

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges
Eigentum

Internationales Büro

(43) Internationales
Veröffentlichungsdatum
9. September 2016 (09.09.2016)



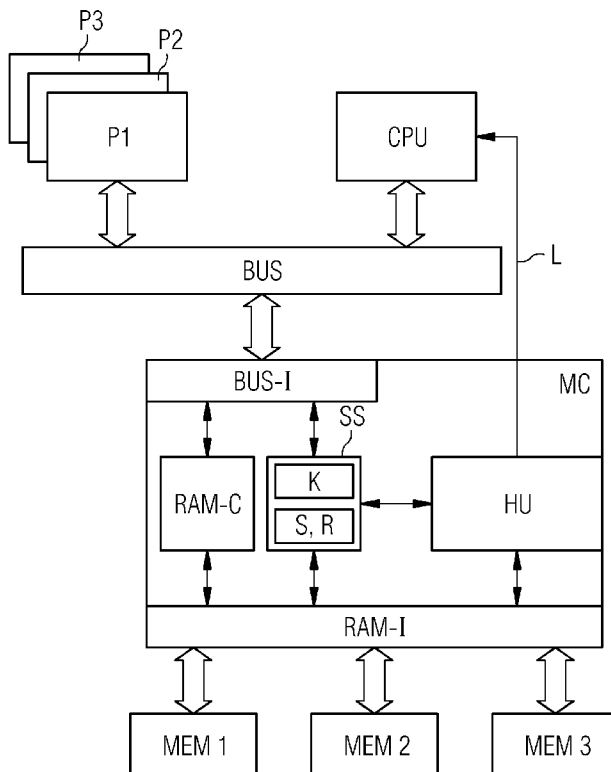
(10) Internationale Veröffentlichungsnummer
WO 2016/139079 A1

- (51) Internationale Patentklassifikation:
G06F 21/64 (2013.01) *G06F 21/78* (2013.01)
G06F 21/70 (2013.01)
- (21) Internationales Aktenzeichen: PCT/EP2016/053677
- (22) Internationales Anmeldedatum:
22. Februar 2016 (22.02.2016)
- (25) Einreichungssprache: Deutsch
- (26) Veröffentlichungssprache: Deutsch
- (30) Angaben zur Priorität:
15464004.9 2. März 2015 (02.03.2015) EP
- (71) Anmelder: **SIEMENS AG ÖSTERREICH** [AT/AT];
Siemensstraße 90, 1210 Wien (AT).
- (72) Erfinder: **FISCHER, Bernhard**; Dörfelstraße 3A/19,
1120 Wien (AT). **GHAMESHLU, Majid**; Kopalgasse
40/10, 1110 Wien (AT). **MATSCHNIG, Martin**;
Kirschenallee 15, 3430 Tulln (AT). **PITU, Ciprian-
Leonard**; Lamaitei 125, 500371 Brasov (RO).
- (74) Anwalt: **MAIER, Daniel**; Postfach 22 16 34, 80506
München (DE).
- (81) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare nationale Schutzrechtsart): AE, AG, AL,
AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW,
BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK,
DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM,
GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP,
KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,
SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM,
ZW.

[Fortsetzung auf der nächsten Seite]

(54) Title: PROTECTION OF MEMORY CONTENTS OF A MEMORY OF A COMPUTER SYSTEM BY USING A HASH FUNCTION

(54) Bezeichnung : SCHUTZ VON SPEICHERINHALTEN EINES SPEICHERS EINES COMPUTERSYSTEMS UNTER VERWENDUNG EINER HASHFUNKTION



(57) Abstract: The invention relates to a method for protecting memory contents of a memory (MEM1, MEM2, MEM3) of a computer system by using a hash function. In order to claim less processor computing time and to generate less additional data transfer, a memory controller (MC) is provided, which comprises a hash unit (HU), which is arranged inside the memory controller and which independently and autonomously computes a cryptographic checksum (S) over each of certain memory ranges and compares the checksums with reference values, wherein an error notification is generated if the checksum deviates from a reference value.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zum Schutz von Speicherinhalten eines Speichers (MEM1, MEM2, MEM3) eines Computersystems unter Verwendung einer Hashfunktion. Um weniger Prozessor-Rechenzeit in Anspruch zu nehmen und weniger zusätzlichen Datentransfer zu generieren, ist ein Speicherkontroller (MC) vorgesehen, der eine in seinem Inneren angeordnete Hash-Einheit (HU) umfasst, welche selbstständig und autark jeweils eine kryptografische Prüfsumme (S) über bestimmte Speicherbereiche berechnet und mit Referenzwerten vergleicht, wobei bei einer Abweichung der Prüfsumme von einem Referenzwert eine Fehlermeldung generiert wird.



(84) **Bestimmungsstaaten** (soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,

CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— mit internationalem Recherchenbericht (Artikel 21 Absatz 3)

Beschreibung

Schutz von Speicherinhalten eines Speichers eines Computersystems unter Verwendung einer Hashfunktion

5

Technisches Gebiet

Die Erfindung betrifft ein Verfahren zum Schutz von Speicherinhalten eines Speichers eines Computersystems unter Verwendung einer Hashfunktion.

10

Der Speicher kann dabei aus nur einer Speichereinheit oder aus mehreren, insbesondere mehreren physischen, Speichereinheiten bestehen.

15

Eine Hashfunktion (auch Streuwertfunktion) ist eine Abbildung, die eine große Eingabemenge auf eine kleinere Zielmenge (die Hashwerte) abbildet. Dabei kann die Eingabemenge auch Elemente mit unterschiedlichen Längen enthalten, die Elemente der Zielmenge haben dagegen meist eine feste Länge. Die Hashwerte werden auch als Prüfsumme bezeichnet.

20

Das erfindungsgemäße Verfahren ist insbesondere dazu geeignet, in sicherheitsrelevanten eingebetteten Systemen (embedded systems) eingesetzt zu werden. Ein eingebettetes System bezeichnet einen elektronischen Rechner oder Computer, der in einen technischen Kontext eingebunden (eingebettet) ist. Dabei übernimmt der Rechner etwa Überwachungs-, Steuerungs- oder Regelfunktionen oder ist für eine Form der Daten- bzw. Signalverarbeitung zuständig. Meist wird dabei eine gemischte Hardware-Software-Implementierung gewählt, welche die große Flexibilität von Software mit der Leistungsfähigkeit der Hardware vereint. Die Software dient

25

30

dabei sowohl zur Steuerung des eingebetteten Systems selbst als auch gegebenenfalls zur Interaktion des eingebetteten Systems mit der Außenwelt über definierte Schnittstellen oder Protokolle.

5

Stand der Technik

Die Verwendung von Hashfunktionen in Computersystemen ist für einige Anwendungen bereits bekannt.

10

In der US 2009/0287901 A1 „System and Method for Content Replication Detection and Elimination in Main Memory“ wird ein Memory Controller, also ein Speicherkontroller, mit integrierter Hashfunktion beschrieben, wo die Prüfsumme dazu benutzt wird, doppelt vorhandene Speicherinhalte zu identifizieren.

15

In der US 2007/0234009 A1 „Processor having a Dedicated Hash Unit Integrated Within“ wird ein Prozessor mit Hashfunktion beschrieben, wobei Hashing hier die Optimierung der Zugriffe auf einen Cache-Bereich zum Ziel hat.

20

Auch die Verwendung von signaturbildenden kryptografischen Hashfunktionen zur Sicherung eines Speicherbereichs ist eine bereits bekannte Methode. Eine kryptografische Hashfunktion ist kollisionsresistent oder eine Einwegfunktion (oder beides).

25

Eine Hashfunktion h liefert zu einem Dokument x , aufgefasst als beliebig lange Bitfolge, eine Bitfolge $h(x)$ fester Länge. Falls zwei Dokumente x_1 und x_2 verschiedene Hashwerte $h(x_1)$ ungleich $h(x_2)$ haben, ist damit sichergestellt, dass die Dokumente x_1 und x_2 unterschiedlich sind. Die Umkehrung gilt jedoch nicht, da es viel mehr verschiedene mögliche Dokumente

30

als mögliche Hashwerte (= Prüfsummen) gibt. Zwei ungleiche Dokumente x_1 , x_2 mit gleichem Hashwert $h(x_1)=h(x_2)$ werden als Kollision bezeichnet. Soweit der Bereich der (zulässigen) Dokumente nicht eingeschränkt wird, kann eine Hashfunktion
5 also nicht echt kollisionsfrei sein. Inwieweit es zumindest in der praktischen Anwendung dennoch gerechtfertigt ist, aus gleichen Hashwerten auf gleiche Dokumente zu schließen, hängt von der verwendeten Hashfunktion ab.

10 Eine Einwegfunktion ist eine mathematische Funktion, die komplexitätstheoretisch „leicht“ berechenbar, aber „schwer“ umzukehren ist. In einem erweiterten Sinn werden auch Funktionen so bezeichnet, zu denen bisher keine in angemessener Zeit praktisch ausführbare Umkehrung bekannt
15 ist.

Es existieren standardisierte kryptografische Hashfunktionen, wie z.B. MD5, SHA256 oder SHA512. Dabei werden Speicherbereiche vor oder während des Schreibens in den Speicher
20 mittels einer Hashfunktion signiert und die Prüfsumme an sicherer Stelle als Referenz abgelegt. Im Falle einer verschlüsselten kryptografischen Hashfunktion wird auch noch ein geheimer Schlüssel einbezogen, der aus der Prüfsumme eine sogenannte Signatur bildet. Dadurch wird es einem Angreifer
25 erschwert, einen Speicherbereich zusammen mit der Prüfsumme zu manipulieren, da er den/die nötigen Schlüssel nicht kennt.

Während der Laufzeit werden die gesicherten Speicherabschnitte in periodischen Abständen ausgelesen und die
30 jeweilige Prüfsumme bzw. Signatur neu berechnet, um sie mit der Referenz vergleichen zu können. Diese Methode wird zum Beispiel in der Veröffentlichung „Runtime Execution Monitoring (REM) to Detect and Prevent Malicious Code Execution“, A. M. Fiskran und R.B. Lee, IEEE 30th

International Conference on Computer Design (ICCD) 2004,
Seiten 452-457, beschrieben.

Bisher werden diese, zum Teil sehr rechenintensiven
5 Operationen, entweder in Software abgebildet oder durch
eigene Hardware-Module realisiert. Im ersten Fall wird für
die Berechnung Prozessor-Rechenzeit, also CPU-Rechenzeit,
benötigt. In beiden Fällen wird zusätzlicher Datentransfer
generiert.

10

Darstellung der Erfindung

Es ist eine Aufgabe der vorliegenden Erfindung, ein Verfahren
zum Schutz von Speicherinhalten eines Speichers eines
15 Computersystems unter Verwendung einer Hashfunktion zur
Verfügung zu stellen, welches weniger CPU-Rechenzeit in
Anspruch nimmt. Im Vergleich zu eigenen Hardware-Modulen zur
Ausführung der Hashfunktion sowie im Vergleich zur Verwendung
des Hauptprozessors zur Ausführung der Hashfunktion soll
20 weniger zusätzlichen Datentransfer im Computersystem erzeugt
werden.

Mit dem erfindungsgemäßen Verfahren soll beispielsweise
sichergestellt werden, dass die Anwender-Software eines
25 eingebetteten Systems nicht manipuliert wird. Insbesondere
soll garantiert werden, dass die Software nur aus vertrauens-
würdigen Quellen stammt und während der Laufzeit nicht
verändert werden kann bzw. sollen Veränderungen des Programm-
codes während der Laufzeit erkannt werden, um Gegenmaßnahmen
30 einleiten zu können. Dies wird in der Informatik mit dem
Begriff „Secure Code Execution“ bezeichnet. Auch der
statische Speicherinhalt, wie Konfigurationsdateien, welche
in der Regel besonders schützenswert sind, soll geschützt
werden. Man spricht hier von „Integrity Protection“.

Die gestellte Aufgabe wird durch ein Verfahren mit den Merkmalen des Patentanspruchs 1 gelöst, indem ein Speicherkontroller vorgesehen ist. Der Speicherkontroller umfasst eine Hash-Einheit, welche selbstständig jeweils eine

5 kryptografische Prüfsumme über bestimmte Speicherbereiche berechnet und mit Referenzwerten vergleicht. Dabei wird bei einer Abweichung der Prüfsumme von einem Referenzwert eine Fehlermeldung generiert.

10 Der Speicherkontroller (auch Memory Controller) ist ein Hardware-Bauteil (z.B. ein Chip), durch welchen bei Computersystemen einen Datenfluss zwischen Prozessor einerseits und Arbeitsspeicher (oder weiteren Speichern) andererseits geregelt wird. Der Speicherkontroller ist entweder direkt im

15 Prozessor (Integrated Memory Controller – IMC) oder auf dem Mainboard untergebracht.

Die Hash-Einheit ist Teil des – in der Regel ohnehin vorhandenen – Speicherkontrollers und führt selbstständig die

20 notwendigen Berechnungen durch. Dadurch wird für die Berechnung der Hash-Funktionen keine CPU-Zeit benötigt. Auch fällt wenig zusätzlicher Datenverkehr an, weil die Daten nur zwischen dem Speicher, insbesondere dem Arbeitsspeicher, und dem Speicherkontroller ausgetauscht werden müssen. Dies

25 erfolgt in der Regel nicht über einen Bus des Computersystems, wie dies bei einem eigenen Bauteil zur Berechnung der Hash-Funktionen oder bei Verwendung des Prozessors der Fall wäre.

30 Aufgrund der Fehlermeldung können dann Gegenmaßnahmen gegen eine erfolgte Manipulation des Speichers eingeleitet werden.

Am einfachsten kann die Fehlermeldung, welche von der Hash-Einheit bei einer Abweichung der Prüfsumme von einem

Referenzwert generiert wird, zur Weiterverarbeitung an den Prozessor des Computersystems weitergeleitet werden, etwa in Form eines Interrupts.

5 Der Prozessor kann dann geeignete Gegenmaßnahmen treffen. So kann vorgesehen sein, dass der Prozessor den Zugriff auf den fehlerhaften Speicherbereich so lange unterbindet, bis der Speicherinhalt dieses Bereichs zurückgesetzt ist. Oder es wäre auch denkbar, dass die gesamte Speichereinheit, auf der
10 sich der fehlerhafte Speicherbereich befindet, gelöscht wird, also ein sogenannter „zero-erase“ durchgeführt wird.

Es wäre aber auch möglich, eine eigene Software oder Anwendung zur Bearbeitung der Fehlermeldungen zu verwenden,
15 etwa eine gegen Manipulationen gesicherte Software bzw. Anwendung. Bekannte derartige Software bzw. Anwendungen teilen das Prozessorsystem (oder die einzelnen, auf diesem Prozessor ablaufenden Prozesse (Programme)) logisch, also virtuell, in zwei Zonen oder „worlds“ auf, eine sichere Zone
20 oder „secure world“ und eine normale Zone oder „normal world“. Die sichere Zone könnte dann auch die Bearbeitung der Fehlermeldungen der Hash-Einheit übernehmen. Das Konzept der Aufteilung in zwei virtuelle Zonen wird beispielsweise durch die ARM® TrustZone® Technologie verwirklicht.

25 Von Vorteil ist, wenn die Berechnung der Prüfsumme für einen bestimmten Speicherbereich dann erfolgt, wenn der zugehörige Speicher unbenutzt ist, also keine Zugriffe von anderen Einheiten des Computersystems auf den Speicher erfolgen. Der
30 Speichercontroller nutzt also Phasen, in denen der Speicher unbenutzt ist, um die jeweiligen Speicherbereiche auszulesen und intern die Prüfsumme bzw. Signatur zu bilden. Dadurch werden andere Prozesse, welche auf diesen Speicher angewiesen sind, nicht verzögert.

Wenn der Speicherkontroller eine anteilige Speicher-Bandbreite für die Berechnung der Prüfsumme reserviert, dann ist damit eine maximale Zeitdauer festgelegt, innerhalb derer eine Manipulation des Speichers spätestens erkannt wird. Die Hash-Einheit würde also laufend auf den Speicher zugreifen und Prüfsummen berechnen, auch wenn andere Einheiten des Computersystems gerade auf den Speicher, bzw. die gleiche Speichereinheit, zugreifen. Wenn andere Einheiten des Computersystems später wieder nicht auf den Speicher zugreifen, steht der Hash-Einheit die gesamte Bandbreite des Speichers zur Verfügung.

Damit die Referenzwerte der kryptografischen Prüfsumme selbst möglichst nicht manipuliert werden können, kann vorgesehen sein, dass die Referenzwerte der kryptografischen Prüfsumme im Speicherkontroller in einem abgesicherten Speicherbereich abgespeichert werden.

Bei schlüsselabhängigen Hashfunktionen können auch die Schlüssel zur Verschlüsselung der Prüfsummen im Speicherkontroller im abgesicherten Speicherbereich abgespeichert werden. Es werden also zuerst die Prüfsummen mittels eines Schlüssels verschlüsselt und dann die verschlüsselten Prüfsummen, die auch als Signaturen bezeichnet werden, als Referenzwert abgespeichert.

In Zusammenhang mit dem abgesicherten Speicherbereich des Speicherkontrollers besteht eine Ausführungsvariante des erfindungsgemäßen Verfahrens darin, dass der abgesicherte Speicherbereich nur über zuvor als sicher eingestufte Einheiten des Computersystems abgefragt werden kann. Eine solche Einstufung der Einheiten des Computersystems in sichere und nicht sichere Einheiten kann zum Beispiel über eine bereits oben beschriebene Software oder Anwendung

erfolgen, welche auf dem Prozessor ablaufende Prozesse (Programme) und die dafür benötigten Einheiten logisch, also virtuell, in zwei Zonen oder „worlds“ aufteilt, eine sichere Zone oder „secure world“ und eine normale Zone oder „normal world“. Der Speichercontroller erkennt dann z.B. über ein
5 Seitenband-Signal des Busses oder über ein eigenes Bit, ob ein Zugriff auf den abgesicherten Speicherbereich von einer vertrauenswürdigen, also sicheren, Quelle kommt oder nicht.

10 Ein Computersystem zur Durchführung des erfindungsgemäßen Verfahrens umfasst zumindest einen Prozessor, einen Speichercontroller und einen Speicher, auf welchen über den Speichercontroller zugegriffen werden kann. Der Speichercontroller umfasst eine Hash-Einheit, welche so ausgebildet ist, dass
15 diese selbstständig jeweils eine kryptografische Prüfsumme über bestimmte Speicherbereiche berechnen und mit Referenzwerten vergleichen kann. Dabei ist eine Leitung zwischen Hash-Einheit und Prozessor vorgesehen, über welche bei einer Abweichung der Prüfsumme von einem Referenzwert eine Fehler-
20 meldung von der Hash-Einheit an den Prozessor gesendet werden kann.

Im Speichercontroller kann ein abgesicherter Speicherbereich vorgesehen sein, in welchem die Referenzwerte der krypto-
25 grafischen Prüfsumme abgespeichert werden können. Wie bereits oben erläutert, können dort auch die Schlüssel von schlüsselabhängigen Hashfunktionen sowie die verschlüsselten Prüfsummen (Signatures) abgelegt werden.

30 Das erfindungsgemäße Computersystem kann zum Beispiel als anwendungsspezifische, integrierte Schaltung (ASIC) oder als sogenanntes Field Programmable Gate Array (FPGA) ausgeführt sein. Insbesondere kann das erfindungsgemäße Computersystem

auch als Ein-Chip-System oder System-on-Chip (SoC) ausgestaltet sein.

Die Erfindung wird in der Regel unter Verwendung eines
5 Computerprogramms verwirklicht werden. Dementsprechend ist ein Computerprogrammprodukt vorgesehen, welches ein Programm umfasst, welches direkt in eine Hash-Einheit eines Speicherkontrollers eines Computersystems ladbar ist. Das Computerprogrammprodukt weist Programm-Mitteln auf, um alle jene
10 Schritte des erfindungsgemäßen Verfahrens auszuführen, welche von der Hash-Einheit ausgeführt werden, wenn das Programm ausgeführt wird.

Die gegenständliche Erfindung dient zur Sicherung von
15 kritischen Speicherbereichen eines Speichers gegen böswillige Manipulationen. Im Gegensatz zu bekannten Lösungen, bei welchen die Signaturprüfung mit Hilfe eines Prozessors erfolgt, kann durch die erfindungsgemäße Integration der Hash-Funktionalität direkt im Speicherkontroller das
20 restliche Computersystem deutlich entlastet werden.

Die erfindungsgemäße Lösung kann auch in Kombination mit sogenannten error-correcting codes (ECC) verwendet werden. Ein error-correcting code ist ein Algorithmus um eine Abfolge
25 von Zahlen so auszudrücken, dass auftretende Fehler in der Abfolge später erkannt und - mit Einschränkungen - auf Basis der restlichen Zahlen korrigiert werden können. Bei der error-correcting code Methode steht die Sicherung gegen zufällig auftretende Bit-Fehler, z.B. aufgrund von Strahlung,
30 im Vordergrund.

Kurzbeschreibung der Figuren

Zur weiteren Erläuterung der Erfindung wird im nachfolgenden Teil der Beschreibung auf die Figur Bezug genommen, aus welcher weitere vorteilhafte Ausgestaltungen, Einzelheiten und Weiterbildungen der Erfindung zu entnehmen sind. Die Figur ist beispielhaft zu verstehen und soll den Erfindungscharakter zwar darlegen, ihn aber keinesfalls einengen oder gar abschließend wiedergeben.

Die Figur zeigt ein Blockdiagramm eines erfindungsgemäßen Computersystems. Für das Computersystem sind in der Figur nur die für die Erfindung wesentlichen Einheiten dargestellt. Es kann und wird in der Regel darüber hinaus weitere Einheiten, wie z.B. Ein-/Ausgabeeinheiten, weitere Controller, zusätzliche Schnittstellen, weitere Prozessoren, Speicher, etc. enthalten.

Ausführung der Erfindung

In der Figur ist ein Computersystem dargestellt mit einem als Hauptprozessor dienenden Prozessor CPU, einem Arbeitsspeicher (RAM), der aus mehreren Speichereinheiten MEM1, MEM2, MEM3, besteht, sowie einem Speicherkontroller MC. Der Speicherkontroller MC ist den Speichereinheiten MEM1, MEM2, MEM3 vorgeschaltet und über einen Systembus BUS mit dem Prozessor CPU verbunden.

Mit dem Begriff Systembus werden die verschiedenen Daten-schienen (Busse) zusammengefasst, über welche in einem Mikrorechner der Prozessor CPU mit seiner Umgebung kommuniziert. In der Regel werden drei solcher Busse unterschieden: der Datenbus, der Adressbus und der Steuerbus. Der Systembus BUS kann als sogenannte Busmatrix ausgeführt sein,

von welcher parallele Zugriffswege von mehreren Master-Einheiten auf mehrere Slave-Einheiten bereitgestellt werden.

Der Systembus BUS bindet hier auch mehrere Peripherie-
5 einheiten P1, P2, P3, z.B. Slave-Einheiten an das Computersystem an.

Der Speicherkontroller MC weist in üblicher Weise zum Systembus BUS hin ein Bus-Interface BUS-I und zu den Speicher-
10 einheiten MEM1, MEM2, MEM3 hin ein RAM Interface RAM-I auf. Dadurch verbindet der Speicherkontroller MC den Prozessor CPU mit den Speichereinheiten MEM1, MEM2, MEM3. Ein Arbeitsspeicher- bzw. RAM-Controller RAM-C des Speicherkontrollers MC steht sowohl mit dem Bus-Interface BUS-I als auch mit dem
15 RAM Interface RAM-I in Verbindung. Gleiches gilt für den abgesicherten Speicherbereich SS, in welchem die Prüfsummen (Signatures) S und die Adressen R der zugehörigen Speicherbereiche der einzelnen Speichereinheiten MEM1, MEM2, MEM3 abgelegt sind. Für die Schlüssel K von schlüsselabhängigen
20 Hashfunktionen ist ebenfalls ein eigener Bereich im abgesicherten Speicherbereich SS vorgesehen.

Ein Zugriff auf den abgesicherten Speicherbereich SS des Speicherkontrollers MC kann von außerhalb des Speicherkontrollers MC nur über das Bus-Interface BUS-I erfolgen,
25 welches nur Zugriffe von vertrauenswürdigen Busteilnehmern zulässt. Dies kann etwa durch die TrustZone® Technologie sichergestellt werden.

30 Der abgesicherte Speicherbereich SS des Speicherkontrollers MC ist weiterhin mit der Hash-Einheit HU verbunden, welche ebenfalls im Inneren des Speicherkontrollers MC angeordnet ist. Die Hash-Einheit HU ist darüber hinaus mit dem RAM Interface RAM-I verbunden, um auf die Speichereinheiten MEM1,

- MEM2, MEM3 zugreifen zu können. Über eine Leitung L ist die Hash-Einheit HU direkt mit dem Prozessor CPU verbunden, um Fehlermeldungen, wenn eine Signatur als nicht korrekt erkannt worden ist, als Interrupt an den Prozessor CPU senden zu können. Der Prozessor CPU kann dann geeignete Gegenmaßnahmen vornehmen. So kann der Prozessor CPU einen Zugriff auf einen fehlerhaften Speicherbereich so lange verhindern, bis eine sichere Anwendung den Speicherinhalt zurücksetzt.
- 10 Die Hash-Einheit HU berechnet nun selbstständig für einzelne Speicherbereiche der Speichereinheiten MEM1, MEM2, MEM3 jeweils eine kryptografische Prüfsumme S. Die Hash-Einheit HU verschlüsselt diese und speichert die so entstandene verschlüsselte Prüfsumme S (Signatur) dieses Speicherbereichs
- 15 als Referenzwert im abgesicherten Speicherbereich SS des Speicherkontrollers MC ab. Ebenso wird der zugehörigen Schlüssel K im abgesicherten Speicherbereich SS abgespeichert. Die Adresse R des untersuchten Speicherbereichs oder eine sonstige Kennzeichnung dieses Speicherbereichs wird ebenso abgespeichert. Wenn für diesen Speicherbereich dann später wieder die kryptografische Prüfsumme S gebildet wird, dann wird diese durch die Hash-Einheit HU mit dem abgespeicherten Referenzwert verglichen. Sind neu
- 20 berechnete Prüfsumme und Referenzwert gleich, so ist dieser Speicherbereich in Ordnung. Gibt es eine Abweichung, so wird von der Hash-Einheit HU eine Fehlermeldung bzw. ein so genannter Interrupt an den Prozessor CPU, von welchem dann Gegenmaßnahmen gesetzt werden.
- 30 Als Hashfunktionen verwendet die Hash-Einheit HU eingangs genannte kryptografische Hashfunktionen, wie z.B. basierend auf MD5, SHA256 oder SHA512, insbesondere basierend auf Letzterer.

Bezugszeichenliste:

	BUS	Systembus
	BUS-I	Bus-Interface
5	CPU	Prozessor
	HU	Hash-Einheit (hashing unit)
	K	Schlüssel (keys)
	L	Leitung zwischen Hash-Einheit HU und Prozessor CPU
	MC	Speichercontroller (memory controller)
10	MEM1	erste Speichereinheit (memory unit)
	MEM2	zweite Speichereinheit (memory unit)
	MEM3	dritte Speichereinheit (memory unit)
	P1	erste Peripherieeinheit (peripheral unit)
	P2	zweite Peripherieeinheit (peripheral unit)
15	P3	dritte Peripherieeinheit (peripheral unit)
	R	Adressen der Speicherbereiche der Speichereinheiten (range)
	RAM-C	RAM Controller
	RAM-I	RAM Interface
20	S	Prüfsumme (signature)
	SS	abgesicherter Speicherbereich (secure storage)

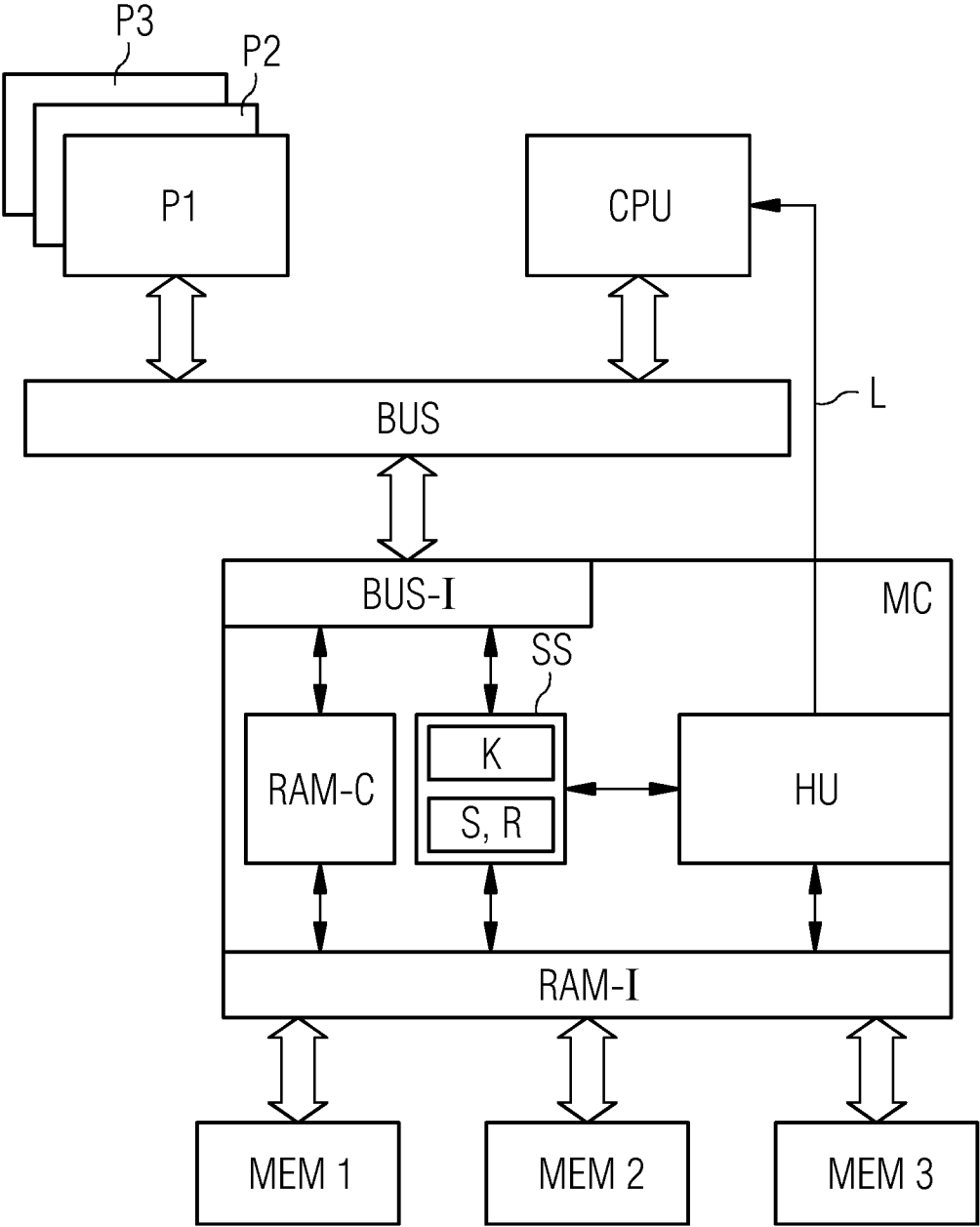
Patentansprüche

1. Verfahren zum Schutz von Speicherinhalten eines Speichers (MEM1, MEM2, MEM3) eines Computersystems unter Verwendung einer Hashfunktion, **dadurch gekennzeichnet**, dass ein Speicherkontroller (MC) vorgesehen ist, welcher eine im Inneren angeordnete Hash-Einheit (HU) umfasst, welche selbstständig jeweils eine kryptografische Prüfsumme (S) über bestimmte Speicherbereiche berechnet und mit Referenzwerten vergleicht, wobei bei einer Abweichung der Prüfsumme von einem Referenzwert eine Fehlermeldung generiert wird.
2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass die Fehlermeldung an den Prozessor (CPU) des Computersystems weitergeleitet wird.
3. Verfahren nach Anspruch 2, **dadurch gekennzeichnet**, dass der Prozessor (CPU) den Zugriff auf den fehlerhaften Speicherbereich so lange unterbindet, bis der Speicherinhalt dieses Bereichs zurückgesetzt ist.
4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet**, dass die Fehlermeldung durch eine gegen Manipulationen gesicherte Software bearbeitet wird.
5. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet**, dass die Berechnung der Prüfsumme (S) für einen bestimmten Speicherbereich dann erfolgt, wenn der zugehörige Speicher (MEM1, MEM2, MEM3) unbenutzt ist.
6. Verfahren nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet**, dass der Speicherkontroller (MS) eine anteilige Speicher-Bandbreite für die Berechnung der Prüfsumme (S) reserviert.

7. Verfahren nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet**, dass die Referenzwerte der kryptografischen Prüfsumme (S) im Speichercontroller (MC) in einem abgesicherten Speicherbereich (SS) abgespeichert werden.
8. Verfahren nach Anspruch 7, **dadurch gekennzeichnet**, dass bei schlüsselabhängigen Hashfunktionen die Schlüssel (K) zur Verschlüsselung der Prüfsummen (S) im Speichercontroller (MC) im abgesicherten Speicherbereich (SS) abgespeichert werden.
9. Verfahren nach einem der Ansprüche 7 oder 8, **dadurch gekennzeichnet**, dass der abgesicherte Speicherbereich (SS) nur über zuvor als sicher eingestufte Einheiten des Computersystems abgefragt werden kann.
10. Computersystem zur Durchführung des Verfahren nach einem der Ansprüche 1 bis 9, umfassend zumindest einen Prozessor (CPU), einen Speichercontroller (MC) und einen Speicher (MEM1, MEM2, MEM3), auf den über den Speichercontroller (MC) zugegriffen werden kann, **dadurch gekennzeichnet**, dass der Speichercontroller (MC) eine im Inneren angeordnete Hash-Einheit (HU) umfasst, welche so ausgebildet ist, dass diese selbstständig jeweils eine kryptografische Prüfsumme (S) über bestimmte Speicherbereiche berechnen und mit Referenzwerten vergleichen kann, wobei eine Leitung (L) zwischen Hash-Einheit (HU) und Prozessor (CPU) vorgesehen ist, über welche bei einer Abweichung der Prüfsumme von einem Referenzwert eine Fehlermeldung von der Hash-Einheit (HU) an den Prozessor (CPU) gesendet werden kann.
11. Computersystem nach Anspruch 10, **dadurch gekennzeichnet**, dass im Speichercontroller (MC) ein abgesicherter

Speicherbereich (SS) vorgesehen ist, in welchem die Referenzwerte der kryptografischen Prüfsumme (S) abgespeichert werden können.

12. Computerprogrammprodukt, welches ein Programm umfasst,
5 das direkt in eine Hash-Einheit (HU) eines
Speicherkontrollers (MC) eines Computersystems ladbar
ist, mit Programm-Mitteln, um alle Schritte des
Verfahrens nach einem der Ansprüche 1, 2 oder 5 bis 9
auszuführen, wenn das Programm ausgeführt wird.



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/053677

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/64 G06F21/70 G06F21/78
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/226551 A1 (JANKE MARCUS [DE] ET AL) 27 September 2007 (2007-09-27) paragraph [0002] paragraph [0006] - paragraph [0007]; figure 1 paragraph [0010] paragraph [0049]	1-12
X	US 2002/099946 A1 (HERBERT HOWARD C [US] ET AL) 25 July 2002 (2002-07-25) paragraph [0008] paragraph [0015] - paragraph [0018] paragraph [0032] paragraph [0030] claim 15 figure 5b	1-12



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

25 April 2016

Date of mailing of the international search report

03/05/2016

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Dobre, Dan

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2016/053677

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Anonymous: "Memory scrubbing - Wikipedia, the free encyclopedia", 22 February 2015 (2015-02-22), XP055207484, Retrieved from the Internet: URL:https://en.wikipedia.org/w/index.php?t itle=Memory_scrubbing&oldid=648287843 [retrieved on 2015-08-12] Patrol scrubbing -----	1-12
A	US 2011/145600 A1 (RUDELIC JOHN C [US]) 16 June 2011 (2011-06-16) the whole document -----	1-12

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2016/053677

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007226551 A1	27-09-2007	DE 102006001873 A1	19-07-2007
		US 2007226551 A1	27-09-2007

US 2002099946 A1	25-07-2002	US 2002099946 A1	25-07-2002
		US 2004186994 A1	23-09-2004

US 2011145600 A1	16-06-2011	NONE	

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES INV. G06F21/64 G06F21/70 G06F21/78 ADD.		
Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC		
B. RECHERCHIERTE GEBIETE Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole) G06F		
Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen		
Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe) EPO-Internal, WPI Data		
C. ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2007/226551 A1 (JANKE MARCUS [DE] ET AL) 27. September 2007 (2007-09-27) Absatz [0002] Absatz [0006] - Absatz [0007]; Abbildung 1 Absatz [0010] Absatz [0049]	1-12
X	US 2002/099946 A1 (HERBERT HOWARD C [US] ET AL) 25. Juli 2002 (2002-07-25) Absatz [0008] Absatz [0015] - Absatz [0018] Absatz [0032] Absatz [0030] Anspruch 15 Abbildung 5b ----- -/-	1-12
☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie		
* Besondere Kategorien von angegebenen Veröffentlichungen : "A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist "E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist "L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt) "O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht "P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist "T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist "X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden "Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist "&" Veröffentlichung, die Mitglied derselben Patentfamilie ist		
Datum des Abschlusses der internationalen Recherche 25. April 2016		Absendedatum des internationalen Recherchenberichts 03/05/2016
Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Bevollmächtigter Bediensteter Dobre, Dan

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	Anonymous: "Memory scrubbing - Wikipedia, the free encyclopedia", 22. Februar 2015 (2015-02-22), XP055207484, Gefunden im Internet: URL:https://en.wikipedia.org/w/index.php?title=Memory_scrubbing&oldid=648287843 [gefunden am 2015-08-12] Patrol scrubbing -----	1-12
A	US 2011/145600 A1 (RUDELIC JOHN C [US]) 16. Juni 2011 (2011-06-16) das ganze Dokument -----	1-12

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2016/053677

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2007226551 A1	27-09-2007	DE 102006001873 A1	19-07-2007
		US 2007226551 A1	27-09-2007

US 2002099946 A1	25-07-2002	US 2002099946 A1	25-07-2002
		US 2004186994 A1	23-09-2004

US 2011145600 A1	16-06-2011	KEINE	
