(19) Deutsches Patent- und Markenamt

(10) **DE 11 2008 003 855 T5** 2011.04.07

(12) # Veröffentlichung

der internationalen Anmeldung mit der
(87) Veröffentlichungs-Nr.: **WO 2009/136944**
in deutscher Übersetzung (Art. III § 8 Abs. 2 IntPatÜG)
(21) Deutsches Aktenzeichen: **11 2008 003 855.4**
(86) PCT-Aktenzeichen: **PCT/US2008/063280**
(86) PCT-Anmeldetag: **09.05.2008**
(87) PCT-Veröffentlichungstag: **12.11.2009**
(43) Veröffentlichungstag der PCT Anmeldung
in deutscher Übersetzung: **07.04.2011**

(51) Int Cl.[8]: ***H04L 9/20*** (2006.01)
G06F 12/14 (2006.01)
G06F 21/00 (2006.01)

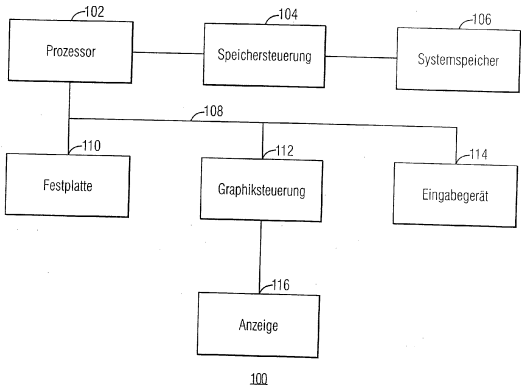
(71) Anmelder:
Hewlett-Packard Development Co., L.P. a Texas Limited Partnership, Houston, Texas, US

(74) Vertreter:
Schoppe, Zimmermann, Stöckeler, Zinkler & Partner, 82049 Pullach

(72) Erfinder:
Novoa, Manuel, Houston, Tex., US; Fry, Walter G., Houston, Tex., US; Ali, Valiuddin Y., Houston, Tex., US

(54) Bezeichnung: **System und Verfahren zum Bereitstellen von sicherem Zugriff auf einen Systemspeicher**

(57) Hauptanspruch: Ein Verfahren zum Bereitstellen von sicherem Zugriff auf Daten, die in einem Systemspeicher eines Computersystems gespeichert sind, wobei das Computersystem eine Speichersteuerung umfasst zum Schreiben von Daten in den und Lesen von Daten von dem Systemspeicher, wobei das Verfahren folgende Schritte umfasst:
Erzeugen eines Zufallsverschlüsselungsschlüssels jedes Mal, wenn das Computersystem hochgefahren wird;
Speichern des Zufallsverschlüsselungsschlüssels in einer flüchtigen Speicherregion der Speichersteuerung;
Verschlüsseln von Daten unter Verwendung des Zufallsverschlüsselungsschlüssels, um verschlüsselte Daten zu erzeugen; und
Speichern der verschlüsselten Daten in dem Systemspeicher.



Beschreibung

Hintergrund

[0001] In einem typischen Computersystem wird ein Systemspeicher als ein vorübergehender Speicher unter anderem für Sicherheitsschlüssel und Berechtigungsnachweise verwendet. In letzter Zeit haben Hacker begonnen, zu versuchen, unerlaubten Zugriff auf sichere Daten zu erlangen durch physikalisches Entfernen von Speichermodulen von einem Computer eines Nutzers, wobei die Speichermodule möglicherweise eingefroren werden, um den Zerfall der Daten, die darin enthalten sind, zu verzögern. Der Hacker installiert dann die gestohlenen Speichermodule in einen anderen Computer, um ihre Inhalte zu lesen. Auf solch eine Weise können Hacker in der Lage sein, die Sicherheitsschlüssel und Berechtigungsnachweise wiederzugewinnen, die in den Speichermodulen gespeichert sind, und die gestohlenen Informationen zu verwenden, um unbefugten Zugriff auf empfindliche Daten des Nutzers zu erhalten.

Kurze Beschreibung der Zeichnungen

[0002] Bestimmte beispielhafte Ausführungsbeispiele werden nachfolgend in der detaillierten Beschreibung und in Bezugnahme auf die Zeichnungen beschrieben.

[0003] Fig. 1 ist ein Blockdiagramm eines Computersystems gemäß einem beispielhaften Ausführungsbeispiel der vorliegenden Erfindung;

[0004] Fig. 2 ist ein Blockdiagramm eines Speicherteilsystems des in Fig. 1 gezeigten Computersystems gemäß einem beispielhaften Ausführungsbeispiel der vorliegenden Erfindung; und

[0005] Fig. 3 ist ein Flussdiagramm, das ein Verfahren zum Betreiben eines geschützten Systemspeichers gemäß einem beispielhaften Ausführungsbeispiel der vorliegenden Erfindung zeigt.

Detaillierte Beschreibung spezifischer Ausführungsbeispiele

[0006] Fig. 1 ist ein Blockdiagramm eines Computersystems gemäß einem beispielhaften Ausführungsbeispiel der vorliegenden Erfindung. Das Computersystem wird allgemein mit dem Bezugszeichen **100** bezeichnet. Durchschnittsfachleute auf diesem Gebiet werden erkennen, dass das Computersystem **100** Hardwareelemente, die Schaltungsanordnung umfassen, Softwareelemente, die Computercode umfassen, der auf einem maschinenlesbaren Medium gespeichert ist, oder eine Kombination von sowohl Hardware- als auch Softwareelementen enthalten kann. Außerdem sind die in Fig. 1 gezeigten Funktionsblöcke lediglich ein Beispiel von Funktionsblöcken, die in einem beispielhaften Ausführungsbeispiel der vorliegenden Erfindung implementiert sein können. Durchschnittsfachleute auf diesem Gebiet wären ohne weiteres in der Lage, spezifische Funktionsblöcke zu definieren basierend auf Entwurfsüberlegungen für ein bestimmtes Computersystem.

[0007] Ein Prozessor **102**, wie z. B. eine zentrale Verarbeitungseinheit oder CPU, ist angepasst, um den Gesamtbetrieb des Computersystems **100** zu steuern. Der Prozessor **102** ist mit einer Speichersteuerung **104** verbunden, die angepasst ist, um Daten von einem Systemspeicher **106** zu lesen und in denselben zu schreiben. Die Speichersteuerung **104** kann Speicher umfassen, der eine nichtflüchtige Speicherregion und eine flüchtige Speicherregion enthält. Wie es nachfolgend näher beschrieben wird, ist ein beispielhaftes Ausführungsbeispiel der vorliegenden Erfindung angepasst, um Datendiebstahl zu verhindern durch Bereitstellen sicherer Kommunikation zwischen der Speichersteuerung **104** und dem Systemspeicher **106**.

[0008] Der Systemspeicher **106** kann aus einer Mehrzahl von Speichermodulen bestehen, wie es für einen Durchschnittsfachmann auf diesem Gebiet offensichtlich ist. Außerdem kann der Systemspeicher **106** nichtflüchtige und flüchtige Abschnitte umfassen. Ein System-Basis-Eingabe-/Ausgabesystem (BIOS; BIOS = basic input-output system) kann in einem nichtflüchtigen Abschnitt des Systemspeicher **106** gespeichert sein. Das System-BIOS ist angepasst, um einen Einschalt- oder Hochfahrprozess zu steuern und den Betrieb des Computersystems **100** auf niedriger Ebene zu steuern.

[0009] Der Prozessor **102** ist mit zumindest einem Systembus **108** verbunden, um Kommunikation zwischen dem Prozessor **102** und anderen Systemvorrichtungen zu ermöglichen. Der Systembus kann unter einem Standardprotokoll arbeiten, wie z. B. einer Variation des PCI-Busses (PCI = peripheral component interconnect = Peripheriekomponentenverbindung) oder dergleichen. Bei dem in Fig. 1 gezeigten beispielhaften Ausführungsbeispiel verbindet der Systembus **108** den Prozessor **102** mit einem Festplattenlaufwerk **110**, einer Graphiksteuerung **112** und zumindest einem Eingabegerät **114**. Das Festplattenlaufwerk **110** stellt nichtflüchtige Speicherung für Daten bereit, die durch das Computersystem verwendet werden. Die Graphiksteuerung **112** wiederum ist mit einem Anzeigegerät **116** verbunden, das einem Nutzer ein Bild bereitstellt basierend auf Aktivitäten, die durch das Computersystem **100** durchgeführt werden.

[0010] Fig. 2 ist ein Blockdiagramm eines Speicherteilsystems des in Fig. 1 gezeigten Computersystems gemäß einem beispielhaften Ausführungsbeispiel der vorliegenden Erfindung. Das Speicherteilsystem wird

allgemein mit dem Bezugszeichen **200** bezeichnet. Das Speicherteilsystem **200** umfasst die Speichersteuerung **104** und den Systemspeicher **106**.

[0011] Wenn das Computersystem **100** hochgefahren wird oder anderweitig eine Systemrücksetzung empfängt, empfängt die Speichersteuerung **106** einen Zufallsverschlüsselungsschlüssel, der in einer flüchtigen Speicherregion **202** gespeichert ist. Bei einem beispielhaften Ausführungsbeispiel der vorliegenden Erfindung umfasst die flüchtige Speicherregion **202** ein Nur-Schreib-/einmal beschreibbares Register, das über eine Systemrücksetzung zurückgesetzt wird. Der Zufallsverschlüsselungsschlüssel kann durch ein System-BIOS erzeugt werden, das verschiedene Initialisierungsfunktionen durchführt, wenn das Computersystem hochgefahren wird. Wie es nachfolgend näher erläutert wird, wird der Zufallsverschlüsselungsschlüssel verwendet, um Daten zu verschlüsseln, die in den Systemspeicher **106** geschrieben werden.

[0012] Bei einem beispielhaften Ausführungsbeispiel der vorliegenden Erfindung werden nachfolgende Zufallsverschlüsselungsschlüssel selektiv durch die Speichersteuerung **104** verwendet, um Daten zu verschlüsseln. Die nachfolgenden Zufallsverschlüsselungsschlüssel können beispielsweise durch die Speichersteuerung **104** erzeugt werden. Alternativ können die nachfolgenden Zufallsverschlüsselungsschlüssel durch eine andere Komponente des Computersystems **100** bereitgestellt werden, wie z. B. das System-BIOS. Falls nachfolgende Zufallsverschlüsselungsschlüssel verwendet werden, würden unterschiedliche Bereiche des Systemspeichers **106** mit unterschiedlichen Zufallsverschlüsselungsschlüsseln verschlüsselt. Die Verwendung von mehreren Zufallsverschlüsselungsschlüsseln macht es für einen Hacker schwierig, einen Zahlengenerator zu verwenden, um alle Zufallsverschlüsselungsschlüssel zu identifizieren, die verwendet werden, um die Inhalte des Systemspeichers **106** zu verschlüsseln.

[0013] Ein Verschlüsselungsblock **204** der Speichersteuerung **104** verwendet den aktuellen Zufallsverschlüsselungsschlüssel, um alle Daten zu verschlüsseln, die in den Systemspeicher **106** geschrieben werden. Bei einem beispielhaften Ausführungsbeispiel der vorliegenden Erfindung kann ein einfacher Verschlüsselungsalgorithmus, wie z. B. ein XOR-Algorithmus, durch den Verschlüsselungsblock **204** verwendet werden, um die Auswirkung auf den Durchsatz des Speicherteilsystems **200** zu minimieren. Ein beispielhafter XOR-Algorithmus umfasst das Durchführen einer XOR-Operation unter Verwendung der Daten, die in den Systemspeicher geschrieben sind, und des Zufallsverschlüsselungsschlüssels. Das folgende Beispiel stellt dar, wie ein beispielhaftes Ausführungsbeispiel der vorliegenden Erfindung verbesserte Sicherheit für Daten bereitstellt, die im Systemspeicher gespeichert sind. Angenommen Datenelemente A und B sind in den Systemspeicher zu schreiben, nachdem dieselben unter Verwendung eines Zufallsverschlüsselungsschlüssels R XOR-verschlüsselt wurden. Dieser Prozess kann unter Verwendung der folgenden Gleichungen beschrieben werden:

$$A \oplus R = C$$

$$B \oplus R = D$$

wobei C die verschlüsselte Version von A ist und D die verschlüsselte Version von B ist. Die verschlüsselten Daten C und D sind in dem Systemspeicher gespeichert und nicht A oder B selbst. Mit einer mathematischen Manipulation wird das folgende Ergebnis erhalten:

$$C \oplus D = A \oplus B$$

[0014] Somit kann ein fähiger Hacker in der Lage sein, Daten von einem gestohlenen Speichermodul zu manipulieren, um ein Konglomerat von A und B wiederherzustellen. Trotzdem wäre es äußerst schwierig, A und B selbst zu erhalten, ohne Zugriff auf den Zufallsverschlüsselungsschlüssel R. Die Verwendung eines beispielhaften Ausführungsbeispiels der vorliegenden Erfindung erhöht wesentlich die Schwierigkeit, eine unbefugte Wiederherstellung von Daten von dem Systemspeicher durchzuführen.

[0015] Durchschnittsfachleute auf diesem Gebiet werden erkennen, dass andere Verschlüsselungsalgorithmen als eine XOR-Verknüpfung eines Zufallsverschlüsselungsschlüssels mit Daten, die in den Systemspeicher zu schreiben sind, verwendet werden können, um Daten zu verschlüsseln, die in den Systemspeicher **106** geschrieben werden. Darüber hinaus ist der spezifische Verschlüsselungsalgorithmus, der durch den Verschlüsselungsblock **204** verwendet wird, kein wesentliches Merkmal der vorliegenden Erfindung.

[0016] Wenn verschlüsselte Daten von dem Systemspeicher **106** gelesen werden, werden dieselben durch einen Entschlüsselungsblock **208** in der Speichersteuerung **104** entschlüsselt. Der Entschlüsselungsblock **208** führt die Entschlüsselung durch unter Verwendung des Zufallsverschlüsselungsschlüssels, der verwendet wurde, um die Verschlüsselung der Daten durch den Verschlüsselungsblock **204** durchzuführen. Die entschlüsselten Daten können dann an den Prozessor **102** geliefert werden. Ein beispielhaftes Ausführungsbeispiel der vorliegenden Erfindung liefert verbesserte Datensicherheit indem nur verschlüsselte Daten in den Systemspeicher **106** geschrieben werden.

[0017] Durch Speichern des Zufallsverschlüsselungsschlüssels in einer flüchtigen Speicherregion in der Speichersteuerung **104** reduziert ein beispielhaftes Ausführungsbeispiel der vorliegenden Erfindung das Risiko, dass ein Hacker oder anderer potentieller Datendieb in der Lage wäre, den Verschlüsselungsschlüssel wiederzugewinnen und Zugriff zu gewinnen auf Daten, die mit dem bestimmten Zufallsverschlüsselungsschlüssel verschlüsselt wurden und nachfolgend in dem Systemspeicher **106** gespeichert wurden. Die Speichersteuerung **104** könnte nicht umgekehrt konstruiert werden oder „zerlegt" werden, um den Schlüssel zu bestimmen, weil der Wert des Schlüssels auf die Entfernung der Leistung zu der Speichersteuerung hin nicht in der nichtflüchtigen Speicherregion **202** vorliegen würde. Dies würde Zugriff auf Daten verhindern, die unter Verwendung des speziellen Zufallsverschlüsselungsschlüssels verschlüsselt wurden, selbst wenn die Daten, die in dem Systemspeicher gespeichert sind, irgendwie beibehalten würden, beispielsweise durch Einfrieren von Speichermodulen, die der Systemspeicher oder dergleichen umfassen.

[0018] Fig. 3 ist ein Flussdiagramm, das ein Verfahren zeigt zum Betreiben eines geschützten Systemspeichers, wie des Systemspeichers **106** (Fig. 1) gemäß einem beispielhaften Ausführungsbeispiel der vorliegenden Erfindung. Das Verfahren wird allgemein durch das Bezugszeichen **300** bezeichnet. Bei Block **302** beginnt der Prozess.

[0019] Bei Block **304** wird jedes Mal ein Zufallsverschlüsselungsschlüssel erzeugt, wenn ein Computersystem, wie z. B. das Computersystem **100** (Fig. 1), hochgefahren wird. Wie es bei Block **306** gezeigt ist, ist der Zufallsverschlüsselungsschlüssel in einer flüchtigen Speicherregion einer Speichersteuerung gespeichert, wie z. B. der Speichersteuerung **104** (Fig. 1).

[0020] Daten werden unter Verwendung des Zufallsverschlüsselungsschlüssels verschlüsselt, wie es bei Block **308** gezeigt ist. Die verschlüsselten Daten werden in dem Systemspeicher gespeichert, wie es bei Block **310** gezeigt ist. Bei Block **312** endet der Prozess.

[0021] Ein beispielhaftes Ausführungsbeispiel der vorliegenden Erfindung schafft ein sicheres Kommunikationsverfahren zwischen einer Speichersteuerung und einem Systemspeicher, der beispielsweise aus einer Mehrzahl von Speichermodulen besteht. Ein solches beispielhaftes Ausführungsbeispiel schützt Systemspeicher vor einem großen Bereich von Hackerangriffen. Insbesondere ist ein beispielhaftes Ausführungsbeispiel der vorliegenden Erfindung angepasst, um Systemspeicher vor physikalischen Angriffen und Hochfahrangriffen zu schützen. Darüber hinaus können Standardspeicherkomponenten und -module verwendet werden. Kein zusätzlicher Aufwand ist erforderlich, wenn eine neue Generation von Speichertechnologie eingeführt wird. Ein beispielhaftes Ausführungsbeispiel der vorliegenden Erfindung schafft Systemspeichersicherheit, ohne die Systemleistungsfähigkeit wesentlich zu beeinträchtigen und ohne die Leistungsfähigkeit des Betriebssystems und der Softwareanwendung zu beeinträchtigen. Schließlich kann ein beispielhaftes Ausführungsbeispiel der vorliegenden Erfindung mit minimalem Einfluss auf die Gesamtsystemkosten und -komplexität implementiert werden.

Zusammenfassung

[0022] Ein Verfahren zum Bereitstellen von sicherem Zugriff auf Daten, die in einem Systemspeicher eines Computersystems gespeichert sind, ist vorgesehen, wobei das Computersystem eine Speichersteuerung umfasst zum Schreiben von Daten in und Lesen von Daten von dem Systemspeicher. Das Verfahren umfasst das Erzeugen eines Zufallsverschlüsselungsschlüssels jedes Mal, wenn das Computersystem hochgefahren wird, und das Speichern des Zufallsverschlüsselungsschlüssels in einer flüchtigen Speicherregion der Speichersteuerung. Das Verfahren umfasst zusätzlich das Verschlüsseln von Daten unter Verwendung des Zufallsverschlüsselungsschlüssels, um verschlüsselte Daten zu erzeugen, und das Speichern der verschlüsselten Daten in dem Systemspeicher. Außerdem ist ein Speicherteilsystem und ein Computersystem zum Durchführen des Verfahrens vorgesehen.

Patentansprüche

1. Ein Verfahren zum Bereitstellen von sicherem Zugriff auf Daten, die in einem Systemspeicher eines Computersystems gespeichert sind, wobei das Computersystem eine Speichersteuerung umfasst zum Schreiben von Daten in den und Lesen von Daten von dem Systemspeicher, wobei das Verfahren folgende Schritte umfasst:
Erzeugen eines Zufallsverschlüsselungsschlüssels jedes Mal, wenn das Computersystem hochgefahren wird;
Speichern des Zufallsverschlüsselungsschlüssels in einer flüchtigen Speicherregion der Speichersteuerung;
Verschlüsseln von Daten unter Verwendung des Zufallsverschlüsselungsschlüssels, um verschlüsselte Daten zu erzeugen; und
Speichern der verschlüsselten Daten in dem Systemspeicher.

2. Das Verfahren gemäß Anspruch 1, das folgende Schritte umfasst:
Lesen der verschlüsselten Daten von dem Systemspeicher; und

Entschlüsseln der verschlüsselten Daten unter Verwendung des Zufallsverschlüsselungsschlüssels.

3. Das Verfahren gemäß Anspruch 1, bei dem die flüchtige Speicherregion der Speichersteuerung ein Nur-Schreib-/einmal beschreibbares Register umfasst.

4. Das Verfahren gemäß Anspruch 1, das das Zurücksetzen der flüchtigen Speicherregion der Speichersteuerung umfasst, wenn eine Systemrücksetzung durchgeführt wird.

5. Das Verfahren gemäß Anspruch 1, bei dem das Verschlüsseln der Daten das Durchführen einer XOR-Operation unter Verwendung der Daten und des Zufallsverschlüsselungsschlüssels umfasst.

6. Das Verfahren gemäß Anspruch 1, bei dem der Zufallsverschlüsselungsschlüssel erzeugt wird durch ein System-Basis-Eingabe-/Ausgabesystem (BIOS), jedes Mal, wenn das Computersystem hochgefahren wird.

7. Das Verfahren gemäß Anspruch 1, das folgende Schritte umfasst:
Erzeugen zumindest eines nachfolgenden Zufallsverschlüsselungsschlüssels; und
Verschlüsseln von Daten unter Verwendung des zumindest einen nachfolgenden Zufallsverschlüsselungsschlüssels.

8. Ein Speicherteilsystem eines Computersystems, wobei das Speicherteilsystem folgendes Merkmal umfasst:
eine Speichersteuerung, die angepasst ist, um jedes Mal, wenn das Computersystem hochgefahren wird, einen Zufallsverschlüsselungsschlüssel zu empfangen, um den Zufallsverschlüsselungsschlüssel in einer flüchtigen Speicherregion in der Speichersteuerung zu speichern, um den Zufallsverschlüsselungsschlüssel zu verwenden, um Daten zu verschlüsseln, und um verschlüsselte Daten in einem Systemspeicher zu speichern.

9. Das Speicherteilsystem gemäß Anspruch 8, bei dem die Speichersteuerung angepasst ist, um die verschlüsselten Daten von dem Systemspeicher zu lesen, und um die verschlüsselten Daten unter Verwendung des Zufallsverschlüsselungsschlüssels zu entschlüsseln.

10. Das Speicherteilsystem gemäß Anspruch 8, bei dem die flüchtige Speicherregion der Speichersteuerung ein Nur-Schreib-/einmal beschreibbares Register umfasst.

11. Das Speicherteilsystem gemäß Anspruch 8, bei dem die flüchtige Speicherregion der Speichersteuerung zurückgesetzt wird, wenn eine Systemrücksetzung durchgeführt wird.

12. Das Speicherteilsystem gemäß Anspruch 8, bei dem Speichersteuerung angepasst ist, um die Daten zu verschlüsseln durch Durchführen einer XOR-Operation unter Verwendung der Daten und des Zufallsverschlüsselungsschlüssels.

13. Das Speicherteilsystem gemäß Anspruch 8, das ein System-Basis-Eingabe-/Ausgabesystem (BIOS) umfasst, das angepasst ist, um den Zufallsverschlüsselungsschlüssel jedes Mal zu erzeugen, wenn das Computersystem hochgefahren wird.

14. Das Speicherteilsystem gemäß Anspruch 8, bei dem die Speichersteuerung angepasst ist, um zumindest einen nachfolgenden Zufallsverschlüsselungsschlüssel zu verwenden, um Daten zu verschlüsseln.

15. Ein Computersystem, das folgende Merkmale umfasst:
eine Festplatte, die angepasst ist, um Daten zu speichern für die Verwendung durch das Computersystem;
einen Prozessor, der angepasst ist, um Daten zu lesen, die auf der Festplatte gespeichert sind;
eine Speichersteuerung, die angepasst ist, um jedes Mal, wenn das Computersystem hochgefahren wird, einen Zufallsverschlüsselungsschlüssel zu empfangen, um den Zufallsverschlüsselungsschlüssel in einer flüchtigen Speicherregion in der Speichersteuerung zu speichern, um Daten von dem Prozessor zu empfangen, um den Zufallsverschlüsselungsschlüssel zu verwenden, um die Daten zu verschlüsseln, und um verschlüsselte Daten in einem Systemspeicher zu speichern; und
einen Systemspeicher, der angepasst ist, um verschlüsselte Daten zu speichern, die von der Speichersteuerung empfangen werden.

16. Das Computersystem gemäß Anspruch 15, bei dem Speichersteuerung angepasst ist, um die verschlüsselten Daten von dem Systemspeicher zu lesen, und um die verschlüsselten Daten unter Verwendung des Zufallsverschlüsselungsschlüssels zu entschlüsseln.

17. Das Computersystem gemäß Anspruch 15, bei dem die flüchtige Speicherregion der Speichersteuerung ein Nur-Schreib-/einmal beschreibbares Register umfasst.

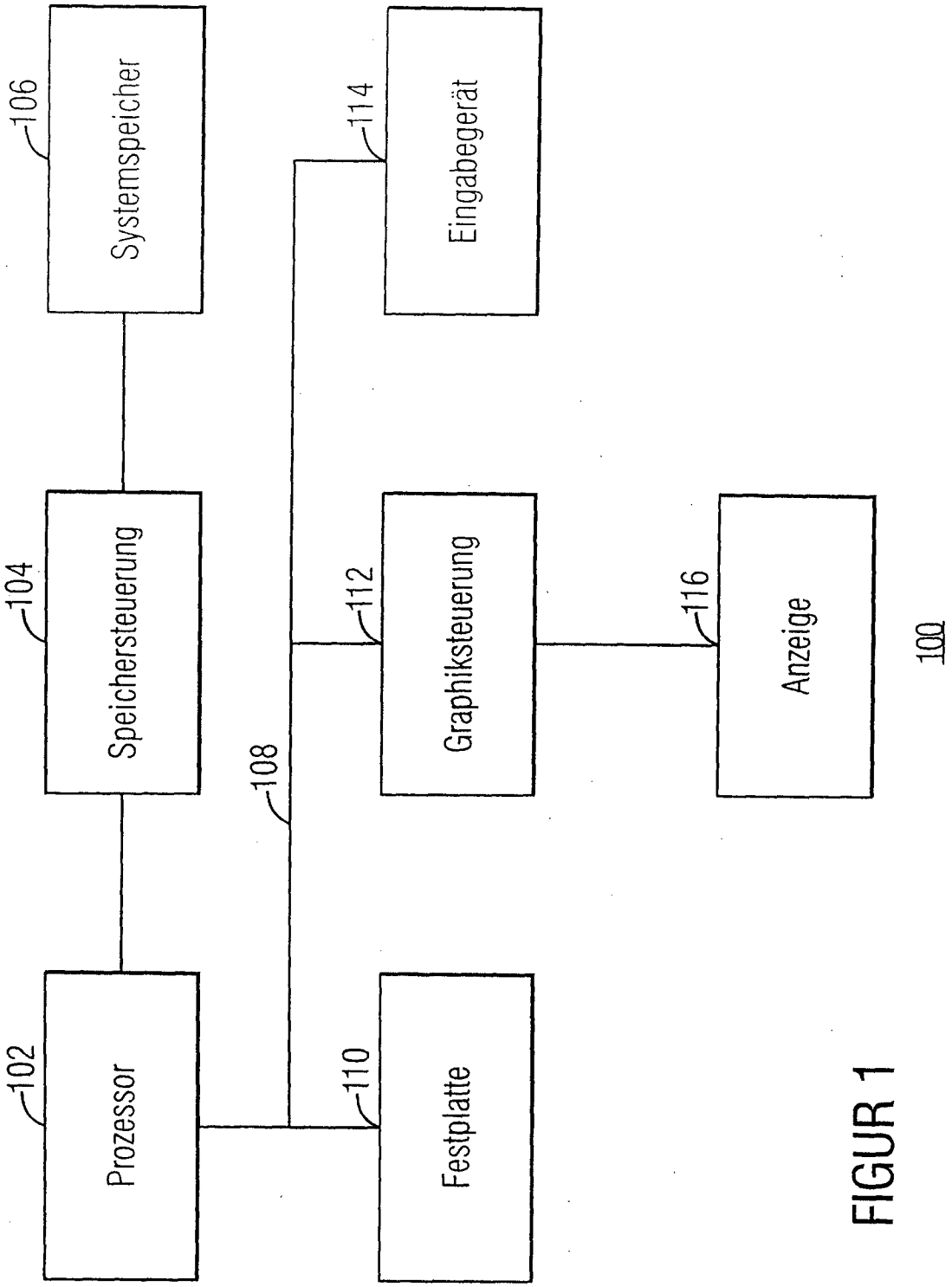
18. Das Computersystem gemäß Anspruch 15, bei dem die flüchtige Speicherregion der Speichersteuerung zurückgesetzt wird, wenn eine Systemrücksetzung durchgeführt wird.

19. Das Computersystem gemäß Anspruch 15, bei dem die Speichersteuerung angepasst ist, um die Daten zu verschlüsseln durch Durchführen einer XOR-Operation unter Verwendung der Daten und des Zufallsverschlüsselungsschlüssels.

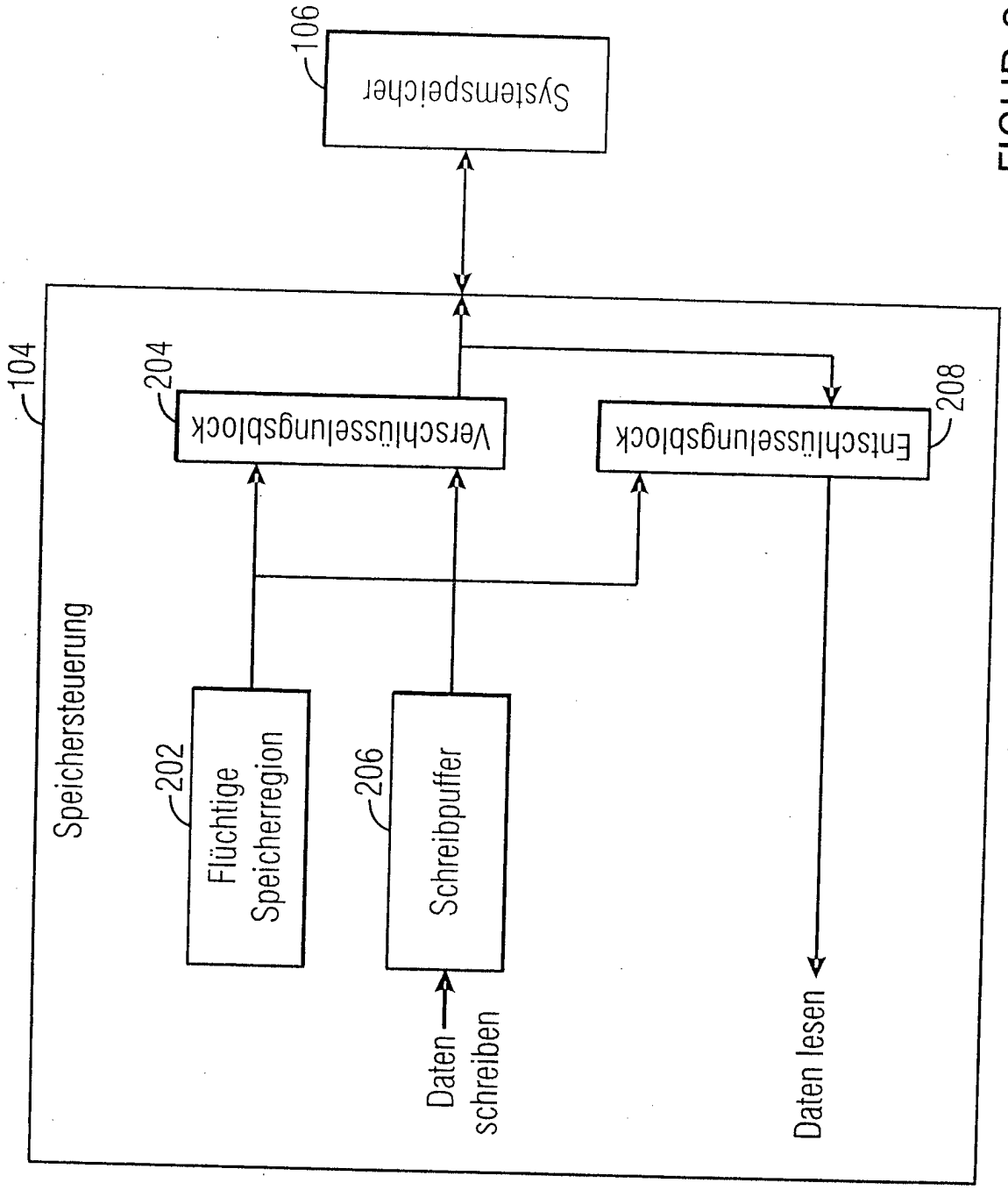
20. Das Computersystem gemäß Anspruch 15, das ein System-Basis-Eingabe-/Ausgabesystem (BIOS) umfasst, das angepasst ist, um den Zufallsverschlüsselungsschlüssel jedes Mal zu erzeugen, wenn das Computersystem hochgefahren wird.

Es folgen 3 Blatt Zeichnungen

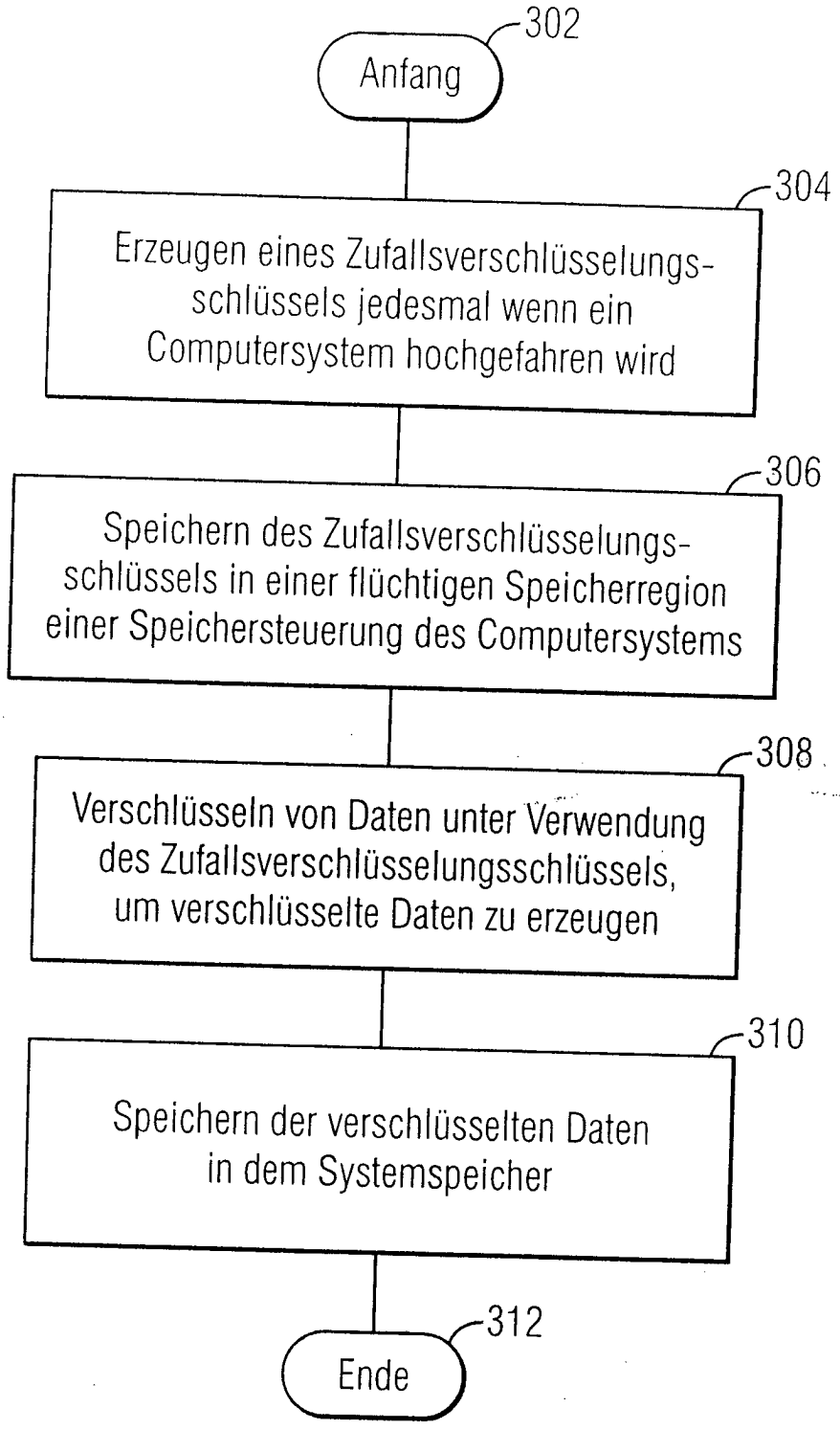
Anhängende Zeichnungen



FIGUR 1


106
Systemspeicher
104
204
Verschlüsselungsblock
208
Entschlüsselungsblock
Speichersteuerung
202
Flüchtige Speicherregion
206
Schreibpuffer
Daten schreiben
Daten lesen
200

FIGUR 2


302
Anfang
304
Erzeugen eines Zufallsverschlüsselungs-schlüssels jedesmal wenn ein Computersystem hochgefahren wird
306
Speichern des Zufallsverschlüsselungs-schlüssels in einer flüchtigen Speicherregion einer Speichersteuerung des Computersystems
308
Verschlüsseln von Daten unter Verwendung des Zufallsverschlüsselungsschlüssels, um verschlüsselte Daten zu erzeugen
310
Speichern der verschlüsselten Daten in dem Systemspeicher
312
Ende
300

FIGUR 3