(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 602 13 878 T2** 2007.01.25

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 485 857 B1**
(21) Deutsches Aktenzeichen: **602 13 878.7**
(86) PCT-Aktenzeichen: **PCT/FR02/04285**
(96) Europäisches Aktenzeichen: **02 804 606.8**
(87) PCT-Veröffentlichungs-Nr.: **WO 2003/050750**
(86) PCT-Anmeldetag: **11.12.2002**
(87) Veröffentlichungstag der PCT-Anmeldung: **19.06.2003**
(97) Erstveröffentlichung durch das EPA: **15.12.2004**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **09.08.2006**
(47) Veröffentlichungstag im Patentblatt: **25.01.2007**

(51) Int Cl.[8]: ***G06K 7/00*** (2006.01)
G06K 19/07 (2006.01)

(30) Unionspriorität:
0116114 **13.12.2001** **FR**

(84) Benannte Vertragsstaaten:
DE, ES, FR, GB, IT

(73) Patentinhaber:
NAGRA THOMSON LICENSING, Boulogne-Billancourt, FR

(74) Vertreter:
Diehl & Partner, 80333 München

(72) Erfinder:
DAUVOIS, Jean-Luc, F-75116 Paris, FR; PERRINE, Jerôme, F-92100 Boulogne, FR

(54) Bezeichnung: **DIGITALES ELEKTRONISCHES BAUELEMENT, DAS GEGEN ELEKTRISCHE UND ELEKTROMAGNETISCHE ANALYSEN GESCHÜTZT IST**

Beschreibung

TECHNISCHER BEREICH

[0001] Die vorliegende betrifft ein digitales elektronisches Bauelement, das gegen elektrische und/oder elektromagnetische Analysen geschützt ist, insbesondere im Bereich der Chipkarte.

STAND DER TECHNIK

[0002] Der Bereich der Erfindung ist derjenige der Schaffung von Mechanismen zur Bekämpfung von Extraktionen von Daten (im Allgemeinen mit Verschlüsselungsschlüssel) durch eine Analyse des Stromverbrauchs oder durch eine Analyse der abgegebenen elektromagnetischen Strahlung in einem digitalen elektronischen Bauelement, beispielsweise einer Chipkarte. Diese Analysen werden allgemein SPA ("Simple Power Analysis")/DPA ("Differential Power Analysis") oder SEMA ("Simple Electrical Magnetic Analysis")/DEMA ("Differential Electrical Magnetic Analysis") genannt.

[0003] Mit Hilfe dieser Analysen ist es möglich, zu bestimmen, was die Zentraleinheit einer Chipkarte macht, welches die von ihr manipulierten Daten sind. Man kann auf diese Weise Zugriff auf den oder die geheimen Schlüssel haben, die für die Übertragung dieser Daten verwendet werden. Ein solches Eindringen geschieht ohne Risiko, da es nicht möglich ist, später nachzuweisen, dass es stattgefunden hat, da das Bauelement unversehrt geblieben ist.

[0004] Wie in dem Artikel von Paul Kocher, Joshua Jaffe und Benjamin Jun mit dem Titel "Introduction to differential power analysis and related attack" (Internetseite: www.cryptography.com, Cryptography Research, 1998), beschrieben wird, können diese Analysetechniken erhebliche Folgen haben, da sie die Extraktion von Geheimschlüsseln gestatten, die für verschlüsselte Mitteilungen verwendet werden. Ausserdem können solche Angriffe schnell ausgeführt werden und unter Verwendung von leicht verfügbarem Material vorgenommen werden. Der für ihre Durchführung erforderliche Zeitaufwand hängt von dem Typ des Angriffs ab (DPA, SPA) und schwankt in Abhängigkeit von dem betreffenden Bauelement. Ein SPA-Angriff kann einige Sekunden pro Bauelement benötigen, während ein DPA-Angriff mehrere Stunden dauern kann.

[0005] Gegenwärtig sind die digitalen Elektroniksysteme wenig oder nicht gegen solche elektrische oder elektromagnetische Analysen geschützt. Es gibt zwei Schutzfamilien: die eine ist rein informatisch (oder "Software"), die andere ist rein materiell (oder "Hardware"). Im Fall von Daten, die von der Zentraleinheit einer Chipkarte manipuliert werden:

– besteht in der ersten Familie eine technische Lösung darin, dass der Verbrauch des Stroms so zufällig wie möglich gemacht wird, wobei dieser Stromverbrauch so wenig wie möglich mit den von der Zentraleinheit manipulierten Daten verbunden ist. Man kann auf diese Weise den Ablauf der Befehle zufällig machen oder auch die manipulierten Daten so zufällig wie möglich machen.

– kann man in der zweiten Familie:

• entweder den Strom so gleichmäßig wie möglich machen, so dass es sehr schwierig ist, eine Entsprechung zwischen dem Stromverbrauch und den von der Zentraleinheit manipulierten Befehlen herzustellen,

• oder den Stromverbrauch zufällig zu machen, so dass zwei identische Arbeitsweisen der Zentraleinheit desynchronisiert werden.

[0006] Die Erfindung ist in diesem zweiten Fall angesiedelt.

[0007] Eine europäische Patentanmeldung 1 113 386 beschreibt eine Lösung zum Schützen einer Chipkarte gegen solche Angriffe. Bei dieser Lösung sind in die Chipkarte zwei Kondensatoren eingebaut, so dass zu jedem beliebigen Zeitpunkt einer von ihnen durch eine externe Energieversorgung geladen wird und der anderen entladen wird, indem er das Bauelement der Chipkarte betätigt. Die Rollen der beiden Kondensatoren wechseln sich schnell ab und die Energieversorgung ist von dem Bauelement der Chipkarte in dem Sinn isoliert, dass Analysen des Stromverbrauchs keine Informationen über den Betrieb dieses Bauelements liefern.

[0008] Ziel der Erfindung ist es, das oben dargelegte Problem zu lösen, indem man die Arbeitsgeschwindigkeit eines betrachteten digitalen elektronischen Bauelements, beispielsweise einer Chipkarte, sich zufällig ändern lässt, so dass SPA/DPA- und/oder SEMA/DEMA-Analysen schwierig oder sogar unmöglich werden.

BESCHREIBUNG DER ERFINDUNG

[0009] Gegenstand der Erfindung ist ein digitales elektronisches Bauelement, das gegen elektrische und elektromagnetische Analysen geschützt ist, umfassend ein durch einen Zeitgeber gesteuertes synchrones Element, dadurch gekennzeichnet, dass es einen Zufallsfrequenzsollwert-Generator umfasst, der einen Frequenzgenerator steuert, der diesen Zeitgeber liefert, dessen Frequenz sich zwischen einem Minimumwert und einem Maximumwert während mindestens eines gegebenen Zeitraums zufällig ändert, sowie Mittel zur Prüfung des zufälligen Charakters der Frequenzänderung dieses Zeitgebers.

[0010] Diese Mittel zur Erzeugung eines Zeitgebers können einen Zufallsfrequenzsollwert-Generator umfassen, der einen Frequenzgenerator steuert.

[0011] Der Frequenzgenerator kann mindestens zwei Frequenzsynthetisatoren oder PLL-Schaltungen ("Phase Locked Loop") und Mittel zum Umschalten zwischen diesen Synthetisatoren oder Schaltungen umfassen.

[0012] Das synchrone Element kann die Zentraleinheit einer Chipkarte, ein Speicher oder eine synchrone verdrahtete Funktion sein, beispielsweise vom Typ FPGA ("Field Programmable Gate Arrays") oder ASIC ("Application Specific Integrated Circuit").

[0013] Der Frequenzänderungsbereich muss so breit wie möglich sein, um DPA/SPA- und DEMA/SEMA-Analysen maximal zu stören. Der betreffende Zufall ist hier ein echter Zufall, da es sich hierbei nicht um eine Phasen- oder Frequenzverschiebung des Zeitgebers handelt, sondern um eine gesteuerte zufällige Frequenzänderung. Indem auf diese Weise der Zeitgeber gestört wird, wird der Stromverbrauch des synchronen Elements zufällig gemacht.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0014] Die einzige Figur zeigt ein erfindungsgemäßes digitales elektronisches Bauelement, das gegen elektrische und/oder elektromagnetische Angriffe geschützt ist.

AUSFÜHRLICHE BESCHREIBUNG VON BESONDEREN AUSFÜHRUNGSBEISPIELEN

[0015] Wie in der Figur dargestellt, umfasst das gegen elektrische und/oder elektromagnetische Angriffe geschützte digitale elektronische Bauelement gemäß der Erfindung:

– eine Zentraleinheit **10** dieser Chipkarte,
– einen Zufallsfrequenzsollwert-Generator **11**,
– einen durch diesen Generator **10** gesteuerten Frequenzgenerator **12**, dessen Frequenz sich zufällig zwischen einem Minimumwert und einem Maximum ändert,
– ein Prüforgan **13**, das die Aufgabe hat, die Frequenz des Zeitgebers H zu messen und die tatsächlich zufällige Arbeitsweise der Frequenzänderung zu verifizieren.

[0016] Der Frequenzhub des Zeitgebers H, der so groß wie möglich ist, beträgt zwischen 1 MHz und 100 MHz.

[0017] Bei dem in der Figur dargestellten Ausführungsbeispiel umfasst der Frequenzgenerator **12** mindestens zwei Frequenzsynthetisatoren SF1...SFn, die durch von den Ausgängen **15** des Prüforgans **13** kommende Signale gesteuert werden, und eine Multiplexier- und Synchronisierschaltung **20**, die die Ausgänge F1...Fn dieser Synthetisatoren SF1...SFn empfängt.

[0018] Bei einer Frequenzänderung, bevor eine der Frequenzen am Ausgang der Synthetisatoren SF1...SFn ausgewählt wird, indem ein Signal SEL zu der Multiplexier- und Synchronisierschaltung gesendet wird, überprüft das Prüforgan **13**, dass es keine möglichen Störungen gibt, indem es die an seinen Eingängen erhaltenen Signale analysiert.

[0019] Das Prüforgan **13** kann auf diese Weise folgendermaßen arbeiten:

– Anforderung eines neuen Werts von dem Zufallsfrequenzsollwert-Generator **11**,
– Wert von diesem Generator **11** dem Prüforgan **13** geliefert,
– Überprüfung des zufälligen Charakters dieses Werts bezüglich der vorhergehenden Werte durch das Prüforgan **13**,
– Übertragung dieses Werts zu den Synthetisatoren SF1...SFn.

[0020] Die Erfindung gestattet es, die Arbeitsweise der Zentraleinheit, die die Rechnungen ausführt, zufällig zu machen und das Aussehen eines zufälligen Stromverbrauchs zu ergeben. SPA/DPA- und/oder SEMA/DEMA-Analysen sind schwierig oder unmöglich durchzuführen, da sie eine starke Erhöhung der Anzahl von Stromanalysen erfordern.

[0021] Die Erfindung gestattet es, die Zentraleinheit an sich nicht zu verändern, was gestattet, sie in ihrem eigenen Frequenzbereich arbeiten zu lassen.

[0022] Die Schutzqualität der Erfindung ist von dem Zufallsfrequenzsollwert-Generator und von dem Zyklus der Frequenzänderung in Abhängigkeit von der Dauer eines Befehlszyklus der Zentraleinheit abhängig.

[0023] Bei einer vorteilhaften Ausführungsform kann das Prüforgan durch die Zentraleinheit gesteuert werden.

[0024] Bei einer abgewandelten Arbeitsweise kann man die zufällige Änderung der Frequenz des erfindungsgemäßen Zeitgebers H nur während eines gegebenen Zeitraums in als kritisch betrachteten Fällen aktivieren.

Patentansprüche

1. Digitales elektronisches Bauelement, das gegen elektrische und elektromagnetische Analysen geschützt ist, umfassend ein durch einen Zeitgeber (H) gesteuertes synchrones Element (**10**), **dadurch gekennzeichnet**, dass es einen Zufallsfrequenzsollwert-Generator (**11**) umfasst, der einen Frequenzgenerator (**12**) steuert, der diesen Zeitgeber (H) liefert, dessen Frequenz sich zwischen einem Minimumwert und einem Maximumwert während mindestens eines gegebenen Zeitraums zufällig ändert, sowie Mittel

(**13**) zur Prüfung des zufälligen Charakters der Frequenzänderung dieses Zeitgebers (H).

2. Bauelement nach Anspruch 1, bei dem der Frequenzgenerator mindestens zwei Frequenzsynthetisatoren (SF1, ...SFn) und Schaltmittel (**20**) umfasst.

3. Bauelement nach Anspruch 1, bei dem der Frequenzgenerator mindestens zwei PLL-Schaltungen und Schaltmittel umfasst.

4. Bauelement nach Anspruch 1, bei dem das synchrone Element die Zentraleinheit (**10**) einer Chipkarte ist.

5. Bauelement nach Ansnpruch 4, bei dem das Prüforgan (**13**) durch die Zentraleinheit gesteuert wird.

6. Bauelement nach Anspruch 1, bei dem das synchrone Element (**10**) ein Speicher ist.

7. Bauelement nach Anspruch 1, bei dem das synchrone Element (**10**) eine verdrahtete synchrone Funktion ist.

8. Bauelement nach Anspruch 1, bei dem der Frequenzhub des Zeitgebers (H) zwischen 1 MHz und 100 MHz beträgt.

Es folgt ein Blatt Zeichnungen

Anhängende Zeichnungen