República Federativa do Brasil
Ministério do Desenvolvimento, Indústria
e do Comércio Exterior
Instituto Nacional da Propriedade Industrial

(11) **PI 0309079-5 B1**

BRPI0309079B1

(22) Data do Depósito: 02/04/2003

(45) Data de Concessão: 19/01/2016

(RPI 2350)

(54) Título: MÉTODO E DISPOSITIVO DE PROTEÇÃO DE DADOS NUMÉRICOS ARMAZENADOS EM UMA MEMÓRIA

(51) Int.Cl.: G06F 1/00

(30) Prioridade Unionista: 08/04/2002 FR 02/04321

(73) Titular(es): NAGRA FRANCE SAS

(72) Inventor(es): JEAN LUC DAUVOIS

Relatório Descritivo da Patente de Invenção para: **"MÉTODO E DISPOSITIVO DE PROTEÇÃO DE DADOS NUMÉRICOS ARMAZENADOS EM UMA MEMÓRIA".**

Campo Técnico

A invenção se situa no domínio da luta contra a pirataria dos conteúdos das memórias de armazenamento de dados e se refere mais particularmente a um método de proteção de dados digitais armazenados em uma memória de um cartão eletrônico e previamente encriptados por uma chave de cifragem.

A invenção se refere também a um cartão eletrônico e a um dispositivo de proteção da memória desse cartão eletrônico.

Estado da Técnica

A pirataria de um cartão eletrônico é feita, em geral, pela extração do código ROM e dos dados secretos contidos na memória do cartão. Uma técnica conhecida para evitar que esses dados críticos sejam utilizáveis após uma extração fraudulenta consiste em cifrá-los por meio de chaves secretas, antes de armazená-los na memória do cartão eletrônico. As chaves de cifragem utilizadas são também armazenadas nessa memória e são, dessa forma, também expostas ao risco de uma extração fraudulenta a mesmo título que os dados úteis memorizados. Portanto, essa

técnica não permite lutar eficazmente contra a pirataria.

A finalidade da invenção é garantir uma segurança ótima dos dados memorizados sob a forma encriptada em uma memória.

Uma outra finalidade da invenção é de ligar intimamente as chaves de cifragem a um ou vários parâmetros de funcionamento intrínseco a pelo menos um elemento que compõe o cartão eletrônico. Esses parâmetros de funcionamento podem ser grandezas físicas que dependem da estrutura física da memória ou do microcontrolador associado a essa memória ou ainda grandezas que refletem um comportamento determinado dessa memória e do microcontrolador em condições particulares de utilização.

Descrição da Invenção

De forma mais precisa, a invenção se refere a um método e a um dispositivo de proteção de dados digitais armazenados sob a forma encriptada em uma memória que pode ser do tipo EEPROM ou do tipo flash, por exemplo.

O método, de acordo com a invenção, é caracterizado pelo fato de essa chave de cifragem ser definida dinamicamente em função de pelo menos um parâmetro de funcionamento intrínseco a esse cartão eletrônico.

De acordo com a invenção, esse parâmetro de funcionamento intrínseco ao cartão eletrônico é gerado por

um gerador de função integrado ao cartão eletrônico.

De acordo com a invenção, esse parâmetro de funcionamento é intrínseco à memória do cartão eletrônico.

De acordo com um modo de realização, o método compreende as seguintes etapas:

- durante a fase de escrita dos dados na memória:

a) derivar um sinal analógico de uma tensão analógica para escrita na memória;

b) converter esse sinal em uma seqüência binária;

c) cifrar os dados a serem armazenados por meio dessa seqüência binária;

d) armazenar os dados cifrados na memória;

- e, durante uma fase posterior de leitura dos dados memorizados:

- recalcular a chave de cifragem definida nas etapas a) e b) da fase de escrita; e

- descriptar os dados por meio da chave recalculada.

De acordo com esse modo de realização, a tensão analógica de escrita é fornecida por uma bomba de carga.

O dispositivo, de acordo com a invenção, é caracterizado pelo fato de comportar um módulo de cálculo apto a definir uma chave de cifragem dos dados numéricos a

serem memorizados em função de pelo menos um parâmetro de funcionamento intrínseco a esse cartão eletrônico.

De acordo com um modo de realização da invenção, o módulo de cálculo extrai um sinal analógico de uma tensão analógica de escrita proporcionado por uma bomba de carga e converte esse sinal analógico em uma seqüência binária para constituir a chave de cifragem.

A invenção se refere também a um cartão de controle de acesso que comporta uma unidade central de processamento de dados, pelo menos uma memória de armazenagem de dados, um módulo para cifragem de dados digitais e um módulo para computar pelo menos uma chave de cifragem desses dados.

O cartão de controle de acesso, de acordo com a invenção, comporta meios para definir a chave de cifragem, em função de pelo menos um parâmetro de funcionamento intrínseco à memória desse cartão, e meios para recalcular dinamicamente a chave de cifragem previamente definida a cada leitura dos dados memorizados.

De acordo com uma característica da invenção, o módulo de cálculo é funcionalmente independente da unidade central, de modo que o cálculo da chave de cifragem é simplesmente iniciado e não supervisionado pela unidade central de processamento.

De acordo com um modo particular de realização da

invenção, o módulo de cálculo comporta uma bomba de carga destinada a fornecer uma tensão analógica para escriver dados no cartão eletrônico, um conversor analógico/digital destinado a converter um sinal analógico extraído dessa tensão analógica em uma seqüência binária que constitui a chave de cifragem.

Breve Descrição dos Desenhos

Outras características e vantagens da invenção sobressairão da descrição que vai ser feita a seguir, considerada a título de exemplo não limitativo, com referência às figuras anexadas, nas quais:

- a figura 1 representa um esquema geral de um dispositivo, de acordo com a invenção;

- a figura 2 representa esquematicamente um modo particular de realização do dispositivo da figura 1;

- a figura 3 representa uma curva que ilustra uma aplicação da invenção no caso do exemplo ilustrado pela figura 2.

Descrição Detalhada dos Modos de Realização Particulares

A invenção vai a seguir ser descrita no âmbito da proteção dos dados armazenados na memória de um cartão eletrônico.

Os cartões eletrônicos são amplamente utilizados particularmente para armazenar parâmetros de controle que

permitem o acesso a dados ou serviços, tais como, por exemplo, programas audiovisuais encriptados. Nesse tipo de aplicação, as informações necessárias para desembaralhar são transmitidas em mensagens de controle de acesso, denominados ECM (Entitlement Control Message) e são geradas a partir dos seguintes dados de entradas:

- uma palavra de controle (Control Word) destinada a inicializar a seqüência de desebaralhamento;

- uma chave de serviço (Service Key) utilizada para embaralhar a palavra de controle, para um grupo de um ou de vários usuários;

- uma chave de usuário (user key) utilizada para embaralhar a chave de serviço.

Previamente, a chave de serviço é transmitida em mensagens denominadas EMM geradas a partir de uma chave de usuário individual ou de grupo.

As ECM são notadamente constituídas da palavra de controle e processadas em com intervalos regulares.

As EMM são notadamente constituídas da chave de serviço e processadas pela(s) chave(s) de usuário(s), e são também transmitidas aos usuários em intervalos regulares.

Ao recebimento, o princípio de desencriptação consiste em encontrar a chave de serviço a partir da(s) chave(s) do(s) usuário(s) contida(s) na memória de um cartão

eletrônico (EMM). Essa chave de serviço é em seguida utilizada para desencriptar as ECM, a fim de encontrar a palavra de controle, permitindo a inicialização do sistema de desembaralhamento.

Conforme foi explicado anteriormente, o conteúdo da memória do cartão eletrônico pode ser extraído e reutilizado de forma fraudulenta para encontrar as chaves para processar as EMM e as ECM que, diretamente ou indiretamente, permitem calcular a palavra de controle, permitindo a inicialização do sistema de desembaralhamento.

A figura 1 representa um esquema bloco geral de um dispositivo com memória que comporta uma unidade central de processamento 2 ligada a uma memória 4 via um módulo de encriptação/desencriptação 6. Um módulo de cálculo 10, ajustado externamente à unidade central 2, é também ligado ao módulo de encriptação/desencriptação 6.

Quando os dados processados na unidade central 2 devem ser armazenados na memória 4, a unidade de processamento 2 envia ao módulo de cálculo 10 um sinal de ativação. Ao receber esse sinal, o módulo de cálculo 10 define uma chave de cifragem dos dados a serem memorizados e transmite essa chave ao módulo de encriptação/desencriptação 6.

De acordo com uma característica essencial da invenção, a chave de cifragem é calculada no momento do

armazenamento dos dados na memória 4, em função de pelo menos um parâmetro de funcionamento intrínseco à memória 4. A chave de cifragem assim calculada não é armazenada na memória 4. Contudo, a pirataria dos cartões consiste geralmente em extrair os programas de cálculo utilizados na unidade central 2 e os dados críticos contidos na memória 4 associada à unidade central 2. Também, em caso de extração fraudulenta desses programas e do conteúdo da memória 4, os dados extraídos serão inutilizáveis sem a chave de cifragem que é calculada dinamicamente, quando da memorização desses dados e quando da leitura desses dados.

Preferencialmente, essa chave é calculada em função de um parâmetro ou de uma combinação de vários parâmetros de funcionamento intrínseco a essa memória 4.

A chave de cifragem definida é inacessível do exterior, uma vez que o módulo de cálculo 10 é independente da unidade central 2.

Em funcionamento, no momento da transferência dos dados da unidade central 2 para o módulo de cálculo 10, este último recebe da unidade central 2 um primeiro sinal de ativação, permitindo-lhe começar o cálculo da chave de cifragem. A chave assim calculada é transmitida ao módulo de encriptação/desencriptação 6 que o utiliza para cifrar os dados, antes que estes sejam memorizados na memória 4.

Quando os dados encriptados devem ser lidos, a unidade de processamento 2 envia ao módulo de cálculo 10 um segundo sinal de ativação para recalcular dinamicamente a chave de cifragem que é em seguida utilizada pelo módulo de encriptação/desencriptação 6 para desencriptar esses dados e transmiti-los à unidade central 2.

Um exemplo particular de cálculo da chave de cifragem vai ser descrito, fazendo referência à figura 2 que representa um exemplo de realização da invenção no qual o módulo 10 é constituído pela bomba de carga 12 destinada a fornecer uma tensão analógica de escrita dos dados na memória 4, um conversor analógico-digital (CAN) 14 destinado a converter um sinal analógico extraído dessa tensão analógica em uma seqüência numérica que constitui a chave de cifragem, um relógio 16 ligado à bomba de carga 12 destinada a determinar a duração do sinal analógico extraído da tensão de escrita.

A tensão analógica pode ser fornecida por um gerador de tensão analógica independente da bomba de carga.

Em um outro modo de realização não representado, o cartão pode comportar um circuito digital independente da unidade central 2 que fornece diretamente uma seqüência digital S.

A figura 3 representa esquematicamente a evolução em

função do tempo da tensão de escrita 18 dos dados digitais provenientes da unidade central 2 na memória 4. Um valor A da tensão 18 é fixado por programação da duração t, por meio do relógio 16. Esse valor A é em seguida convertido pelo CAN 14 em uma seqüência numérica S que é utilizada pelo módulo de encriptação/desencriptação 6 para encriptar/desencriptar os dados digitais.

A cada reset, o módulo de cálculo 10 calcula a chave de cifragem, considerando-se a duração t programada por meio do relógio 16. Assim, se um pirata extrair os dados numéricos, ele não poderá recalcular a chave de cifragem que depende do valor A que é intrínseco ao cartão autêntico. A chave de cifragem é calculada pela primeira vez, quando da personalização do cartão.

Em uma variante de realização da invenção, várias durações t correspondentes a vários valores A podem ser pré-programadas, a fim de serem utilizados sucessivamente para calcular várias chaves de cifragem diferentes, cada chave podendo ser utilizada durante um período pré-definido.

Em uma outra variante de realização, a duração t pode ser modificada à distância.

REIVINDICAÇÕES

1. Método para proteger dados digitais armazenados em uma memória (4) de um cartão de chip por uma chave de cifragem, a referida chave de cifragem sendo definida dinamicamente como uma função de pelo menos um parâmetro de funcionamento intrínseco ao referido cartão de chip, o método **caracterizado pelo** fato de que compreende as etapas de:

durante uma fase de escrita de dados na memória (4),

a) derivar um sinal analógico de uma tensão analógica (18) para escrita na memória (4) gerada no referido cartão de chip, o referido sinal analógico representando o parâmetro intrínseco, sendo derivado da tensão analógica em um tempo predefinido (t),

b) converter este sinal em uma sequência digital,

c) criptografar dados a serem memorizados por meio da sequência digital,

d) armazenar os dados encriptados na memória (4),

durante uma fase subsequente de leitura dos dados armazenados,

- calcular a chave de cifragem como definido nas etapas de derivar e converter um sinal analógico, e

- descriptografar os dados usando a chave recalculada.

2. Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de que os referidos dados digitais encriptados são chaves digitais para codificação criptográfica de mensagens EMM e ECM.

3. Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de que o referido parâmetro de funcionamento intrínseco ao cartão de chip é fornecido por uma bomba de carga (12) de escrita de dados na memória.

4. Dispositivo para proteger dados digitais armazenados em uma memória (4) de um cartão de chip e previamente encriptados por uma chave de cifragem, compreendendo um módulo de cálculo (10) capaz de definir a chave de cifragem dos referidos dados de acordo com pelo menos um parâmetro de funcionamento intrínseco ao referido cartão de chip e compreendendo um gerador de tensão analógico (18) para escrever na memória (4), **caracterizado pelo** fato de que o módulo de cálculo (10) compreende meios para extrair um sinal analógico da referida tensão analógica (18) em um tempo predefinido (t), este sinal analógico representando o parâmetro intrínseco, e meios para converter este sinal analógico em uma sequência digital para formar a chave de cifragem.

5. Dispositivo, de acordo com a reivindicação 4, **caracterizado pelo** fato de que os referidos dados digitais

encriptados são chaves digitais para codificação criptográfica de mensagens de EMM e ECM.

6. Dispositivo, de acordo com a reivindicação 4, **caracterizado pelo** fato de que o referido parâmetro de funcionamento intrínseco ao cartão de chip é fornecido por uma bomba de carga (12) de escrita de dados na memória.

7. Dispositivo, de acordo com a reivindicação 4, **caracterizado pelo** fato de que o módulo de cálculo (10) compreende um conversor analógico/digital (14).

8. Cartão de chip **caracterizado pelo** fato de que compreende o dispositivo como definido em qualquer uma das reivindicações 4 a 7 e compreende uma unidade central de processamento (2) de dados.

9. Cartão de chip, de acordo com a reivindicação 8, **caracterizado pelo** fato de que o módulo de cálculo (10) é funcionalmente independente da unidade central (2) com o intuito do cálculo da chave de cifragem não seja supervisionado pela unidade central de processamento (2).

10. Cartão de chip, de acordo com a reivindicação 8, **caracterizado pelo** fato de que compreende um circuito digital independente da unidade central (2) para gerar a sequência digital (S) formando a chave de cifragem.

11. Cartão de chip, de acordo com a reivindicação 8, **caracterizado pelo** fato de que o módulo de cifragem (6) é um circuito lógico.

12. Cartão de chip, de acordo com qualquer uma das reivindicações 8 a 11, **caracterizado pelo** fato de que a memória (4) é do tipo EEPROM.

13. Cartão de chip, de acordo com a reivindicação 12, **caracterizado pelo** fato de que a memória (4) é do tipo flash.

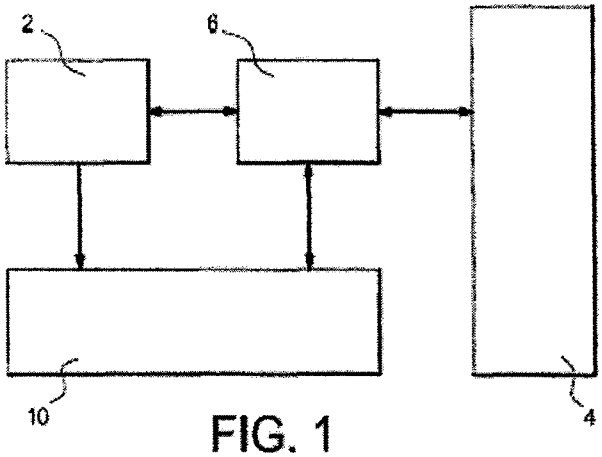

FIG. 1

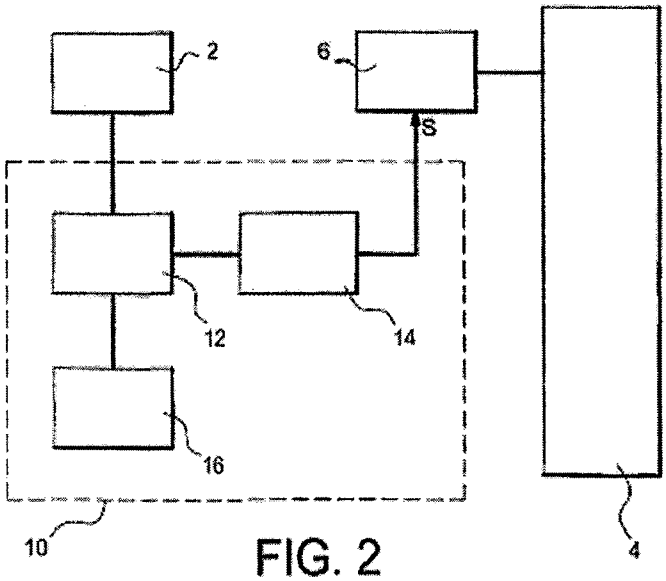

FIG. 2

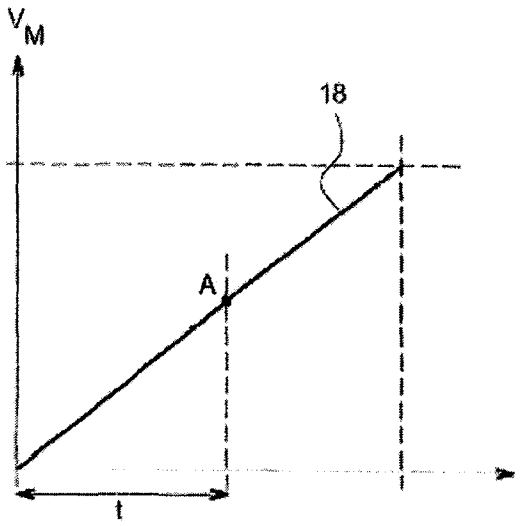

FIG. 3

Resumo da Patente de Invenção para: **"MÉTODO E DISPOSITIVO DE PROTEÇÃO DE DADOS NUMÉRICOS ARMAZENADOS EM UMA MEMÓRIA".**

A invenção se refere a um método de dados numéricos armazenados em uma memória (4) e previamente encriptadas por uma chave de cifragem. O método, de acordo com a invenção, é caracterizado pelo fato de essa chave de cifragem ser definida dinamicamente em função de pelo menos um parâmetro de funcionamento intrínseco a esse cartão.