

①9 BUNDESREPUBLIK  
DEUTSCHLAND



DEUTSCHES  
PATENT- UND  
MARKENAMT

⑫ **Offenlegungsschrift**  
⑩ **DE 102 20 629 A 1**

⑤1 Int. Cl.<sup>7</sup>:  
**G 06 F 3/06**  
G 06 F 13/12  
G 06 F 12/14

⑳ Aktenzeichen: 102 20 629.5  
㉒ Anmeldetag: 8. 5. 2002  
㉔ Offenlegungstag: 27. 11. 2003

DE 102 20 629 A 1

㉑ Anmelder:  
Infineon Technologies AG, 81669 München, DE  
  
㉔ Vertreter:  
Epping Hermann Fischer,  
Patentanwaltsgesellschaft mbH, 80339 München

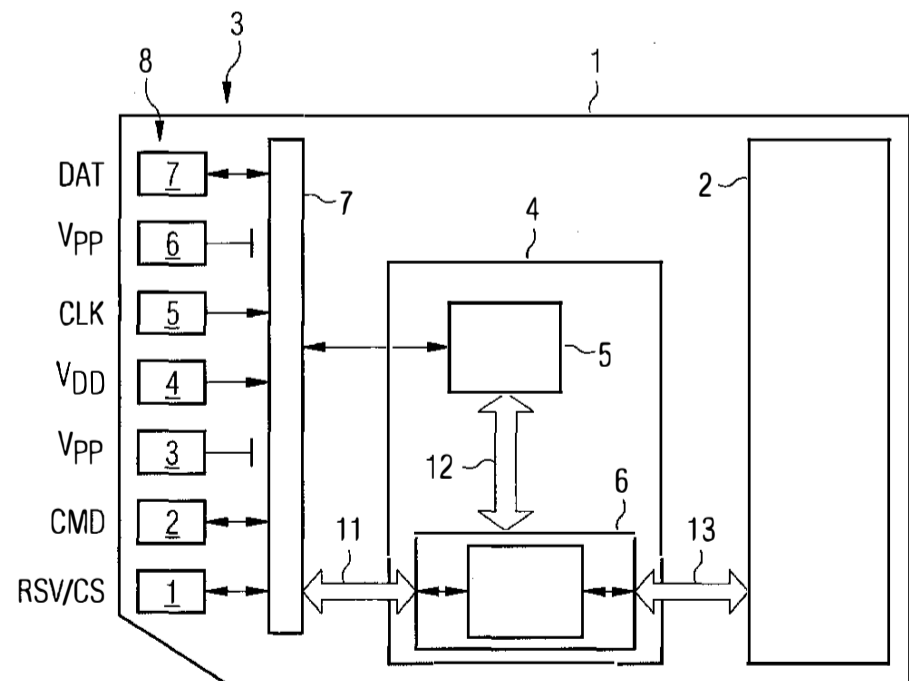
㉒ Erfinder:  
Böker, Thorsten, Dr., 85579 Neubiberg, DE  
  
⑤6 Entgegenhaltungen:  
US 56 23 637 A  
SMART CARDS (online), Im Internet:  
URL.:<http://www.uni-weimar.de/~schott2/sc/>

**Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen**

Prüfungsantrag gem. § 44 PatG ist gestellt

⑤4 Datenträger

⑤7 Die Erfindung betrifft einen Datenträger (1) mit einem nichtflüchtigen Speicher (2), einer Datenschnittstelle (3), über die Daten in den nichtflüchtigen Speicher (2) schreibbar und aus diesem lesbar sind, und einem Interface-Modul (4), das zwischen die Datenschnittstelle (3) und den Speicher (2) geschaltet ist und durch das die Daten ver- und/oder entschlüsselbar sind. Der erfindungsgemäße Datenträger (1) ist dadurch gekennzeichnet, daß das Interface-Modul (4) eine Steuereinheit (5) und eine mit dieser verbundene Logikkomponente (6) aufweist, wobei die Ver- und/oder Entschlüsselung durch die Logikkomponente (6) erfolgt und der anzuwendende Schlüssel durch die Steuereinheit (5) festlegbar ist.



DE 102 20 629 A 1

[0001] Die Erfindung betrifft einen Datenträger mit einem nicht-flüchtigen Speicher, einer Datenschnittstelle, über die Daten in den nichtflüchtigen Speicher schreibbar und aus diesem lesbar sind und einem Interface-Modul, das zwischen die Datenschnittstelle und den Speicher geschaltet ist und durch das die Daten ver- und/oder entschlüsselbar sind.

[0002] Solche Datenträger werden beispielsweise als Speicherkarten verwendet. Dabei können auf einer kleinen Karte Daten jeglicher Art gespeichert werden. Ein Host sendet die Daten über ein Interface an die Karte. Handelt es sich um sensitive Daten, so werden die Daten üblicherweise verschlüsselt abgespeichert. Um die Daten zu ver- und zu entschlüsseln, stehen im Prinzip zwei Möglichkeiten zur Verfügung. Entweder der Host oder die Karte selber übernehmen diese Aufgabe. Da jedoch die angestrebten Datenraten sehr hoch sind, muß die Übertragung mit Ver- beziehungsweise Entschlüsselung sehr schnell geschehen und im besten Fall mit derselben Geschwindigkeit als würden die Daten nicht verschlüsselt.

[0003] Wenn die Ver- und Entschlüsselung durch den Host geschieht, ist dies weniger problematisch, da dort in der Regel genügend Prozessorleistung zur Verfügung steht. Viele Speicherkarten sind jedoch so konzipiert, daß sie von nahezu allen Hosts, die zu unterschiedlichen Applikationen gehören können, gelesen und beschrieben werden können. Speichert also eine erste Applikation einen Datensatz, den sie zuvor mit einem bestimmten Algorithmus verschlüsselt hat, so muß der Host einer zweiten Applikation, durch die der Datensatz wieder gelesen werden soll, ebenfalls über diesen Algorithmus verfügen, da sonst die Daten nicht wieder entschlüsselt werden können.

[0004] Aus diesem Grund ist es von Vorteil, wenn die Karte selbst das Ver- und Entschlüsseln übernimmt, da in diesem Fall nicht zuvor bekannt sein muß, mit welchen Applikationen die Speicherkarte zusammenarbeiten soll und es muß nicht dafür Sorge getragen werden, daß diese Applikationen die passenden Algorithmen besitzen.

[0005] Bei Datenträgern sind heutige Chipkartencontroller in der Lage, nahezu sämtliche Verschlüsselungsalgorithmen auf beliebige Daten anzuwenden. Hinsichtlich einer flexiblen Datenverschlüsselung ist dies eine praktikable Lösung, allerdings sind die Datenraten äußerst begrenzt. Sie liegen heute bei zirka 100 kbit pro Sekunde und erfüllen damit nicht annähernd die geforderten Datenraten einer Speicherkarte, die über 10 Mbit pro Sekunde liegen. Mit üblichen Chipkartencontrollern kann die Ver- und Entschlüsselung daher nur sehr langsam durchgeführt werden. Leistungsfähigere Controller mit ausreichender Prozessorleistung sind prinzipiell zwar machbar, aus Kostengründen meist aber nicht einsetzbar.

[0006] Die Aufgabe der Erfindung besteht daher darin, einen Datenträger anzugeben, der dazu geeignet ist, eine Datenver- und/oder -entschlüsselung mit einer wesentlich höheren Geschwindigkeit durchzuführen, ohne daß dazu ein besonders leistungsfähiger Prozessor erforderlich ist.

[0007] Diese Aufgabe wird durch einen Datenträger der eingangs genannten Art gelöst, der dadurch gekennzeichnet ist, daß das Interface-Modul eine Steuereinheit und eine mit dieser verbundene Logikkomponente aufweist, wobei die Ver- und/oder Entschlüsselung durch die Logikkomponente erfolgt und der anzuwendende Schlüssel durch die Steuereinheit festlegbar ist.

[0008] Das Interface-Modul eines erfindungsgemäßen Datenträgers ist also zweigeteilt. Einerseits besitzt es eine Steuereinheit, die ein herkömmlicher Chipkartencontroller oder ein Teil davon sein kann, zur Steuerung der Abläufe

und Vorgabe der zu verwendenden Schlüssel. Andererseits weist das Interface-Modul eine Logikkomponente auf, die für den Ver- und/oder Entschlüsselungsvorgang selber zuständig und für diese Aufgabe optimiert ist. Eine hardwaretechnische Lösung zur Umsetzung einer Funktion ist dabei immer wesentlich schneller als eine softwaretechnische Umsetzung.

[0009] Der Vorteil einer solchen Anordnung liegt darin, daß eine leistungsfähige Logikkomponente wesentlich günstiger herzustellen ist als ein für diese Aufgabe geeigneter Prozessor.

[0010] Eine besonders flexible Lösung zur Bereitstellung der Logikkomponente besteht darin, diese durch eine funktionsprogrammierbare Logikschaltung bereitzustellen. Dadurch ist das Interface-Modul an geänderte Anforderungen anpaßbar.

[0011] Weitere vorteilhafte Ausgestaltungen der Erfindung sind in den Unteransprüchen angegeben.

[0012] Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels näher erläutert. Fig. 1 zeigt einen erfindungsgemäßen Datenträger in einer schematischen Darstellung.

[0013] Die Figur zeigt einen Datenträger 1, in diesem Fall eine Speicherkarte. Die Speicherkarte besitzt einen nicht-flüchtigen Speicher 2, vorzugsweise einen Flash-Speicher, der eine hohe Kapazität besitzt, damit die Speicherkarte als Massenspeichermedium geeignet ist. Zur Verbindung mit einem Host ist die Speicherkarte mit einer Datenschnittstelle 3 ausgestattet. Zur Kontaktierung sind Kontaktflächen 8 vorgesehen, die im Betrieb mit verschiedenen Signalen beaufschlagt werden, wie einem Taktsignal CLK, einer Betriebsspannung VDD, einem Steuerbefehl CMD und vor allem mit einem Datensignal DAT. Eine Eingangsschaltung 7 ist zum Empfang dieser Signale vorgesehen und stellt darüber hinaus eine Treiberebene dar, durch die eine Anpassung an verschiedene Hosts durchgeführt wird, so daß die Speicherkarte flexibel mit verschiedenen Hosts beziehungsweise Applikationen eingesetzt werden kann. Ebenfalls ist an dieser Stelle eine Umwandlung serieller Signale in parallele Signale und umgekehrt möglich.

[0014] Die Datenschnittstelle 3 ist mit einem Interface-Modul 4 verbunden, das im gezeigten Ausführungsbeispiel aus einem Controller 5 und einer Logikkomponente 6 besteht. Die Logikkomponente 6 besitzt drei Schnittstellen. Über eine erste Schnittstelle 11 ist eine Verbindung zu der Datenschnittstelle 3 gegeben, eine zweite Schnittstelle 12 verbindet die Logikkomponente 6 mit dem Controller 5 und eine dritte Schnittstelle 13 verbindet die Logikkomponente 6 mit dem Speicher 2.

[0015] Daten, die von der Datenschnittstelle 3 zu dem Speicher 2 zu übertragen sind, werden in der Logikkomponente 6 verschlüsselt. Beim Lesen von Daten aus der Speicherkarte werden Daten von dem Speicher 2 zu der Datenschnittstelle 3 übermittelt, wobei durch die Logikkomponente 6 eine Entschlüsselung erfolgt. Der Datenpfad zur Ver- und Entschlüsselung verläuft in beiden Fällen ausschließlich über die Logikkomponente 6, aber nicht über den Controller 5. Dieser ist lediglich für Steuer- und Überwachungsaufgaben zuständig.

[0016] Der durch die Logikkomponente 6 anzuwendende Schlüssel wird durch den Controller 5 vorgegeben. Der Controller übernimmt aber auch weitere Aufgaben. Diese liegen in der Kontrolle des Datenstromes, wodurch sichergestellt wird, daß die Daten richtig geschrieben und gelesen werden. Angewendete Mechanismen sind beispielsweise Bad-Block-Management oder die Überwachung "Physical versus Logical Memory Address".

[0017] In einer vorteilhaften Implementierung wird die

Logikkomponente **6** als zusätzliches Modul eines Chipkartencontrollers **5** ausgeführt. Dadurch ist eine kompakte und kostengünstige Realisierung möglich.

|  |    |
|--|----|
| Bezugszeichenliste                                   | 5  |
| <b>1</b> Speicherkarte                               |    |
| <b>2</b> nicht-flüchtiger Speicher                   |    |
| <b>3</b> Datenschnittstelle                          |    |
| <b>4</b> Interface-Modul                             | 10 |
| <b>5</b> Controller                                  |    |
| <b>6</b> Logikkomponente                             |    |
| <b>7</b> Eingangsschaltung                           |    |
| <b>8</b> Kontaktflächen                              |    |
| <b>11, 12, 13</b> Schnittstellen der Logikkomponente | 15 |

#### Patentansprüche

1. Datenträger mit
  - einem nichtflüchtigen Speicher (**2**), 20
  - einer Datenschnittstelle (**3**), über die Daten in den nichtflüchtigen Speicher (**2**) schreibbar und aus diesem lesbar sind, und
  - einem Interface-Modul (**4**), das zwischen die Datenschnittstelle (**3**) und den Speicher (**2**) 25 geschaltet ist und durch das die Daten ver- und/oder entschlüsselbar sind,

**dadurch gekennzeichnet**, daß das Interface-Modul (**4**) eine Steuereinheit (**5**) und eine mit dieser verbundene Logikkomponente (**6**) aufweist, wobei die Ver- und/ 30 oder Entschlüsselung durch die Logikkomponente (**6**) erfolgt und der anzuwendende Schlüssel durch die Steuereinheit (**5**) festlegbar ist.
2. Datenträger nach Anspruch 1, dadurch gekennzeichnet, daß es sich um eine Massenspeicherkarte 35 handelt.
3. Datenträger nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Steuereinheit (**5**) durch einen Mikrocontroller gebildet ist.
4. Datenträger nach einem der Ansprüche 1 bis 3, da- 40 durch gekennzeichnet, daß die durch die Logikkomponente (**6**) ver- und/oder entschlüsselbaren Daten eine Datenrate größer als 10 Mbit/s aufweisen.
5. Datenträger nach einem der Ansprüche 1 bis 4, da- 45 durch gekennzeichnet, daß die Logikkomponente (**6**) eine funktionsprogrammierbare Logikschaltung ist.

---

Hierzu 1 Seite(n) Zeichnungen

---

50

55

60

65

