(19) Deutsches Patent- und Markenamt

(10) **DE 10 2020 213 611 A1** 2022.05.05

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2020 213 611.4**
(22) Anmeldetag: **29.10.2020**
(43) Offenlegungstag: **05.05.2022**

(51) Int Cl.: ***G06F 21/72*** (2013.01)
H04L 9/14 (2006.01)

(71) Anmelder:
Robert Bosch Gesellschaft mit beschränkter Haftung, 70469 Stuttgart, DE

(72) Erfinder:
Poinstingl, Peter, Purgstall/Erlauf, AT; Boeswart, Klaus, Wien, AT

(56) Ermittelter Stand der Technik:

US	**9 172 532**	**B1**
US	**9 866 375**	**B2**
US	**10 719 567**	**B2**
US	**2015 / 0 310 219**	**A1**
US	**2018 / 0 109 508**	**A1**
US	**2019 / 0 081 775**	**A1**
US	**2020 / 0 053 065**	**A1**

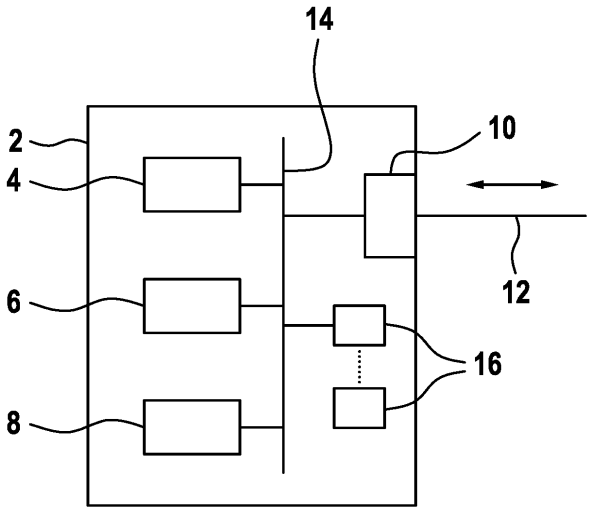
Hardware security module. In: Wikipedia, The Free Encyclopedia. Bearbeitungsstand: 27. Oktober 2020. URL: https://en.wikipedia.org/w/index.php?title=Hardware_security_module&oldid=985784016 [abgerufen am 12. Mai 2021]

Rechercheantrag gemäß § 43 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Verfahren zur Anwendung kryptographischer Funktionen auf Daten unter Verwendung verschiedener Schlüssel**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Anwendung kryptographischer Funktionen auf Daten unter Verwendung verschiedener Schlüssel in einer Recheneinheit, die ein Hostsystem (4), ein Hardware-Sicherheits-Modul, Hardware-Sicherheits-Modul (6), und ein Beschleunigermodul (8), das eingerichtet ist, kryptographische Funktionen durchzuführen umfasst, umfassend ein Bereitstellen, in dem Hostsystem (4), verschlüsselter Schlüssel, wobei die verschlüsselten Schlüssel aus den verschiedenen Schlüsseln durch Verschlüsseln mit einem Hauptschlüssel gebildet sind, der vom Hardware-Sicherheits-Modul (6) gespeichert wird, ein Laden, durch das Hardware-Sicherheits-Modul (6), des Hauptschlüssels in das Beschleunigermodul (8), wobei beim Anwenden einer kryptographischen Funktion auf Daten jeweils durchgeführt wird: ein Laden, durch das Hostsystem (4), eines den Daten zugeordneten verschlüsselten Schlüssels in das Beschleunigermodul (8), ein Entschlüssen, durch das Beschleunigermodul (8), des verschlüsselten Schlüssels mit dem Hauptschlüssel, ein Laden, durch das Hostsystem (4), der Daten in das Beschleunigermodul (8), ein Anwenden, durch das Beschleunigermodul (8), der kryptographischen Funktion auf die Daten unter Verwendung des entschlüsselten Schlüssels, um ein entsprechendes Ergebnis zu erhalten und ein Lesen, durch das Hostsystem (4), des Ergebnisses aus dem Beschleunigermodul (8).



Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren zur Anwendung kryptographischer Funktionen auf Daten unter Verwendung verschiedener Schlüssel sowie eine Recheneinheit und ein Computerprogramm zu dessen Durchführung.

Hintergrund der Erfindung

[0002] In Maschinen und Fahrzeugen werden programmierbare Steuergeräte eingesetzt, um diese oder auch Komponenten davon, zu steuern. Beispielsweise kann ein Kraftfahrzeug Steuergeräte für die Motorsteuerung, für das Bremssystem usw. enthalten. Die Steuergeräte umfassen üblicherweise mindestens einen Prozessor mit einem oder mehreren Prozessor-Kernen. In diesen Prozessorkernen wird eine Steuerungssoftware ausgeführt (vereinfacht auch als Host bzw. Hostsystem bezeichnet), d.h. es werden einem Speicher gespeicherte Anwendungsprogramme ausführt, um die Steuerungsfunktion des Steuergeräts zu erzielen.

[0003] Die Steuergeräte eines Fahrzeugs oder einer Maschine können miteinander und oftmals auch mit externen Recheneinheiten vernetzt sein, d.h. zur Datenkommunikation verbunden sein. Aus Sicherheitsgründen wird diese Kommunikation kryptografisch abgesichert. Dabei kann beispielsweise eine Verschlüsselung und/oder Signierung von Botschaften, mit denen Daten übermittelt werden, vorgesehen sein. Zur Implementierung der kryptografischen Absicherung können Steuergeräte mit einem Hardware-Sicherheits-Modul (HSM) ausgestattet, das als Vertrauensanker im Steuergerät dient, d.h. aus Sicht des Hostsystems (bzw. der darin ausgeführten Anwendungsprogramme) werden Informationen vom HSM bzw. von im HSM ausgeführten Programmen als korrekt, nicht kompromittiert, erachtet. Das HSM kann ein dezidierter Prozessor oder ein dezidierter Prozessorkern sein, der auf einen eigenen Datenspeicher und einen eigenen Programmspeicher zugreift, auf die andere Prozessorkerne, d.h. Prozessorkerne des Hosts, nicht zugreifen können. Zur Beschleunigung der Ausführung kryptografischer Funktionen können diese in einem entsprechenden Beschleunigermodul, das als Hardwaremodul ausgeführt ist, realisiert sein.

Offenbarung der Erfindung

[0004] Erfindungsgemäß werden ein Verfahren zur Anwendung kryptographischer Funktionen auf Daten unter Verwendung verschiedener Schlüssel sowie eine Recheneinheit und ein Computerprogramm zu dessen Durchführung mit den Merkmalen der unabhängigen Patentansprüche vorgeschlagen. Vorteilhafte Ausgestaltungen sind Gegenstand der Unteransprüche sowie der nachfolgenden Beschreibung.

[0005] Die Erfindung ermöglicht die Verwendung einer hohen, skalierbaren Anzahl voneinander verschiedener Schlüssel, da die Anzahl nicht durch den Speicherplatz, der in der sicheren Umgebung (HSM, Beschleunigermodul) zur Verfügung steht, begrenzt wird. Daraus resultiert eine Verringerung der Angriffsfläche, wenn ein Anwendungsprogramm in einer Recheneinheit kompromittiert ist, so dass die Sicherheit eines darauf basierenden Systems erhöht werden kann.

[0006] Erfindungsgemäß werden dazu ein Verfahren zur Anwendung kryptographischer Funktionen auf Daten unter Verwendung verschiedener Schlüssel und eine Recheneinheit, die ein Hostsystem, ein Hardware-Sicherheits-Modul, HSM, und ein Beschleunigermodul umfasst, vorgeschlagen. Um zu gewährleisten, dass die Schlüssel selbst dem möglicherweise kompromittierten Hostsystem bzw. einem darin ausgeführten Anwendungsprogramm nicht bekannt werden, werden die Schlüssel dem Hostsystem als verschlüsselte Schlüssel bereitgestellt, wobei die verschlüsselten Schlüssel aus den verschiedenen Schlüsseln durch Verschlüsseln mit einem Hauptschlüssel gebildet sind, der vom HSM gespeichert wird. Das HSM lädt den Hauptschlüssel in das Beschleunigermodul, so dass dieses jeweils im weiteren Verfahren empfangene verschlüsselte Schlüssel entschlüsseln kann. Beim Anwenden einer kryptographischen Funktion auf Daten wird jeweils ein den Daten zugeordneter verschlüsselter Schlüssel in das Beschleunigermodul geladen und mit dem Hauptschlüssel entschlüsselt. Ebenso werden die Daten in das Beschleunigermodul geladen und durch das Beschleunigermodul die kryptographische Funktion auf die Daten unter Verwendung des entschlüsselten Schlüssels angewendet, um ein entsprechendes Ergebnis zu erhalten. Das Ergebnis wird dann aus dem Beschleunigermodul gelesen.

[0007] Das Hostsystem bildet im Prinzip eine Umgebung, in der die eigentliche Funktion der Recheneinheit, z.B. Steuerungsfunktionen eines Kraftfahrzeugs oder einer Maschine, mittels entsprechender Anwendungssoftware implementiert wird. Das Hostsystem umfasst einen oder mehrere Prozessorkerne, die dazu eingerichtet sind, Anwendungsprogramme auszuführen. Die Anwendungsprogramme und Daten werden vom Hostsystem in einem Speicher gespeichert. Der Speicher umfasst typischerweise einen flüchtigen und/oder einen nichtflüchtigen Speicher. In dem Speicher können insbesondere auch die verschlüsselten Schlüssel gespeichert werden, vorzugsweise in einem nichtflüchtigen Speicher, so dass sie nicht mit jedem Neustart der Recheneinheit erneut übermittelt werden müssen. Die verschlüsselten Schlüssel können, etwa nach Neustart der Recheneinheit, selbstverständlich auch durch das Hostsystem aus dem nichtflüchtigen in einen flüchti-

gen Speicher (Arbeitsspeicher) geladen werden, um darauf schneller zugreifen zu können.

[0008] Das Hostsystem ist üblicherweise weiterhin über eine Kommunikationsverbindung der Recheneinheit mit anderen Recheneinheiten verbunden. Diese Verbindung kann drahtlos oder drahtgebunden sein, etwa ein CAN-Bus in einem Kraftfahrzeug. Daten, die von den Anwendungsprogrammen in Form von Botschaften bzw. Nachrichten über die Kommunikationsverbindung gesendet oder empfangen werden, werden aus Sicherheitsgründen kryptographisch abgesichert, d.h. verschlüsselt und/oder mittels eines Nachrichtenauthentifizierungsverfahrens abgesichert. Um kryptographische Verfahren zu beschleunigen, werden diese unter Verwendung des Beschleunigermoduls durchgeführt.

[0009] Das Beschleunigermodul ist dazu eingerichtet, kryptographische Funktionen durchzuführen. Dabei werden von einer aufrufenden Einheit (hier Hostsystem oder HSM) dem Beschleunigermodul ein Schlüssel und Daten übermittelt, bzw. in das Beschleunigermodul geladen, etwa an jeweils dafür vorgesehene Adressen des Beschleunigermoduls. Das Beschleunigermodul führt dann für die Daten die kryptographische Funktion unter Verwendung des Schlüssels durch, d.h. das Beschleunigermodul wendet die kryptographische Funktion auf die Daten an, wobei der Schlüssel verwendet wird. Das Ergebnis dieser Anwendung kann dann von der aufrufenden Einheit wieder aus dem Beschleunigermodul gelesen werden. Die Form des Ergebnisses hängt von der kryptographischen Funktion ab. Handelt es sich beispielweise um eine Verschlüsselungsfunktion, werden die Daten mit dem Schlüssel verschlüsselt und das Ergebnis sind die verschlüsselten Daten; umgekehrt, wenn die Daten verschlüsselte Daten sind und es sich um eine Entschlüsselungsfunktion handelt, werden die verschlüsselten Daten mit dem Schlüssel in entschlüsselte Daten gewandelt, welche das Ergebnis der Entschlüsselung sind. Bei einem Nachrichtenauthentifizierungsverfahren wird aus den Daten der Nachrichtenauthentifizierungscode (MAC, Message Authentication Code) als Ergebnis bestimmt oder, wenn die Daten eine Nachricht und einen zugehörigen MAC enthalten, geprüft, ob dieser korrekt oder nicht korrekt ist, was dann das Ergebnis darstellt. Im Allgemeinen kann lediglich das Ergebnis aus dem Beschleunigermodul gelesen werden, zum Beschleunigermodul übertragene Daten und Schlüssel können nicht ausgelesen werden, insbesondere der Hauptschlüssel kann also nicht durch das Hostsystem aus dem Beschleunigermodul gelesen werden.

[0010] Das Beschleunigermodul, das insbesondere ein Hardwaremodul ist, ist dazu eingerichtet, kryptographische Funktion entsprechend bestimmter, an sich bekannter Verfahren durchzuführen. Dies können insbesondere sein: AES (Advanced Encryption Standard), DES (Data Encryption Standard), CMAC (Cipher-Based Message Authentication Code, d.h. ein Nachrichtenauthentifizierungscode, der unter Verwendung eines Blockverschlüsselungsverfahrens, insbesondere AES oder DES, implementiert ist).

[0011] Das Hardware-Sicherheits-Modul (HSM) umfasst einen eigenen Speicher, auf den nur das HSM, bzw. ein Prozessorkern des HSM, zugreifen kann. In diesem kann der Hauptschlüssel gespeichert werden. Dem Hostsystem (oder anderen Recheneinheiten) bzw. darin ausgeführten, möglicherweise kompromittierten Anwendungsprogrammen ist es nicht möglich, auf den Speicher des HSM zuzugreifen, so dass diese nicht in Kenntnis des Hauptschlüssels gelangen können. Das HSM stellt eine sichere Umgebung der Recheneinheit dar, d.h. Information bzw. im HSM ausgeführte Prozessen werden, insbesondere durch das Hostsystem, als vertrauenswürdig erachtet. Ein Zugriff bzw. eine Änderung von Daten und/oder Programmen im HSM ist nur mit entsprechender Authentifizierung möglich, insbesondere das Hostsystem kann (im Regelbetrieb) solche Zugriffe bzw. Änderungen nicht durchführen.

[0012] Die Erfindung entfaltet besondere Vorteile in Fällen, in denen zahlreiche Schlüssel verwendet werden sollen und dafür ggf. nicht genügend sicherer Speicherplatz im HSM zur Verfügung steht. Um beispielsweise zu verhindern, dass die gesamte Kommunikation zwischen den Steuergeräten des Fahrzeugs bzw. der Maschine oder zumindest die gesamte Kommunikation mit dem kompromittierten Steuergerät kompromittiert wird, wenn ein Angreifer in Kenntnis eines Schlüssels gelangt, etwa wenn eines der Steuergeräte kompromittiert wurde, können Botschaften in Botschaftsgruppen mit gleichen Sendern und Empfängern eingeteilt werden, wobei jede Botschaftsgruppe einen eigenen Schlüssel erhält, so dass eine Vielzahl verschiedener Schlüssel verwendet wird. Auf diese Weise kann die Angriffsfläche, die durch Kenntnis eines Schlüssels bzw. durch ein kompromittiertes Steuergerät ausgenutzt werden kann, verringert werden. Insbesondere muss durch die Erfindung beim Design bzw. der Herstellung des HSM die Anzahl der später benötigten Schlüssel noch gar nicht bekannt sein.

[0013] Vorteilhafterweise umfasst der Schritt des Bereitstellens der verschlüsselten Schlüssel ein Verschlüsseln, durch das HSM, eines oder mehrerer der verschiedenen Schlüssel unter Verwendung des Hauptschlüssels und ein Übertragen, durch das HSM, der verschlüsselten Schlüssel an das Hostsystem.

[0014] Bevorzugt werden der eine oder die mehreren der verschiedenen Schlüssel von dem HSM generiert oder von dem HSM über eine verschlüsselte Kommunikation empfangen. Wenn die Schlüssel vom HSM generiert werden, können diese über eine sichere, verschlüsselte Kommunikationsverbindung anderen Recheneinheiten, die Botschaften unter Verwendung dieser Schlüssel von dem System (Hostsystem, HSM, Beschleunigermodul) empfangen und/oder zu diesem senden, übermittelt werden. Die (nicht verschlüsselten) Schlüssel sind somit nur in jeweils sicheren Umgebungen bekannt.

[0015] Bevorzugt umfasst das Verfahren weiterhin ein Bestimmen, durch das Hostsystem, des den Daten zugeordneten verschlüsselten Schlüssels. Weiter bevorzugt sind Zuordnungskennzeichnungen für die verschlüsselten Schlüssel vorgesehen, auf Grundlage derer der den Daten zugeordnete verschlüsselte Schlüssel bestimmt wird. Es kann sich dabei beispielsweise um eine Nummerierung handeln. Solche Zuordnungskennzeichnungen ermöglichen es der Recheneinheit selbst und auch anderen Recheneinheiten, die jeweiligen Daten den richtigen (zugeordneten) Schlüssel zu verwenden.

[0016] Zweckmäßigerweise sind die kryptographischen Funktionen eine oder mehrere von einem symmetrischen Verschlüsselungsverfahren, insbesondere Verschlüsselung und/oder Entschlüsselung von Botschaften, und einem Nachrichtenauthentifizierungsverfahren, insbesondere Berechnung eines Nachrichtenauthentifizierungscodes. Solche Verfahren sind dem Fachmann an sich bekannt, so dass diese in bereits vorhandenen Beschleunigermodulen implementiert sein können, was die Anwendung des erfindungsgemäßen Verfahrens bei bereits vorhandenen Recheneinheiten ermöglicht.

[0017] Eine erfindungsgemäße Recheneinheit, z.B. ein Steuergerät eines Kraftfahrzeugs oder ein in einem solchen umfasster Mikrocontroller, ist, insbesondere programmtechnisch, dazu eingerichtet, ein erfindungsgemäßes Verfahren durchzuführen.

[0018] Auch die Implementierung eines erfindungsgemäßen Verfahrens in Form eines Computerprogramms oder Computerprogrammprodukts mit Programmcode zur Durchführung aller Verfahrensschritte ist vorteilhaft, da dies besonders geringe Kosten verursacht, insbesondere wenn ein ausführendes Steuergerät noch für weitere Aufgaben genutzt wird und daher ohnehin vorhanden ist. Geeignete Datenträger zur Bereitstellung des Computerprogramms sind insbesondere magnetische, optische und elektrische Speicher, wie z.B. Festplatten, Flash-Speicher, EEPROMs, DVDs u.a.m. Auch ein Download eines Programms über Computernetze (Internet, Intranet usw.) ist möglich.

[0019] Weitere Vorteile und Ausgestaltungen der Erfindung ergeben sich aus der Beschreibung und der beiliegenden Zeichnung.

[0020] Die Erfindung ist anhand von Ausführungsbeispielen in der Zeichnung schematisch dargestellt und wird im Folgenden unter Bezugnahme auf die Zeichnung beschrieben.

Figurenliste

Fig. 1 zeigt eine Recheneinheit gemäß einer bevorzugten Ausführungsform, die zur Durchführung eines erfindungsgemäßen Verfahrens verwendet werden kann;und

Fig. 2 zeigt ein Ablaufdiagramm gemäß einer bevorzugten Ausführungsform der Erfindung.

Ausführungsform(en) der Erfindung

[0021] Fig. 1 stellt eine Recheneinheit 2 gemäß einer bevorzugten Ausführungsform dar, die zur Durchführung eines erfindungsgemäßen Verfahrens verwendet werden kann. Die Recheneinheit 2, z.B. ein Mikrocontroller, z.B. eines Steuergeräts, weist ein Hostsystem 4, ein Hardware-Sicherheits-Modul (HSM) 6 und ein Beschleunigermodul 8 auf. Weiter weist die Recheneinheit 2 eine Schnittstelle 10, die dem Datenaustausch mit anderen Recheneinheiten dient, etwa über eine Verbindungsleitung 12 auf. Die Schnittstelle 10 kann eine beliebige drahtlose oder drahtgebundene Schnittstelle sein; sie kann beispielsweise eine serielle oder parallele Schnittstelle sein. Beispiele sind insbesondere Feldbusse, z.B. ein CAN-Bus (Controller Area Network), eine Ethernet-Schnittstelle, eine SPI-Schnittstelle (Serial Peripheral Interface), eine WLAN-Schnittstelle (Wireless Local Area Network) oder ähnliches.

[0022] Das Hostsystem 4, das HSM 6, das Beschleunigermodul 8 und die Schnittstelle 10 sind zumindest teilweise untereinander mit Verbindungen bzw. Leitungen 14 zum Datenaustausch verbunden. Diese Verbindungen können seriell oder parallel sein. Es sind Punkt-zu-Punkt-Verbindungen und/oder Stern-Verbindungen und/oder Bus-Verbindungen (ähnlich wie dargestellt) möglich.

[0023] Weiterhin können weitere Bauelemente 16, z.B. ein Speicher, in der Recheneinheit enthalten sein, die ebenfalls mit dem Hostsystem, dem HSM, dem Beschleunigermodul und der Schnittstelle zum Datenaustausch verbunden sein können.

[0024] Das Hostsystem 4 und das HSM 6 weisen jeweils mindestens einen Prozessorkern, in dem Programme ausgeführt werden, um die Funktion des Hostsystems bzw. HSM zu implementieren, auf. Die Prozessorkerne des Hostsystems und des HSM können in verschiedenen Prozessormodulen

oder auch in einem gemeinsamen Prozessormodul enthalten sein, wobei das Hostsystem, d.h. insbesondere dessen Prozessorkerne, keinen Zugriff auf das HSM, insbesondere dessen Prozessorkerne, hat. Das Hostsystem 4 und das HSM 6 können weitere Elemente umfassen, insbesondere jeweils einen flüchtigen (Arbeits-)Speicher und/oder einen nichtflüchtigen Speicher, z.B. Flash.

[0025] Das Beschleunigermodul 8 ist als Hardwaremodul ausgeführt und dazu eingerichtet, kryptographische Funktionen durchzuführen, wobei dazu ein Schlüssel und Daten von einer aufrufenden Einheit (Hostsystem und/oder HSM) in das Hardwaremodul geladen werden, das Hardwaremodul dann eine entsprechend spezifizierte kryptographische Funktion unter Benutzung des geladen Schlüssels auf die geladenen Daten anwendet, und das Ergebnis dieser Anwendung der kryptographischen Funktion dann von der aufrufenden Einheit ausgelesen werden kann und/oder auch in dem Hardwarebeschleuniger weiterverwendet werden kann.

[0026] Das Hostsystem 4, das HSM 6, das Beschleunigermodul 8, die Schnittstelle 10 und gegebenenfalls weitere Bauelemente 16 können zumindest teilweise miteinander integriert ausgebildet sein, z.B. in einem gemeinsamen Chip (integrierte Schaltung, IC).

[0027] Fig. 2 stellt den Ablauf eines Verfahrens gemäß einer bevorzugten Ausführungsform der Erfindung dar, die auch optionale Verfahrensschritte einschließt.

[0028] In Schritt 22 empfängt, etwa über eine abgesicherte Verbindung, das HSM Schlüssel, die bei der Anwendung kryptographischer Funktionen auf Daten (etwa Nachrichten an andere oder von anderen Recheneinheiten oder zu speichernde oder gespeicherte Daten) verwendet werden sollen, oder generiert diese Schlüssel selbst. Im zweiten Fall können die generierten Schlüssel außerdem, über eine abgesicherte Verbindung, zu anderen Recheneinheiten übertragen werden, da diese die generierten Schlüssel für die Implementierung einer kryptographisch abgesicherten Kommunikation gegebenenfalls ebenfalls kennen müssen. Diese anderen Recheneinheiten empfangen dann also die Schlüssel, wie in der ersten Möglichkeit von Schritt 22 genannt. Die Schlüssel können natürlich auch von einer dritten Stelle generiert werden, die an der späteren Kommunikation zwischen den Recheneinheiten nicht beteiligt ist, und dann zu Recheneinheiten über die abgesicherte Verbindung gesendet werden. Die Schlüssel können weiterhin mittels einer Zuordnungskennzeichnung, z.B. einem Index, versehen werden, so dass eine spätere Zuordnung möglich ist.

[0029] Die Zuordnungskennzeichnung kann ein einfacher Index sein (etwa eine Nummerierung oder die Nummer eines Listeneintrags, wenn die Schlüssel in einer Liste enthalten sind), anhand dessen bestimmt werden kann (z.B. über eine Zuordnungstabelle), für welche Datentypen und/oder für welche kryptographischen Funktionen und/oder für welche Kommunikationspartner der jeweilige Schlüssel verwendet werden soll. Weitergehend kann die Zuordnungskennzeichnung eine solche Verwendung direkt spezifizieren. Die Zuordnungskennzeichnung ermöglicht es also, bestimmten (zu sendenden oder empfangenen) Daten, auf die eine kryptographische Funktion angewendet werden soll, den Schlüssel bzw. verschlüsselten Schlüssel, der dafür verwendet werden soll, zuzuordnen. Es ist auch möglich, eine Zuordnungskennzeichnung nur für die verschlüsselten Schlüssel zu erzeugen.

[0030] Die in Schritt 22 empfangenen oder generierten Schlüssel werden in Schritt 24 durch das HSM verschlüsselt. Diese Verschlüsselung erfolgt unter Verwendung eines Hauptschlüssels, der vom HSM verwaltet wird, so dass andere Elemente der Recheneinheit, z.B. das Hostsystem, (oder anderer Recheneinheiten) keinen Zugriff darauf haben und nicht in Kenntnis dieses Hauptschlüssels gelangen können. Auf diese Weise werden verschlüsselte Schlüssel erhalten. Den verschlüsselten Schlüsseln kann wieder eine Zuordnungskennzeichnung (Index) zugewiesen werden, der z.B. mit der Zuordnungskennzeichnung der Schlüssel übereinstimmt oder zu diesen in eindeutiger Weise korrespondiert.

[0031] Die verschlüsselten Schlüssel werden in Schritt 26 vom HSM zum Hostsystem übertragen, welches diese in Schritt 28 empfängt und speichert. Eine etwaige Zuordnungskennzeichnung (Index) wird mit übernommen und gespeichert, so dass eine eindeutige Identifizierung der verschlüsselten Schlüssel möglich ist.

[0032] Alternativ zu den Schritten 22 bis 24 ist es auch möglich, bereits verschlüsselte Schlüssel zum HSM zu übertragen, welches diese dann entsprechend Schritt 26 zum Hostsystem überträgt. Das Hostsystem empfängt und speichert dann die verschlüsselten Schlüssel wieder entsprechend Schritt 28. Eine Zuordnungskennzeichnung (Index) der verschlüsselten Schlüssel wird dabei jeweils mit übertragen und gespeichert.

[0033] Weiter ist es alternativ zu den Schritten 22 bis 26 auch möglich, bereits verschlüsselte Schlüssel zum Hostsystem zu übertragen, welches diese dann entsprechend der Schritt 28 empfängt und speichert. Eine Zuordnungskennzeichnung (Index) der verschlüsselten Schlüssel wird dabei jeweils mit übertragen und gespeichert.

[0034] Die Schritte 22 bis 26 bilden zusammengenommen einen Bereitstellungsschritt der verschlüsselten Schlüssel in dem Hostsystem. Sie werden einmalig vor Verwendung der Schlüssel ausgeführt. Falls weitere Schlüssel benötigt werden und/oder die Schlüssel durch andere Schlüssel ersetzt werden sollen, können diese Schritte erneut durchgeführt werden.

[0035] In Schritt 30 lädt das HSM den Hauptschlüssel in das Beschleunigermodul. Dieser Schritt wird ebenfalls vor Verwendung der verschlüsselten Schlüssel ausgeführt, etwa im Rahmen einer Initialisierung nach Start der Recheneinheit.

[0036] Wenn im Hostsystem, d.h. in einem Anwendungsprogramm, das im Hostsystem ausgeführt wird, Daten vorliegen, auf die eine kryptographische Funktion angewendet werden soll, wird in Schritt 32 bestimmt, welcher der verschlüsselten Schlüssel verwendet werden soll. Wenn nicht bekannt ist, welcher der verschlüsselten Schlüssel verwendet werden soll, kann mittels der Zuordnungskennzeichnung der verschlüsselten Schlüssel festgestellt werden, welcher verschlüsselte Schlüssel den Daten zugeordnet ist und verwendet werden soll. Die Daten können z.B. eine Nachricht sein, die an eine andere Recheneinheit gesendet werden soll oder die von einer anderen Recheneinheit empfangen wurde, oder Daten, die in verschlüsselter Form gespeichert werden sollen bzw. sind, etwa in einem externen Speicher.

[0037] Prinzipiell ist es auch möglich (z.B. bei zu sendenden Daten oder bei in einem Speicher verschlüsselt zu speichernden Daten), zunächst eine beliebigen der verschlüsselten Schlüssel zu verwenden und eine entsprechende Zuordnungskennzeichnung erst anschließend zu bestimmen und gegebenenfalls zu speichern. Handelt es sich um Daten, die zu einer anderen Recheneinheit gesendet werden, muss dann der empfangenden Recheneinheit diese Zuordnungskennzeichnung mitgeteilt werden (etwa über eine gesonderte abgesicherte Verbindung).

[0038] In Schritt 34 wird der in Schritt 32 bestimmte verschlüsselte Schlüssel vom Hostsystem in das Beschleunigermodul geladen. Durch das Beschleunigermodul wird der geladene verschlüsselte Schlüssel unter Verwendung des in Schritt 30 geladenen Hauptschlüssels entschlüsselt.

[0039] In Schritt 36 werden vom Hostsystem die Daten, auf die die kryptographische Funktion angewendet werden soll, in das Beschleunigermodul geladen. Wenn das Beschleunigermodul eingerichtet ist, verschiedene kryptographisch Funktionen durchzuführen, wird dem Beschleunigermodul vom Hostsystem mitgeteilt, welche zu verwenden ist, dies kann auch erst später, spätestens vor Schritt 40, erfolgen.

[0040] Schritt 34 (Laden des verschlüsselten Schlüssels in Beschleunigermodul) und/oder Schritt 36 (Entschlüsseln des verschlüsselten Schlüssels) können, anders als dargestellt, nach und/oder gleichzeitig mit Schritt 38 (Laden der Daten) durchgeführt werden. Bevorzugt wird insbesondere Schritt 36 gleichzeitig mit Schritt 38 durchgeführt, um das Verfahren zu beschleunigen.

[0041] In Schritt 40 wird vom Beschleunigermodul die kryptographische Funktion auf die geladenen Daten unter Verwendung des in Schritt 36 entschlüsselten verschlüsselten Schlüssels angewandt, um ein entsprechendes Ergebnis zu erhalten. Die Art des Ergebnisses ist abhängig von der kryptographischen Funktion. Bei einer Verschlüsselung oder Entschlüsselung von Daten (etwa mit AES) handelt es sich um die verschlüsselten bzw. entschlüsselten Daten. Bei einem Nachrichtenauthentifizierungsverfahren (etwa CMAC) kann das Ergebnis ein Nachrichtenauthentifizierungscode sein und/oder, wenn vom Beschleunigermodul die Authentizität der Daten mittels des Nachrichtenauthentifizierungscodes geprüft wird, das Ergebnis dieser Prüfung.

[0042] Das Ergebnis des Anwendens der kryptographischen Funktion kann dann in Schritt 42 vom Hostsystem aus dem Beschleunigermodul ausgelesen werden. Anschließend kann das Ergebnis im Hostsystem, bzw. von einem im Hostsystem ausgeführten Anwendungsprogramm, verwendet werden. Z.B. kann mit entschlüsselten Daten weitergearbeitet werden oder verschlüsselte Daten können an andere Recheneinheiten gesendet oder in einem Speicher gespeichert werden. In einem Nachrichtenauthentifizierungsverfahren kann ein Nachrichtenauthentifizierungscode zusammen mit den entsprechenden Daten gesendet werden oder, falls nicht bereits im Beschleunigermodul erfolgt, empfangene Daten anhand des Nachrichtenauthentifizierungscodes auf ihre Authentizität geprüft werden. Abhängig vom Resultat einer solchen Authentizitätsprüfung, oder wenn das Ergebnis bereits ein solches Resultat ist, können empfangende Daten z.B. verwendet werden oder verworfen werden.

[0043] Nach Schritt 42 (Lesen des Ergebnisses) kann für neue Daten wieder zu Schritt 32 (Bestimmen des verschlüsselten Schlüssels) gesprungen werden (Pfeil 44) und für diese neuen Daten ausgehend davon wie vorstehend beschrieben verfahren werden.

Patentansprüche

1. Verfahren zur Anwendung kryptographischer Funktionen auf Daten unter Verwendung verschiedener Schlüssel in einer Recheneinheit, die ein Hostsystem (4), ein Hardware-Sicherheits-Modul (6) und ein Beschleunigermodul (8), das dazu einge-

richtet ist, kryptographische Funktionen durchzuführen, umfasst, umfassend
Bereitstellen (22), in dem Hostsystem (4), verschlüsselter Schlüssel, wobei die verschlüsselten Schlüssel aus den verschiedenen Schlüsseln durch Verschlüsseln mit einem Hauptschlüssel gebildet sind, der vom Hardware-Sicherheits-Modul (6) gespeichert wird;
Laden (30), durch das Hardware-Sicherheits-Modul (6), des Hauptschlüssels in das Beschleunigermodul (8);
wobei beim Anwenden einer kryptographischen Funktion auf Daten jeweils durchgeführt wird:
Laden (34), durch das Hostsystem (4), eines den Daten zugeordneten verschlüsselten Schlüssels in das Beschleunigermodul (8);
Entschlüssen (36), durch das Beschleunigermodul (8), des verschlüsselten Schlüssels mit dem Hauptschlüssel;
Laden (38), durch das Hostsystem (4), der Daten in das Beschleunigermodul (8);
Anwenden (40), durch das Beschleunigermodul (8), der kryptographischen Funktion auf die Daten unter Verwendung des entschlüsselten Schlüssels, um ein entsprechendes Ergebnis zu erhalten; und
Lesen (42), durch das Hostsystem (4), des Ergebnisses aus dem Beschleunigermodul (8).

2. Verfahren nach Anspruch 1, wobei der Schritt des Bereitstellens der verschlüsselten Schlüssel ein Verschlüsseln (24), durch das Hardware-Sicherheits-Modul (6), eines oder mehrerer der verschiedenen Schlüssel unter Verwendung des Hauptschlüssels und ein Übertragen (26), durch das Hardware-Sicherheits-Modul (6), der verschlüsselten Schlüssel an das Hostsystem (4) umfasst.

3. Verfahren nach Anspruch 2, wobei der eine oder die mehreren der verschiedenen Schlüssel von dem Hardware-Sicherheits-Modul (6) generiert werden (22) oder von dem Hardware-Sicherheits--Modul (6) über eine verschlüsselte Kommunikation empfangen werden (22).

4. Verfahren nach einem der vorstehenden Ansprüche, weiterhin umfassend Bestimmen (32), durch das Hostsystem (4), des den Daten zugeordneten verschlüsselten Schlüssels.

5. Verfahren nach Anspruch 4, wobei Zuordnungskennzeichnungen für die verschlüsselten Schlüssel vorgesehen sind, auf Grundlage derer der den Daten zugeordnete verschlüsselte Schlüssel bestimmt wird.

6. Verfahren nach einem der vorstehenden Ansprüche, wobei die kryptographischen Funktionen eines oder mehreres umfassen von: einem symmetrischen Verschlüsselungsverfahren, insbesondere Verschlüsselung und/oder Entschlüsselung von Botschaften, und einem Nachrichtenauthentifizierungsverfahren, insbesondere Berechnung eines Nachrichtenauthentifizierungscodes.

7. Recheneinheit (2), die dazu eingerichtet ist, alle Verfahrensschritte eines Verfahrens nach einem der vorstehenden Ansprüche durchzuführen.

8. Computerprogramm, das eine Recheneinheit dazu veranlasst, alle Verfahrensschritte eines Verfahrens nach einem der Ansprüche 1 bis 6 durchzuführen, wenn es auf der Recheneinheit ausgeführt wird.

9. Maschinenlesbares Speichermedium mit einem darauf gespeicherten Computerprogramm nach Anspruch 8.

Es folgen 2 Seiten Zeichnungen

Anhängende Zeichnungen

Fig. 1

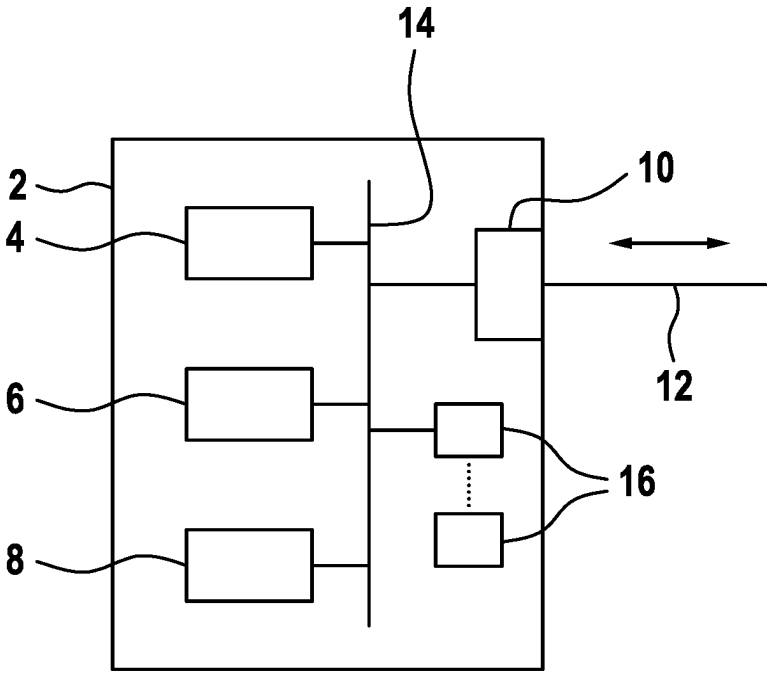
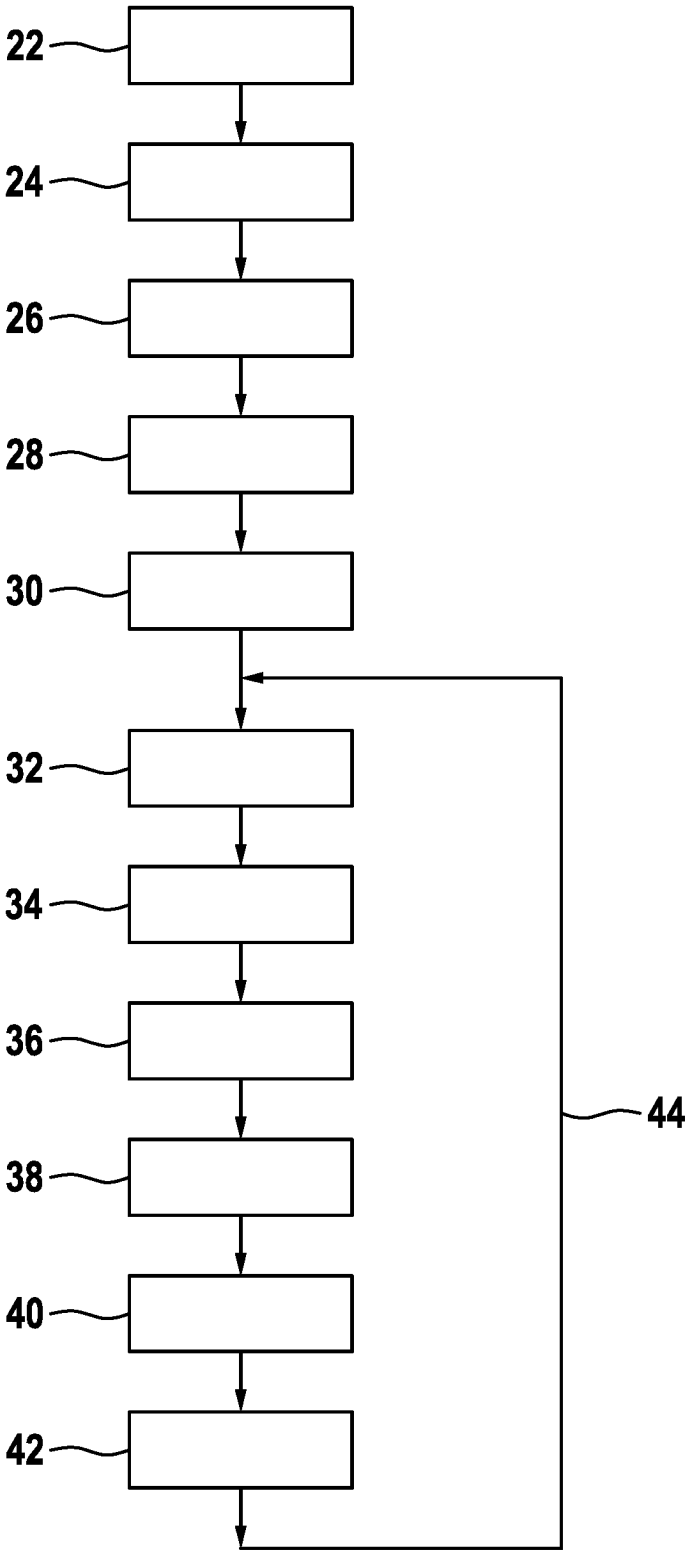


Fig. 2



 Das Dokument wurde durch die Firma Luminess hergestellt.