(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 10 2006 045 906 A1** 2008.04.17

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2006 045 906.7**
(22) Anmeldetag: **28.09.2006**
(43) Offenlegungstag: **17.04.2008**

(51) Int Cl.[8]: ***G06K 19/073*** (2006.01)

(71) Anmelder:
Infineon Technologies AG, 81669 München, DE

(72) Erfinder:
Janke, Marcus, 81541 München, DE; Laackmann, Peter, Dr., 81541 München, DE

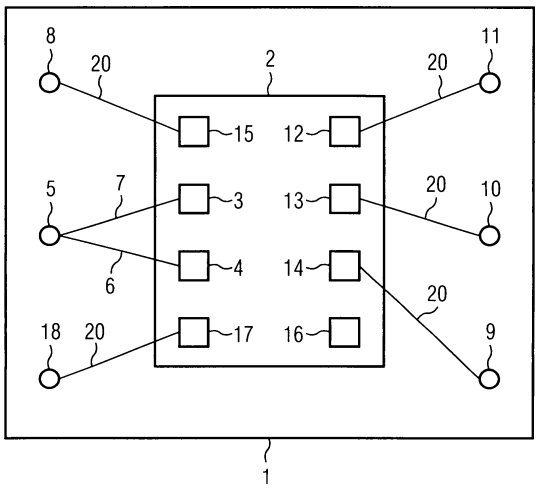
(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
DE 196 34 133 C2
DE 196 10 070 A1
DE 103 09 313 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gemäß § 44 PatG ist gestellt.

(54) Bezeichnung: **Modul mit einem Controller für eine Chipkarte**

(57) Zusammenfassung: Bei einem Modul (1) mit einem Controller (2) für eine Chipkarte weist der Controller (2) zwei I/O-Pads (3, 4) zur Ein- und Ausgabe von Daten und das Modul (1) ein I/O-Pad (5) auf. Beide I/O-Pads (3, 4) des Controllers (2) sind mit dem einen I/O-Pad (5) des Moduls (1) verbunden. Auf diese Weise können über ein I/O-Pad des Controllers (2) ausgegebene Daten vom Controller (2) über das andere I/O-Pad (3) des Controllers (2) eingelesen und überwacht werden.



Beschreibung

[0001] Die vorliegende Erfindung bezieht sich auf eine Halbleitervorrichtung im Allgemeinen und insbesondere auf ein Modul mit einem Controller für eine Chipkarte und auf ein Verfahren zum Erkennen eines Angriffs auf einen Controller eines Moduls für eine Chipkarte.

[0002] Chipkarten besitzen meistens acht Kontaktfelder, von denen in der Regel fünf genutzt werden. Diese sind die elektrische Schnittstelle zwischen beispielsweise einem Terminal und dem Controller der Chipkarte. Eines dieser Kontaktfelder ist ein so genanntes I/O-Pad zum kommunizieren mit externen Systemen. Controller besitzen ebenfalls mindestens ein I/O-Pad zur Kommunikation mit der Außenwelt und sind mit dem Kontaktfeld der Chipkarte verbunden. Auf modernen Sicherheits-Controllern findet man meist zwei I/O-Pads, von denen in der Regel jedoch nur eines mit dem entsprechenden Pad des Chipkarten-Moduls verbunden ist. Der zweite I/O-Port des Controllers bleibt also in der Regel bei der endgültigen Montage ungenutzt.

[0003] Bei herkömmlichen Sicherheits-Controllern ist es sehr schwierig zu überprüfen, welche Daten wirklich vom Sicherheits-Controller über ein I/O-Pad nach außen gelangen. Sollte etwa durch einen Angriff von außen der Programmablauf des Sicherheits-Controllers geändert werden, können unbemerkt beispielsweise vertrauliche Daten nach außen gelangen. Üblicherweise versucht man, den Programmablauf durch geeignete Softwaregegenmaßnahmen zu schützen. Diese Softwaregegenmaßnahmen bieten jedoch nur einen begrenzten Schutz.

[0004] Des Weiteren sind verschiedenste Sensoren zur Erkennung von Angriffen bekannt. Diese erkennen einen großen Teil der Angriffe, leisten aber ebenso keine tatsächliche Überprüfung der korrekten Situation der Datenausgabe.

[0005] Es ist eine Aufgabe der vorliegenden Erfindung, ein Modul für eine Chipkarte mit einer erhöhten Sicherheit gegen Angriffe sowie ein verbessertes Verfahren zum Erkennen eines solchen Angriffs bereitzustellen.

[0006] Diese Aufgabe wird durch ein Modul mit den Merkmalen des Anspruchs 1 und ein Verfahren mit den Merkmalen des Anspruchs 6 gelöst. Die jeweiligen Unteransprüche definieren jeweils vorteilhafte Weiterbildungen.

[0007] Ein Aspekt der vorliegenden Erfindung ist das Verbinden von zwei I/O-Pads des Controllers mit nur einem I/O-Pad des Moduls der Chipkarte.

[0008] Durch die Verbindung zweier I/O-Pads des Controllers mit einem I/O-Pad des Moduls können die von einem ersten I/O-Pad gesendeten Daten mittels eines zweiten I/O-Pads durch den Controller überprüft werden.

[0009] Der Controller der Chipkarte kann in einer weiteren Ausprägung ein Sicherheits-Controller sein.

[0010] Eine weiteres Ausführungsbeispiel des Moduls für eine Chipkarte besteht darin, dass dieses so eingerichtet ist, dass es falsche Daten oder zu lange Antwortzeiten mittels des Controllers erkennt und in diesem Fall einen Alarm auslöst.

[0011] Weiters kann es von Vorteil sein, wenn das Modul der Chipkarte nach der Erkennung eines Angriffs oder zu langer Antwortzeiten sich selbst deaktiviert und dadurch ein Angriff obsolet wird.

[0012] Bei einem Controller mit zwei I/O-Pads zur Ein- und Ausgabe von Daten und einem Modul mit einem I/O-Pad, wobei die beiden I/O-Pads des Controllers mit dem einen I/O-Pad des Modules verbunden sind, werden die gesendeten Daten des ersten I/O-Pads des Controllers mittels des Controllers durch über das zweite I/O-Pad des Controllers empfangene Daten überwacht.

[0013] Eine weitere Ausprägung des Verfahrens besteht darin, dass bei der Erkennung falscher Daten oder zu langer Antwortzeiten ein Alarm ausgelöst wird.

[0014] Weiters ist ein Ausführungsbeispiel der vorliegenden Erfindung denkbar, welches nach Erkennung falscher Daten oder zu langer Antwortzeiten eine Deaktivierung des gesamten Chipkarten-Moduls veranlasst.

[0015] Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels mit Bezugnahme auf die beigefügte Zeichnung näher erläutert, in der

[0016] Fig. 1 eine Prinzipdarstellung eines Ausführungsbeispiels eines erfindungsgemäßen Moduls mit einem Controller für eine Chipkarte zeigt.

[0017] In Fig. 1 ist ein Modul **1** mit einem Controller **2** für eine Chipkarte gemäß einem Ausführungsbeispiel der Erfindung dargestellt. Auf dem Chipkarten-Controller **2** sind Pads **12**, **13**, **14**, **15**, **16**, **17**, **3**, **4** dargestellt, von denen in der Regel allerdings nur fünf Pads **12**, **13**, **15**, **3**, **4** genutzt werden. Dabei sind zwei I/O-Pads **3**, **4** zur Ein- und Ausgabe von Daten auf dem Controller **2** vorgesehen.

[0018] Auf dem Modul **1** sind weiters Pads **5**, **8**, **9**, **10**, **11**, **18** dargestellt. Es besteht eine Verbindung der beiden Controller-I/O-Pads **3**, **4** mit einem I/O-Pad **5** des Moduls **1** über zwei Verbindungen **6**, **7**.

[0019] Werden nun beispielsweise Daten zwischen dem I/O-Pad **3** des Controllers **1** über die Verbindung **7** und dem I/O-Pad **5** des Moduls **1** ausgegeben, kann nun mittels der anderen Verbindung **6** zwischen dem I/O-Pad **5** des Moduls **1** und dem zweiten I/O-Pad **4** des Controllers **2** durch den Controller **2** überprüft werden, ob die korrekten Daten am I/O-Pad **5** des Moduls **1** vorliegen.

[0020] Wenn umgekehrt zwischen dem I/O-Pad **4** des Controllers **2** über die Verbindung **6** und dem I/O-Pad **5** des Moduls **1** Daten versandt werden, kann mittels der anderen Verbindung **7** zwischen dem I/O-Pad **5** des Moduls **1** und dem zweiten I/O-Pad **3** des Controllers **2** durch den Controller **2** überprüft wird, ob die korrekten Daten am I/O-Pad **5** vorliegen. Erkennt der Controller **2**, dass die Daten am I/O-Pad **5** nicht korrekt sind, deaktiviert er sich oder begibt sich in einen Alarmzustand.

Bezugszeichenliste

1	Chipkarten-Modul
2	Controller
3	erstes I/O-Pad des Controllers
4	zweites I/O-Pad des Controllers
5	I/O-Pad des Moduls
6	erste Verbindung
7	zweite Verbindung
8	Spannung Pad **1** Modul
9	Reset Pad Modul
10	Clock Pad Modul
11	Spannung Pad **2** Modul
12	Versorgungsspannung Pad **2** Controller
13	Clock Pad Controller
14	Reset Pad Controller
15	Programmierspannung Pad **2** Controller (nicht benötigt)
16	Reserve Pad Controller
17	Ground Pad Controller
18	Ground Pad Modul
20	Verbindungen zwischen den Pads des Controllers und den Pads des Moduls

Patentansprüche

1. Modul (**1**) mit einem Controller (**2**) für eine Chipkarte, wobei der Controller (**2**) zwei I/O-Pads (**3**, **4**) zur Ein- und Ausgabe von Daten aufweist und das Modul (**1**) ein I/O-Pad (**5**) aufweist und die beiden I/O-Pads (**3**, **4**) des Controllers (**2**) mit einem I/O-Pad (**5**) des Moduls (**1**) verbunden sind.

2. Modul (**1**) nach Anspruch 1, bei dem über ein erstes I/O-Pad (**3**) des Controllers (**2**) gesendete Daten mittels eines zweiten I/O-Pads (**4**) durch den Controller (**2**) überwacht und auf Richtigkeit überprüft werden.

3. Modul (**1**) nach Anspruch 1 oder 2, wobei der Controller (**2**) ein Sicherheits-Controller ist.

4. Modul (**1**) nach einem der vorhergehenden Ansprüche, eingerichtet zum Erkennen falscher Daten oder zu langer Antwortzeiten und zur Auslösung eines Alarms.

5. Modul (**1**) nach einem der vorhergehenden Ansprüche, eingerichtet zum Erkennen falscher Daten oder zu langer Antwortzeiten und zur Deaktivierung desselben.

6. Verfahren zum Erkennen von Angriffen auf einen Controller (**2**) eines Moduls (**1**) für eine Chipkarte, wobei der Controller (**2**) zwei I/O-Pads (**3**, **4**) zur Ein- und Ausgabe von Daten und das Modul (**1**) ein I/O-Pad (**5**) zur Ein- und Ausgabe von Daten aufweist und die beiden I/O-Pads (**3**, **4**) des Controllers (**2**) mit dem I/O-Pad des Moduls verbunden sind, bei welchem Verfahren die mittels des Controllers (**2**) über ein erstes I/O-Pad (**3**) gesendeten Daten mittels des Controllers (**2**) durch über ein zweites I/O-Pad (**4**) empfangene Daten überwacht werden.

7. Verfahren nach Anspruch 6, wobei bei einer Erkennung falscher Daten oder zu langer Antwortzeiten ein Alarm ausgelöst wird.

8. Verfahren nach Anspruch 6 oder 7, wobei bei einer Erkennung falscher Daten oder zu langer Antwortzeiten der Controller (**2**) deaktiviert wird.

Es folgt ein Blatt Zeichnungen

Anhängende Zeichnungen