

(11) Número de Publicação: PT 880737 E

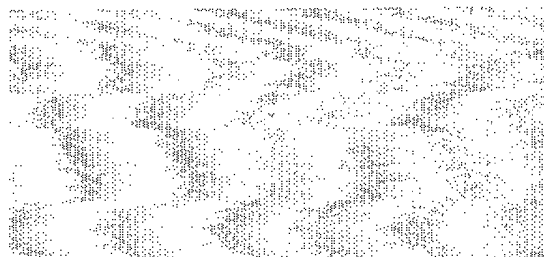
(51) Classificação Internacional: (Ed. 6)
G06F007/10 A

(12) FASCÍCULO DE PATENTE DE INVENÇÃO

(22) Data de depósito: 1997.02.11	(73) Titular(es): KONINKLIJKE KPN N.V. STATIONSPLEIN 7 NL-9726 AE GRONINGEN NL
(30) Prioridade: 1996.02.16 EP 96200402	
(43) Data de publicação do pedido: 1998.12.02	(72) Inventor(es): ALBERTUS FEIKEN NL
(45) Data e BPI da concessão: 2000.05.10	(74) Mandatário(s): JORGE BARBOSA PEREIRA DA CRUZ RUA DE VÍTOR CORDON 10-A 3/AND. 1200 LISBOA PT

(54) Epígrafe: MÉTODO PARA MODIFICAR O CONJUNTO DE INSTRUÇÕES DE UM CARTÃO INTELIGENTE

(57) Resumo:





DESCRIÇÃO

" MÉTODO PARA MODIFICAR O CONJUNTO DE INSTRUÇÕES DE UM CARTÃO INTELIGENTE "

O presente invento diz respeito a um método para modificar a função de uma instrução num conjunto de instruções de um processador de um cartão inteligente. Mais particularmente, o presente invento diz respeito a um método para modificar as funções de instruções individuais num conjunto de instruções de um processador de um cartão inteligente.

Um cartão inteligente, também designado por cartão IC (isto é, cartão de Circuito Integrado), é um dispositivo electrónico próprio para efectuar pagamentos. O circuito integrado do cartão contém um microprocessador, ou qualquer outro dispositivo semelhante, próprio para o processamento de dados. O processador de um cartão inteligente acha-se normalmente dotado de um conjunto de instruções compreendendo instruções (comandos) tais como LER, ESCREVER, ACTUALIZAR, etc., próprias para funcionar mediante os dados (de pagamento) contidos no cartão. São frequentemente utilizados conjuntos de instruções normalizadas, tais como por exemplo as definidas pela Norma Europeia EN726. No entanto, esse tipo de conjuntos de instruções são necessariamente limitados com respeito ao número e ao âmbito das instruções. À medida que o sistema de pagamento electrónico através de cartões inteligentes se vai desenvolvendo, vai surgindo com cada vez maior frequência a necessidade de se adicionar novas funções aos cartões, ou de se alterar funções existentes. Essas alterações implicam normalmente uma modificação do conjunto de instruções dos cartões inteligentes. Normalmente isso implica que o circuito integrado dos



cartões tenha que ser redesenhado, o que, além de ser caro, faz com que os cartões existentes se tornem obsoletos. Além disso, a alteração de um conjunto de instruções normalizadas irá por em perigo a sua compatibilidade com as normas.

Por estes e outros motivos surgiu a necessidade de se poder modificar o conjunto de instruções dos cartões inteligentes sem que isso implique uma substancial alteração do conjunto existente.

Além disso, chama-se a atenção para o facto de que na FR-A-2 667 418 é divulgado um cartão inteligente que compreende um processador e uma memória de aplicação. A memória de aplicação é dividida em várias zonas funcionais, isto é, ROM, PROM, EPROM, etc. Uma segunda memória encontra-se associada palavra a palavra com a referida memória de aplicação. A referida segunda memória encontra-se simultaneamente endereçada com a referida memória de aplicação e indica a funcionalidade da localização da memória de aplicação endereçada. No entanto, não é realizada qualquer modificação de funcionalidades dentro do conjunto de instruções.

Um dos objectivos do invento consiste em ultrapassar os anteriormente referidos, e outros, inconvenientes da técnica anterior. Por conseguinte, o invento proporciona um método próprio para modificar a função de uma instrução num conjunto de instruções de um processador de um cartão inteligente sem adição de comandos, sendo a nova função baseada na instrução do conjunto de instruções original, compreendendo o cartão inteligente ainda uma memória própria para armazenar ficheiros, caracterizado por serem utilizadas tabelas de atributos (por exemplo, CA (condição de acesso), NRCHAVE (número da chave), CHAVE 1) associados aos ficheiros e às instruções (por exemplo, LER) do conjunto de instruções próprias para modificar as funções das instruções, indo a modificação ocorrer apenas nos atributos que especificam a



propriedade da respectiva instrução.

Isto é, de acordo com o presente invento, as instruções são modificadas através da modificação dos seus atributos. Como os atributos podem ser organizados em grupos associados a ficheiros específicos, o método do presente invento permite que as instruções possam ser modificadas de uma maneira selectiva, isto é, modificadas para ficheiros específicos. Tipicamente, um atributo especifica uma condição de acesso ou uma chave específica destinada a ser utilizada pela instrução em questão. No entanto, o atributo pode conter um código de máquina (ou um indicador para um código de máquina) que especifique uma outra operação que desempenhe uma função específica (como por exemplo um processo criptográfico). Através da inserção de uma nova operação, ou de uma operação modificada, num atributo, a função de uma instrução pode ser modificada sem se alterar a instrução propriamente dita.

Será fácil de perceber que a inserção de um atributo pode implicar a substituição de um atributo existente. De uma maneira geral, as localizações da memória podem ser reservadas para a armazenagem de atributos. A inserção de um novo atributo implica geralmente a armazenagem do novo atributo na correspondente localização da memória, indo nesse caso o novo atributo ser escrito por cima de qualquer informação previamente armazenada na localização da memória, informação essa que irá portanto ser apagada.

O método de acordo com o invento pode ser aplicado em situações em que os grupos de atributos do conjunto de instruções compreendem uma primeira tabela contendo primeiros atributos e uma segunda tabela contendo segundos atributos, contendo a primeira tabela referências à segunda tabela e em que um novo atributo é inserido na segunda tabela. Uma primeira tabela desse tipo pode, por exemplo, compreender a referida chave específica, enquanto que a



segunda tabela contém processos (operações) destinados a ser utilizados em combinação com as instruções em questão. Chama-se a atenção para o facto de que a primeira tabela pode ser obtida através de uma tabela de base contendo referências. Através da inserção de um novo atributo na segunda tabela, a modificação é obtida com uma alteração mínima nos atributos.

Os modernos cartões inteligentes podem ter pelo menos dois ficheiros de dados diferentes, por exemplo para diferentes aplicações do cartão inteligente. Nesse caso, um grupo de atributos pode compreender subgrupos associados aos respectivos ficheiros de dados. O invento permite que um novo atributo possa ser inserido num número limitado de subgrupos, indo desse modo fazer modificações de instruções específicas para ficheiros de dados individuais. Deste modo pode obter-se uma grande flexibilidade de instruções.

O invento irá agora ser descrito de uma maneira mais pormenorizada, a título de exemplo, com referência aos desenhos anexos, nos quais:

- a Fig. 1 mostra, em perspectiva, um cartão inteligente tal como os que são utilizados para efeitos de pagamento e de identificação;
- a Fig. 2 mostra esquematicamente o circuito integrado do cartão inteligente da Fig. 1;
- a Fig. 3 mostra esquematicamente uma tabela de atributos de um conjunto de instruções de um cartão inteligente, por exemplo do cartão inteligente da Fig. 2;
- a Fig. 4 mostra esquematicamente uma tabela de chaves associada à tabela de atributos da Fig. 3;
- a Fig. 5 mostra esquematicamente uma tabela de procedimentos associada à tabela de atributos da Fig. 3 e à tabela de chaves da Fig. 4; e



a Fig. 6 mostra esquematicamente um exemplo de uma estrutura hierárquica de ficheiros de um cartão inteligente.

Fazendo agora referência à Fig. 1, vemos que o cartão inteligente ou cartão IC 1 se encontra representado esquematicamente e compreende um substrato 2 no qual é embutido um circuito integrado. O circuito integrado é dotado de contactos 3 próprios para estabelecer contacto com um leitor de cartões ou com qualquer outro dispositivo semelhante. Chama-se a atenção para o facto de que o presente invento também pode ser aplicado no caso dos chamados cartões inteligentes destituídos de contactos.

O circuito integrado 10, que se acha representado esquematicamente e a título de exemplo na Fig. 2, compreende um processador 11, uma memória 12 e um circuito de entrada/saída 13. A memória pode compreender uma parte constituída por uma memória volátil (RAM), própria para armazenar dados de uma maneira temporária, e uma parte constituída por uma memória não volátil (ROM), própria para armazenar dados de uma maneira permanente ou semi-permanente. A última parte é de preferência uma memória do tipo EEPROM (Electrically Erasable Read Only Memory). Os dados armazenados na parte não volátil podem conter tanto dados de programação (instruções, programas) como dados de pagamento, isto é, dados respeitantes a transacções monetárias. Será fácil de perceber que pode ser proporcionada a existência de uma memória separada (não representada) própria para armazenar o conjunto de instruções do processador 11.

O processador 11 pode ser um microprocessador dotado de um conjunto de instruções normalizadas, por exemplo de acordo com a Norma Europeia EN726. Será fácil de perceber que também podem ser utilizadas outras normas, ou conjuntos de instruções não normalizadas. O conjunto de instruções



será melhor explicado com referência à Fig. 3.

O circuito de entrada/saída 13 lida com a comunicação entre o processador 11 e dispositivos externos (não representados) tais como leitores de cartões. O circuito de entrada/saída 13, que pode conter adequadas memórias intermediárias, encontra-se ligado ao processador 11 por intermédio de um barramento (bus) de dados. O processador 11 e a memória 12 podem ser ligados por meio do mesmo barramento de dados.

A tabela de atributos que se acha representada esquematicamente e a título de exemplo na Fig. 3 e que é designada genericamente pelo número de referência 100, compreende várias partes associadas a diferentes ficheiros (mais adiante será explicada com referência à Fig. 6 uma possível estrutura de ficheiros do cartão inteligente). Uma primeira parte associada ao ficheiro A (21 na Fig. 6), compreende os campos 111, 121 e 131. O primeiro campo 111 contém o indicador do ficheiro, neste caso designado por "Ficheiro A". O segundo campo 121 contém o conjunto de instruções, isto é, uma tabela contendo o conjunto de instruções do cartão inteligente, ou pelo menos referências às instruções do conjunto de instruções. Será fácil de perceber que as instruções propriamente ditas compreendem o código de máquina executado pelo processador. No exemplo representado, encontram-se indicadas as instruções "LER", "ESCREVER" e "ACTUALIZAR". O terceiro campo 131 contém atributos das instruções presentes no campo 121. Isto é, para cada uma das instruções do segundo campo pode existir uma entrada no terceiro campo 131, indo essa entrada constituir um grupo de atributos que especificam melhor o funcionamento da instrução. Os atributos podem, por exemplo, compreender condições de acesso e números das chaves, indicados na Fig. 3 por CA e NRCHAVE, respectivamente. As condições de acesso podem compreender SEMPRE, NUNCA, PROTEGIDO, e outras semelhantes. Os números das chaves



podem reportar-se a entradas na Tabela de Chaves representada na Fig. 4. O terceiro campo 131 da tabela 100 pode portanto constituir uma tabela de base de atributos, que se reporta a outras tabelas (representada na Fig. 4).

Apesar dos primeiro, segundo e terceiro campos da tabela de atributos 100 se acharem representados na Fig. 3 sob a forma de campos adjacente por razões de maior clareza, nos modos de realização reais os campos podem ser armazenados em locais diferentes, não adjacentes, da memória 12 do cartão inteligente.

Os atributos indicados no campo 131 correspondem todos ao Ficheiro A, conforme especificado no campo 111. Isto é, os atributos do campo 131 só são válidos para o Ficheiro A. Uma estrutura desse tipo permite que as instruções possam ter diferentes funcionalidades para diferentes (dados) ficheiros. Um ficheiro desse tipo pode conter dados que dizem respeito a uma aplicação (função) específica do cartão inteligente. Entre as aplicações típicas encontram-se incluídas as de "porta-moedas", "programa de fidelidade" e "acesso", próprias para fazer ou receber pagamentos, receber créditos de fidelidade, e ter acesso a edifícios e outros locais semelhantes. Mesmo dentro de uma dessas aplicações pode utilizar-se mais do que um ficheiro de dados, e por conseguinte pode existir mais do que um grupo de atributos associado. Em consequência do facto dos atributos serem específicos para um ficheiro de dados, a função de uma instrução pode, pelo menos para as partes definidas pelos atributos, ser específica para um ficheiro de dados. Portanto, as condições de acesso da instrução "LER" podem variar entre um ficheiro contendo por exemplo dados de porta-moedas (armazenagem de dinheiro electrónico) e um ficheiro contendo dados pessoais do utilizador do cartão inteligente. Isto será melhor explicado com referência às Figs. 4 e 5.



As condições de acesso reais, representadas simbolicamente na Fig. 3 por CA, podem estar contidas na tabela de base de atributos 100, ou podem estar contidas numa tabela separada (não representada). De modo semelhante, as chaves (CHAVE 1, CHAVE 2, ...) representadas na Fig. 4 podem estar contidas na tabela de atributos 100. Por razões relacionadas com a explanação do invento, irá partir-se do princípio de as entradas NRCHAVE, que podem ser simplesmente números (1, 2, ...), dizem respeito à Tabela de Chaves 200 da Fig. 4.

Cada entrada na Tabela de Chaves 200 da Fig. 4 contém um número da chave (NRCHAVE), uma chave (CHAVE 1, CHAVE 2, ...) e uma identificação do procedimento ou número do procedimento (indicado nas Figs. 4 e 5 por NRPRO). Cada identificação de procedimento diz por sua vez respeito a uma entrada na Tabela de Procedimentos 300. Cada entrada na Tabela de Procedimentos 300 contém um número de procedimento e um procedimento (operação), indicado na Fig. 5 por DES ou RSA. Esse procedimento pode ser um procedimento criptográfico, como por exemplo DES e RSA, ou quaisquer outras operações sobre dados.

De acordo com o presente invento, as instruções de um cartão inteligente podem ser modificadas mediante modificação dos seus atributos. Por conseguinte, mediante a modificação de uma entrada na Tabela de Procedimentos 300 é possível obter-se uma nova função ou uma modificação de uma função existente. Na Fig. 5 é possível ver que na segunda entrada da Tabela de Procedimentos foi introduzida uma nova função (por exemplo, multiplicar os dados por um factor comum, ou subtrair um dos dados). Portanto, se na Tabela de Chaves 200 for escolhida a Chave Nr. 3, o Número do Procedimento diz respeito ao Procedimento Nr. 2, sendo essa a nova função. Cada vez que for executada uma instrução que implique a utilização da CHAVE 3, irá ser invocada a nova função.



Será fácil de perceber que as referências a uma nova função podem ser feitas de várias maneiras, por exemplo directamente a partir da tabela 100 da Fig. 3. A Tabela de Chaves 200 também pode conter chaves "fictícias", de maneira a permitir a utilização da tabela sem realmente utilizar uma chave.

Em vez de se inserir a nova função na Tabela de Procedimentos 300, pode-se inserir nessa mesma tabela um indicador que indica qual a localização da memória onde é armazenado o novo código ou o código modificado.

Conforme foi anteriormente explicado, na tabela de base de atributos (100 na Fig. 3) podem existir diferentes atributos para diferentes ficheiros. O método de acordo com o invento permite a existência de um conjunto de instruções flexível mediante modificação dos atributos de ficheiros de dados individuais.

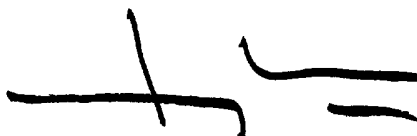
Os cartões inteligentes podem compreender uma estrutura de directórios hierarquizada para organizar os seus ficheiros. Na Fig. 6 encontra-se representado um exemplo de uma estrutura desse tipo. Um ficheiro principal 20 tem três subficheiros 21, 22 e 23. Isto é, o ficheiro principal pode conter referências aos subficheiros, ou então essas referências podem ser armazenadas em qualquer outro local (por exemplo num directório comum). Um grupo de atributos é associado ao ficheiro principal 20. É possível ter grupos individuais de atributos para todos os três subficheiros 21, 22 e 23, conforme representado na Fig. 3. No entanto, no caso de um grupo de atributos ser associado ao ficheiro 20, o referido grupo de atributos pode ser aplicável a todos os ficheiros hierarquicamente mais baixos em relação ao ficheiro principal 20. Isto é, o mesmo grupo de atributos pode ser também associado aos ficheiros 21, 22 e 23. Por outras palavras, se uma instrução for alterada mediante a modificação de um

atributo (de um grupo de atributos) associado a um determinado ficheiro, a modificação pode ser válida para todos os ficheiros hierarquicamente mais baixos em relação ao referido ficheiro. Isto permite que uma instrução possa ser alterada, por exemplo para uma aplicação específica do cartão no caso dessa aplicação envolver vários ficheiros.

Conforme foi anteriormente explicado, de acordo com o presente invento, a modificação das instruções é obtida através da substituição e/ou da modificação dos atributos. Portanto, o método do invento permite a utilização de instruções normalizadas (funções de cartão normalizadas) para efectuar operações não normalizadas. O invento também proporciona um conjunto de instruções modificadas de um cartão inteligente, assim como um cartão inteligente dotado de um conjunto de instruções modificadas. A inserção efectiva de um novo atributo numa tabela de atributos é feita através da armazenagem do novo atributo numa adequada localização da memória. Os dados que representam o novo atributo podem ser transferidos de um computador para a memória do cartão através de um leitor/escritor de cartões. Com referência à Fig. 2, vemos que os dados são transferidos da maneira usual para a memória 12 por intermédio da unidade de I/O 13 (isto é, da unidade de Entrada/Saída).

Para os entendidos na matéria será fácil de perceber que os modos de realização aqui anteriormente descritos são dados apenas a título de exemplo e que é possível efectuar muitas modificações e adições sem se sair do âmbito do presente invento, tal como este é reivindicado.

Lisboa, 17 de Julho de 2000



JORGE CRUZ
Agente Oficial da Propriedade Industrial
RUA VICTOR CORDON, 14
1200 LISBOA



REIVINDICAÇÕES

1. Método para modificar a função de uma instrução num conjunto de instruções de um processador (11) de um cartão inteligente (1) sem adição de comandos, sendo a nova função baseada na instrução do conjunto de instruções original, compreendendo ainda o cartão inteligente uma memória (12) própria para armazenar ficheiros (20), caracterizado por serem utilizadas tabelas (100, 200, 300) de atributos (por exemplo, CA (condição de acesso), NRCHAVE (número da chave), CHAVE 1) associados aos ficheiros (20) e às instruções (por exemplo, LER) do conjunto de instruções para modificar as funções das instruções, indo a modificação ocorrer apenas nos atributos que especificam a propriedade da respectiva instrução.

2. Método de acordo com a reivindicação 1, em que os grupos de atributos são organizados numa primeira tabela (100) que se reporta a uma outra tabela (200, 300), e em que um novo atributo (NOVA FUNÇÃO) é inserido numa outra tabela (por exemplo na tabela 300).

3. Método de acordo com a reivindicação 1 ou 2, em que a inserção de um novo atributo implica a substituição de um atributo existente.

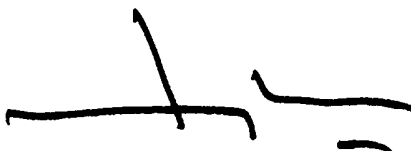
4. Método de acordo com qualquer uma das reivindicações 1 a 3, em que a memória (12) do cartão inteligente (1) compreende pelo menos dois ficheiros (por exemplo 21, 22), encontrando-se a cada um dos ficheiros associado um grupo de atributos (por exemplo 131), indo um novo atributo ser inserido num número limitado de grupos.

5. Método de acordo com qualquer uma das reivindicações 1 a

4, em que os ficheiros (por exemplo 21, 22) são organizados de uma maneira hierárquica, indo cada um dos grupos de atributos ser associado a pelo menos um ficheiro (por exemplo 20) e a todos os ficheiros (por exemplo 21, 22) hierarquicamente inferiores em relação ao referido ficheiro (20).

6. Método de acordo com qualquer uma das reivindicações 1 a 5, em que a todos os ficheiros do cartão inteligente (1) é associado um conjunto de atributos.

Lisboa, 17 de Julho de 2000



JORGE CRUZ
Agente Oficial da Propriedade Industrial
RUA VICTOR CORDON, 14
1200 LISBOA

[Handwritten signature]

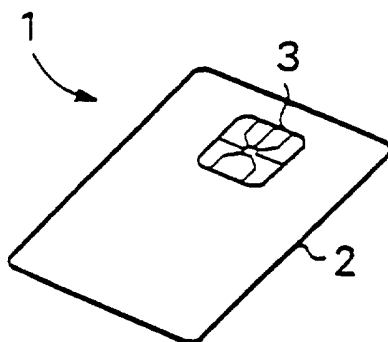


Fig. 1

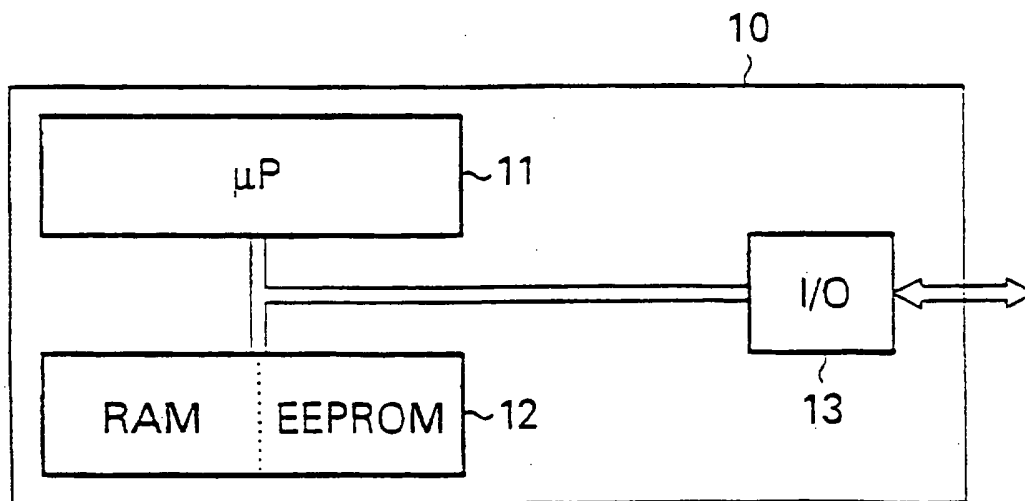


Fig. 2

100

2

TABELA DE ATRIBUTOS		
FICHEIRO A	LER ESCREVER ACTUALIZAR . . .	[AC], [KEYNR.] [AC], [KEYNR.] [AC], [KEYNR.] . . .
<u>111</u>	<u>121</u>	<u>131</u>
FICHEIRO B	LER ESCREVER	[AC], [KEYNR.] [AC], [KEYNR.]
<u>112</u>	<u>122</u>	<u>132</u>
....		

Fig. 3

200

TABELA DE CHAVES		
CHAVE NR.	CHAVE	PRONR.
1	CHAVE 1	1
2	CHAVE 2	3
3	CHAVE 3	2
.	.	.
.	.	.
.	.	.
.	.	.
.	.	.

Fig. 4

300

TABELA DE PROCEDIMENTOS	
PRONR.	PROCEDIMENTO
1	[DES]
2	[NOVA FUNÇÃO]
3	[RSA]
.	.
.	.
.	.
.	.

Fig. 5

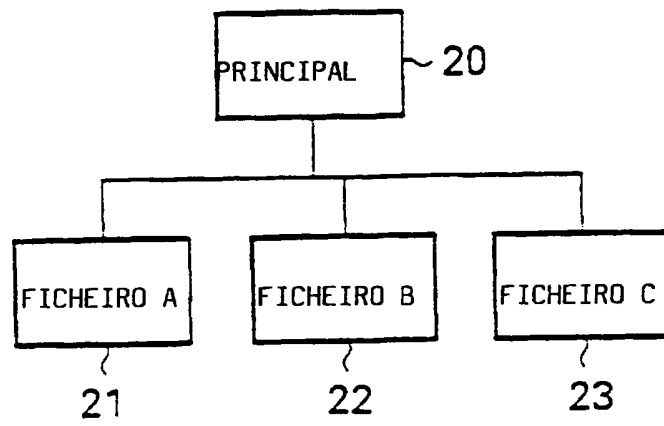


Fig. 6