression anglaise « Extended Data Encryption Standard »), ces deux derniers algorithmes étant réputés pour des systèmes plus exigeant en terme de sécurité tout en assurant de hauts débits de chiffrement à faible coût.

Naturellement, le module d'adaptation AD permet de crypter des données plus longues que la longueur standard. Ce module est prévu pour traiter des données de 64 ou 128 bits enregistrées en deux ou quatre mots de 32 bits dans la mémoire non volatile FL, si bien qu'un accès à une de ces données est divisé en plusieurs accès de 32 bits.

A cet effet, le module d'adaptation AD peut exploiter les accès groupés ou accès consécutifs du contrôle de la mémoire cache du microprocesseur. Cette mémoire cache contient une copie partielle de la mémoire non volatile FL qui est mise à jour en fonction de la partie du programme que le microprocesseur MIC exécute. La mémoire cache étant très rapide et très proche du microprocesseur MIC, elle permet généralement d'améliorer les performances du circuit.

Le remplacement des données présentes dans la mémoire cache au moyen du contrôleur de cache s'effectue par paquets, ces paquets ayant une taille minimale de 2 ou plus souvent 4 mots de 32 bits, ceci quelle que soit la taille des données traitées par le microprocesseur MIC.

On remarquera ici que la mémoire cache peut également être utilisée à d'autres fins par le circuit.

Le contrôleur écrit les données enregistrées dans la mémoire cache qui concernent la mémoire flash FL, par paquets d'une taille multiple de 64 bits.

L'interfaçage de la mémoire cache avec la mémoire flash FL qui n'est capable de gérer que des accès de 32 bits se fait de façon simple en scindant un accès de taille 64bits en deux accès de 32 bits.

L'algorithme DES ou 3DES sera ainsi chargé tous les 2 mots de 32 bits, tandis que l'algorithme AES sera chargé tous les 4 mots de 32 bits. Les données sont chargées à la volée. Dans le cas d'un traitement « pipeline » de l'algorithme

AES, autrement dit lorsque le traitement complet d'une donnée en un ou plusieurs cycles est capable de recevoir une nouvelle donnée à chaque cycle, seul le premier accès introduit un temps de latence sur le temps total du transfert des données.

La clé privée utilisée par l'algorithme est stockée dans une zone non sécurisée du circuit dont l'accès se fait sans chiffrement, de préférence dans un registre programmable une seule fois dit « OTP » (pour l'expression anglaise One Time Programmable). Ce registre peut d'ailleurs prendre place dans la mémoire non volatile FL.

Dans le cas d'une attaque physique telle que décrite ci-dessus, il suffit d'effacer la clé de cryptage dès que l'attaque est détectée, ce qui est une opération très rapide. Il n'est plus nécessaire de vider complètement la mémoire flash FL pour la rendre inopérante, cette opération de vidage pouvant prendre un temps relativement important si cette mémoire a une taille conséquente. Le fait que cette mémoire soit rendue inopérante beaucoup plus rapidement offre un facteur de sécurité supplémentaire.

L'exemple de réalisation de l'invention présenté ci-dessus a été choisi pour son caractère concret. Il ne serait cependant pas possible de répertorier de manière exhaustive tous les modes de réalisation que recouvre cette invention. En particulier, tout moyen décrit peut-être remplacé par un moyen équivalent sans sortir du cadre de la présente invention.

REVENDICATIONS

1) Circuit programmable comprenant un microprocesseur MIC, des périphériques dont une mémoire non volatile FL et une mémoire de travail RAM, un bus d'interconnexion BUS pour relier lesdits périphériques audit microprocesseur MIC,
caractérisé en ce qu'il comprend des moyens de protection AD pour sécuriser ladite mémoire non volatile FL.

2) Circuit selon la revendication 1, caractérisé en ce que lesdits moyens de protection AD comportent des moyens de cryptage pour adresser des mots cryptés à ladite mémoire non volatile FL.

3) Circuit selon la revendication 2, caractérisé en ce que lesdits moyens de cryptage AD font appel à une clé privée.

4) Circuit selon l'une quelconque des revendications 2 ou 3, caractérisé en ce que lesdits moyens de cryptage figurent dans un module d'adaptation AD raccordé d'une part audit bus d'interconnexion BUS et d'autre part à ladite mémoire non volatile FL par l'intermédiaire d'une liaison dédiée DL.

5) Circuit selon l'une quelconque des revendications 2 ou 3 caractérisé en ce que, la longueur de la clé de cryptage étant supérieure à la longueur standard des données que traite ledit microprocesseur MIC, il comprend des moyens AD pour décomposer lesdits mots cryptés en données de longueur standard.

6) Circuit selon la revendication 4 caractérisé en ce que, comportant de plus une mémoire cache associé à un contrôleur, la longueur de la clé de cryptage étant supérieure à la longueur standard des données que traite ledit microprocesseur MIC, ledit module d'adaptation AD est prévu pour exploiter les accès consécutifs dudit contrôleur afin de décomposer lesdits mots cryptés en données de longueur standard.

7) Circuit selon l'une quelconque des revendications 2 à 6, caractérisé en ce que la clé de cryptage est stockée dans un registre programmable une seule fois.

8) Circuit selon la revendication 7, caractérisé en ce que ledit registre figure dans ladite mémoire non volatile FL.

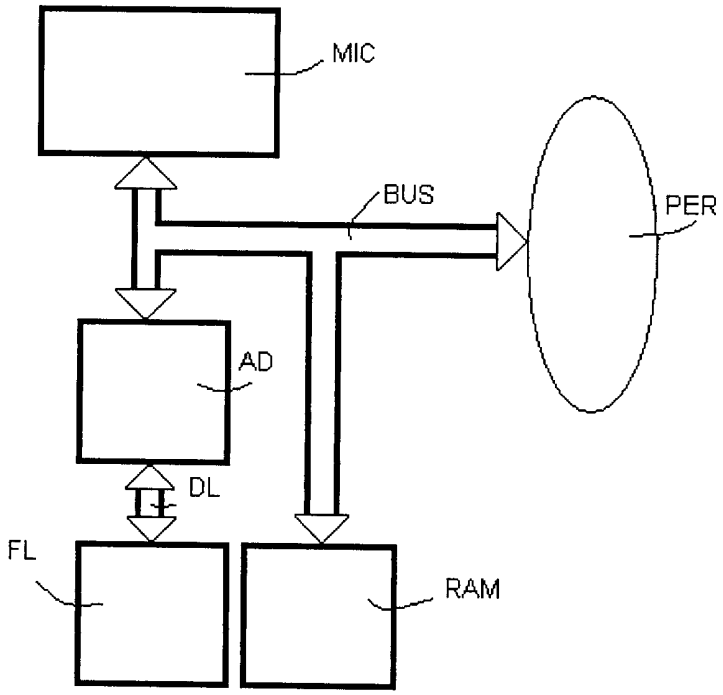


FIGURE UNIQUE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 631435
FR 0303521

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	US 6 195 752 B1 (PFAB STEFAN) 27 février 2001 (2001-02-27) * colonne 1, ligne 13 - ligne 17 * * colonne 4, ligne 21 - ligne 36 * * colonne 8, ligne 15 - colonne 9, ligne 17 * * figure 3 *	1-4,7,8	G06F12/14 G11C8/20
X	US 6 202 152 B1 (TAKAHASHI RICHARD ET AL) 13 mars 2001 (2001-03-13) * colonne 1, ligne 23 - ligne 52 * * colonne 5, ligne 66 - colonne 6, ligne 10 * * colonne 6, ligne 28 - colonne 7, ligne 43 * * figure 2 *	1-6	
X	US 2002/029345 A1 (HASHIMOTO SHIGERU ET AL) 7 mars 2002 (2002-03-07) * page 4, alinéas 90,91 * * page 5, alinéas 95,107 * * page 5, alinéa 109 - page 6, alinéa 122 * * figure 1 *	1-4	DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7) G06F G07F
X	US 6 061 449 A (SPRUNK ERIC ET AL) 9 mai 2000 (2000-05-09) * colonne 18, ligne 1 - ligne 10 * * colonne 18, ligne 46 - ligne 52 * * colonne 19, ligne 10 - ligne 11 * * colonne 19, ligne 65 - colonne 20, ligne 4 * * colonne 28, ligne 47 - ligne 50 *	1-4	
X	US 2003/005313 A1 (GAMMEL BERNDT ET AL) 2 janvier 2003 (2003-01-02) * page 2, alinéa 30 - page 3, alinéa 35 * * figure 1 *	1-4	

Date d'achèvement de la recherche	Examinateur
28 novembre 2003	Arbutina, L

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

.....

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0303521 FA 631435

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 28-11-2003
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
US 6195752	B1	27-02-2001	DE	19642560 A1	16-04-1998
			BR	9712529 A	19-10-1999
			CN	1233333 A ,B	27-10-1999
			WO	9816883 A1	23-04-1998
			EP	0932867 A1	04-08-1999
			JP	2000504137 T	04-04-2000
			KR	2000049114 A	25-07-2000
US 6202152	B1	13-03-2001	AUCUN		
US 2002029345	A1	07-03-2002	JP	2002032268 A	31-01-2002
			EP	1172731 A2	16-01-2002
US 6061449	A	09-05-2000	CA	2249554 A1	10-04-1999
			CN	1236132 A	24-11-1999
			EP	0908810 A2	14-04-1999
			IL	126448 A	14-08-2002
			TW	445402 B	11-07-2001
US 2003005313	A1	02-01-2003	AT	249664 T	15-09-2003
			DE	50003679 D1	16-10-2003
			EP	1249010 A1	16-10-2002
			JP	2003521053 T	08-07-2003
			CN	1423801 T	11-06-2003
			WO	0154083 A1	26-07-2001

EPO FORM P0465