(19) Deutsches Patent- und Markenamt

(10) **DE 10 2016 112 552 A1** 2017.01.12

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2016 112 552.0**
(22) Anmeldetag: **08.07.2016**
(43) Offenlegungstag: **12.01.2017**

(51) Int Cl.: ***H04L 9/00*** (2006.01)
H04L 9/32 (2006.01)
H04L 9/12 (2006.01)

(30) Unionspriorität:
14/796,892 **10.07.2015** **US**

(71) Anmelder:
Infineon Technologies AG, 85579 Neubiberg, DE

(74) Vertreter:
Kraus & Weisert Patentanwälte PartGmbB, 80539 München, DE

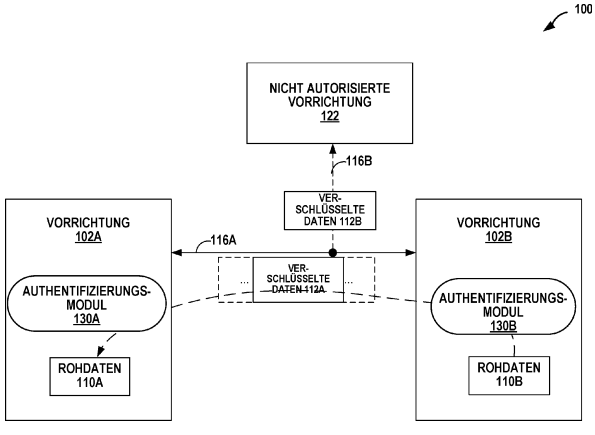
(72) Erfinder:
Lim, Cheow Guan, Singapur, SG

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Datenchiffrierung und -dechiffrierung auf der Grundlage einer Vorrichtungs- und Datenauthentifizierung**

(57) Zusammenfassung: Es wird eine Vorrichtung beschrieben, welche einen Sitzungsschlüssel zum Erzeugen eines Nachrichtenauthentifierungscode(MAC)-Tags in Zusammenhang mit einer Kommunikationssitzung zwischen der Vorrichtung und einer zweiten Vorrichtung bestimmt. Die Vorrichtung bestimmt zumindest teilweise auf der Grundlage des Sitzungsschlüssels einen kryptographischen Schlüssel zum Codieren oder Entschlüsseln einer Nachricht in Zusammenhang mit der zweiten Vorrichtung. Die Vorrichtung codiert oder decodiert die Nachricht dann auf der Grundlage des kryptographischen Schlüssels.



Beschreibung

Hintergrund

[0001] Einige Vorrichtungen führen Schritte zum Gewährleisten der Integrität der von einer anderen Vorrichtung empfangenen Daten sowie der Authentizität der Daten aus, indem sie Nachrichtenauthentifizierungscode-(MAC, vom Englischen „Message Authentification Code“)-Techniken in der Art der im US-Patent 8 630 411 von Lim u.a. beschriebenen Techniken ausführen. MAC-Techniken können es einer Empfängervorrichtung ermöglichen, ein Aufforderung-Antwort-Protokoll ("Challenge-Response Protocol") für das Authentifizieren einer Quellvorrichtung und für das Bestätigen, dass die von der Quellvorrichtung empfangenen Daten nicht manipuliert oder auf andere Weise gegenüber ihrer ursprünglichen Form geändert wurden, zu implementieren.

[0002] In manchen Fällen können die von einer authentifizierten Quelle empfangenen Daten wertvolle und/oder sensitive Informationen aufweisen (beispielsweise Passwörter, proprietäre Geheimnisse, persönliche Informationen oder andere sensitive Informationen). Auch wenn MAC-Techniken eine Empfängervorrichtung in die Lage versetzen können, die Datenintegrität zu gewährleisten, können MAC-Techniken nichts unternehmen, um die tatsächlich übertragenen Daten vor einem Abfangen durch eine nicht autorisierte Vorrichtung zu schützen. Dabei können die Daten für einen Angriff durch nicht autorisierte Schnüffelvorrichtungen anfällig sein, welche den Datenaustausch in einem Versuch ausspionieren oder auf andere Weise belauschen, Zugang zu den beim Austausch geteilten wertvollen und/oder sensitiven Informationen zu erhalten.

[0003] Um vor einem unerlaubten Ausspionieren zu schützen, können einige Vorrichtungen komplexe kryptographische Algorithmen ausführen und komplizierte Operationen durchführen, um Daten vor der Übertragung zu codieren und die Daten beim Empfang zu Entschlüsseln. Das Ausführen komplexer kryptographischer Algorithmen für das Codieren und Entschlüsseln von Daten kann für einige kostengünstige oder weniger komplizierte Systeme zu komplex oder zu kostspielig sein.

[0004] Es ist eine Aufgabe, verbesserte Möglichkeiten hierfür bereitzustellen.

Kurzfassung

[0005] Es werden ein Verfahren nach Anspruch 1, eine erste Vorrichtung nach Anspruch 18 sowie ein System nach Anspruch 22 bereitgestellt. Die Unteransprüche definieren weitere Ausführungsformen. Der Begriff „Codieren“ wird im Rahmen dieser Anmeldung als Oberbegriff für Verschlüsseln (manchmal auch als Codieren bezeichnet) und/oder Entschlüsseln (Decodieren) verwendet.

[0006] Bei einem Beispiel betrifft die Offenbarung ein Verfahren, das Folgendes aufweist: Bestimmen, durch eine erste Vorrichtung, eines Sitzungsschlüssels zum Erzeugen eines Nachrichtenauthentifierungscode(MAC)-Tags in Zusammenhang mit einer Kommunikationssitzung zwischen der ersten Vorrichtung und einer zweiten Vorrichtung, Bestimmen eines kryptographischen Schlüssels zum Codieren einer Nachricht in Zusammenhang mit der zweiten Vorrichtung zumindest teilweise auf der Grundlage des Sitzungsschlüssels durch die erste Vorrichtung und Codieren der Nachricht auf der Grundlage des kryptographischen Schlüssels durch die erste Vorrichtung.

[0007] Bei einem anderen Beispiel betrifft die Offenbarung eine erste Vorrichtung, die wenigstens einen Prozessor aufweist, der in der Lage ist, Folgendes auszuführen: Bestimmen eines Sitzungsschlüssels zum Erzeugen eines Nachrichtenauthentifierungscode(MAC)-Tags in Zusammenhang mit einer Kommunikationssitzung zwischen der ersten Vorrichtung und einer zweiten Vorrichtung, Bestimmen eines kryptographischen Schlüssels zum Codieren oder Entschlüsseln einer Nachricht in Zusammenhang mit der zweiten Vorrichtung zumindest teilweise auf der Grundlage des Sitzungsschlüssels und Codieren der Nachricht auf der Grundlage des kryptographischen Schlüssels.

[0008] Bei einem anderen Beispiel betrifft die Offenbarung ein System, welches Folgendes aufweist: Mittel zum Bestimmen eines Sitzungsschlüssels, um ein Nachrichtenauthentifierungscode(MAC)-Tag in Zusammenhang mit einer Kommunikationssitzung zwischen einer ersten Vorrichtung und einer zweiten Vorrichtung zu erzeugen, Mittel zum Bestimmen eines kryptographischen Schlüssels zum Codieren oder Entschlüsseln einer Nachricht in Zusammenhang mit der zweiten Vorrichtung zumindest teilweise auf der Grundlage des Sitzungsschlüssels und Mittel zum Codieren der Nachricht auf der Grundlage des kryptographischen Schlüssels.

[0009] Die Einzelheiten eines oder mehrerer Beispiele sind in der anliegenden Zeichnung und der nachstehenden Beschreibung dargelegt. Andere Merkmale, Aufgaben und Vorteile der Offenbarung werden anhand der Beschreibung und der Zeichnung sowie der Ansprüche verständlich werden.

Kurzbeschreibung der Zeichnung

[0010] Es zeigen:

[0011] Fig. 1 ein Konzeptdiagramm eines Beispielsystems zum Austauschen codierter Daten zwischen

zwei authentifizierten Vorrichtungen gemäß Techniken dieser Offenbarung,

[0012] Fig. 2 ein Konzeptdiagramm eines zusätzlichen Beispielsystems zum Austauschen codierter Daten zwischen zwei authentifizierten Vorrichtungen gemäß Techniken dieser Offenbarung,

[0013] die **Fig.** 3A und **Fig.** 3B Flussdiagramme von Beispieloperationen, die von Beispielvorrichtungen ausgeführt werden, um Daten zu codieren, gemäß einem oder mehreren Aspekten der vorliegenden Offenbarung,

[0014] Fig. 4 ein Konzeptdiagramm eines Beispieldatenstroms, der zwischen zwei authentifizierten Vorrichtungen übertragen wird, gemäß einem oder mehreren Aspekten der vorliegenden Offenbarung,

[0015] Fig. 5 ein Konzeptdiagramm eines zusätzlichen Beispielsystems zum Austauschen codierter Daten zwischen einer einzigen Host-Vorrichtung und zwei getrennten Slave-Vorrichtungen gemäß Techniken dieser Offenbarung,

[0016] Fig. 6 ein Konzeptdiagramm eines Authentifizierungsablaufs zum Austauschen codierter Daten zwischen zwei authentifizierten Vorrichtungen gemäß Techniken dieser Offenbarung,

[0017] Fig. 7 ein Konzeptdiagramm eines zusätzlichen Beispielsystems zum Austauschen codierter Daten zwischen zwei authentifizierten Vorrichtungen gemäß Techniken dieser Offenbarung,

[0018] Fig. 8 ein Konzeptdiagramm eines Beispielpseudocodes zur Ausführung durch eine der beiden authentifizierten Vorrichtungen des Beispielsystems aus **Fig.** 7 zur Ausführung von Operationen für das Codieren von Daten gemäß einem oder mehreren Aspekten der vorliegenden Offenbarung und

[0019] Fig. 9 ein Flussdiagramm von Beispieloperationen, die von einer der beiden authentifizierten Vorrichtungen des Beispielsystems aus **Fig.** 7 ausgeführt werden, wenn der Beispielpseudocode aus **Fig.** 8 ausgeführt wird, gemäß einem oder mehreren Aspekten der vorliegenden Offenbarung.

Detaillierte Beschreibung

[0020] Es werden allgemein Schaltungen und Techniken beschrieben, die dazu dienen, Vorrichtungen in die Lage zu versetzen, Informationen zu codieren, die zwischen Vorrichtungen ausgetauscht werden, welche Nachrichtenauthentifizierungscode-(MAC)-Techniken verwenden, um die Integrität und Authentizität der Informationen zu überprüfen, ohne dass eine Vorrichtung zum Vorspeichern oder Austauschen eines Passworts oder eines Entschlüsselungsschlüssels erforderlich wäre. Beispielsweise können als ein Weg zum Gewährleisten der Datenintegrität eine erste Vorrichtung und eine zweite Vorrichtung ein Aufforderung-Antwort-Protokoll ("Challenge-Response Protocol") gemäß den im US-Patent 8 630 411 von Lim u.a. beschriebenen Techniken implementieren.

[0021] Als Teil des Implementierens des Aufforderung-Antwort-Protokolls können die erste Vorrichtung und die zweite Vorrichtung jeweils einen Sitzungsschlüssel ableiten, welcher der ersten und der zweiten Vorrichtung gemeinsam ist, jedoch nie tatsächlich über die Kommunikationsleitung geteilt wird. Wenn Daten von der ersten Vorrichtung empfangen werden, kann die zweite Vorrichtung die erste Vorrichtung durch Eingeben des Sitzungsschlüssels in einen MAC-Algorithmus authentifizieren, um eine Instanz eines MAC-Tags abzuleiten. Die zweite Vorrichtung kann das abgeleitete MAC-Tag mit einem zusammen mit der Datenübertragung von der ersten Vorrichtung empfangenen MAC-Tag vergleichen. Falls das abgeleitete und das empfangene MAC-Tag übereinstimmen, kann die zweite Vorrichtung die erste Vorrichtung "authentifizieren" (beispielsweise die Identität der ersten Vorrichtung bestätigen) und die Integrität der empfangenen Daten verifizieren (beispielsweise bestätigen, dass die Daten während der Übertragung nicht geändert wurden).

[0022] Um die von zwei authentifizierten Vorrichtungen ausgetauschten Daten zu codieren und vor einem unerlaubten Ausspionieren (beispielsweise durch eine dritte Partei oder eine auf andere Weise nicht autorisierte Vorrichtung) zu schützen, können die erste und die zweite Vorrichtung über das Ausführen von Authentifizierungs- und Datenintegritätsoperationen hinausgehen und die abgeleiteten Sitzungsschlüssel verwenden, um die Daten vor und nach der Übertragung zu codieren und zu entschlüsseln. Beispielsweise kann die erste Vorrichtung vor der Übertragung zur zweiten Vorrichtung die Daten unter Verwendung des abgeleiteten Sitzungsschlüssels als "Chiffrierungs-" oder "Verschlüsselungsschlüssel" codieren, um die Daten zu verwürfeln und einen nicht autorisierten Zugang zu verhindern. Bei einigen Beispielen kann die erste Vorrichtung Daten vor der Übertragung codieren, indem sie eine "Exklusiv-ODER"-(auch als "XOR"- oder "exklusive Disjunktion" bezeichnet)-Operation zwischen dem abgeleiteten Sitzungsschlüssel und den Daten ausführt. Nach dem Empfang der Daten kann die zweite Vorrichtung die Daten dann unter Verwendung des abgeleiteten Sitzungsschlüssels als "Dechiffrierungs-" oder "Entschlüsselungsschlüssel" entschlüsseln, um die Daten zu entwürfeln. Bei einigen Beispielen kann die zweite Vorrichtung die Daten nach dem Empfang durch Ausführen einer Exklusiv-ODER-Operation zwischen den codierten Daten und dem abge-

leiteten Sitzungsschlüssel entschlüsseln, um die ursprünglichen, uncodierten Daten zu erhalten.

[0023] **Fig.** 1 ist ein Konzeptdiagramm, welches ein System **100** als ein Beispielsystem zum Austauschen codierter Daten zwischen zwei authentifizierten Vorrichtungen **102A** und **102B** gemäß Techniken dieser Offenbarung zeigt. Das System **100** weist eine Vorrichtung **102A** und eine Vorrichtung **102B** (gemeinsam "Vorrichtungen **102**") auf, die dafür ausgelegt sind, Informationen (beispielsweise Daten) über einen Kommunikationskanal oder eine "Verbindung" **116A** auszutauschen. Das System **100** weist auch eine nicht autorisierte Vorrichtung **122** auf, die dafür ausgelegt ist, über eine Verbindung **116B** die über die Verbindung **116A** ausgetauschten Daten abzufangen.

[0024] Die nicht autorisierte Vorrichtung **122** repräsentiert einen beliebigen Vorrichtungstyp, der dafür ausgelegt ist, Informationen, die über einen Datenweg ausgetauscht werden, zu erschnüffeln, auszuspionieren oder auf andere Weise abzufangen. Beispiele einer nicht autorisierten Vorrichtung **122** umfassen Rechenvorrichtungen, Rechensysteme, Netzvorrichtungen oder einen anderen Typ einer Vorrichtung, welche Daten lesen kann, die zwischen Vorrichtungen über einen Datenweg übertragen werden. Beim Beispiel aus **Fig.** 1 kann die nicht autorisierte Vorrichtung **122** über die Verbindung **116B** eine Kopie der Informationen oder Daten empfangen, welche über die Verbindung **116A** zwischen den Vorrichtungen **102** übertragen werden. In Fällen, in denen die über die Verbindung **116A** übertragenen Daten uncodiert sind, kann die nicht autorisierte Vorrichtung **122** die Informationen interpretieren, welche in den über die Verbindung **116B** empfangenen Daten codiert sind. Umgekehrt kann die nicht autorisierte Vorrichtung **122** in Fällen, in denen die über die Verbindung **116A** übertragenen Daten codiert sind, nicht in der Lage sein, die Informationen zu interpretieren, die in den über die Verbindung **116B** empfangenen Daten codiert sind (beispielsweise zumindest ohne Ausführen zusätzlicher Operationen zum Entschlüsseln der Daten).

[0025] Die Vorrichtungen **102** repräsentieren einen Typ von Vorrichtungen, die dafür ausgelegt sind, Informationen über einen Datenweg auszutauschen. Beispielsweise können die Vorrichtungen **102** eine beliebige Kombination mobiler Rechenvorrichtungen, tragbarer Rechenvorrichtungen, persönlicher digitaler Assistenten (PDA), Kameras, Audioabspielgeräte, Spielsysteme oder -konsolen, Audio- und/oder Videosysteme, anderer Unterhaltungsvorrichtungen, Desktop- oder Laptopcomputer, Computersysteme, Netz- oder Rechenvorrichtungen, Kopiergeräte, Scanner, All-in-one- oder anderer digitaler Bildgebungs- oder Wiedergabevorrichtungen, medizinischer Vorrichtungen oder Geräte oder diagnostischer Versorgungen, Automobil- oder Kraftfahrzeugsysteme, Luftfahrzeuge (sowohl bemannter als auch nicht bemannter Luftfahrzeuge) oder Luftfahrzeugsysteme, Seefahrzeuge oder Seesysteme, Luftraum- und Militärfahrzeuge oder Luftraum- und Militärsysteme, industrieller Komponenten oder industrieller Systeme oder eines anderen Teils, Zusatzgeräts oder einer anderen Komponente oder Batterie, Zusatzvorrichtungen, Kopfhörervorrichtungen, Headset-Vorrichtungen, Lautsprechervorrichtungen, Docking-Stations, Spielsteuervorrichtungen, Ladevorrichtungen, Mikrofonvorrichtungen, Tonerkassettenvorrichtungen, Magazinvorrichtungen, einer Netzvorrichtung, Peripherievorrichtungen, innerer oder äußerer Speichervorrichtungen oder anderer Vorrichtungen oder Komponenten, für die eine Authentifizierung und sichere Datenübertragung erforderlich ist, einschließen.

[0026] Die Vorrichtung **102A** weist ein Authentifizierungsmodul **130A** auf, und die Vorrichtung **102B** weist ein Authentifizierungsmodul **130B** auf. Die Authentifizierungsmodule **130A** und **130B** (gemeinsam "Authentifizierungsmodule **130**") ermöglichen es, dass die Vorrichtungen **102** ein Aufforderung-Antwort-Protokoll für authentifizierende Vorrichtungen **102** ausführen und die Integrität der über die Verbindung **116A** ausgetauschten Daten gewährleisten, und sie können ferner einen von der Ausführung des Aufforderung-Antwort-Protokolls abgeleiteten Sitzungsschlüssel verwenden, um die über die Verbindung **116A** ausgetauschten Daten zu codieren und zu entschlüsseln (beispielsweise um ein Eindringen durch eine nicht autorisierte Vorrichtung **122** zu verhindern).

[0027] Authentifizierungsmodule **130** können eine geeignete Anordnung von Hardware, Software, Firmware oder eine beliebige Kombination davon umfassen, um die Authentifizierungsmodulen **130** zugeschriebenen Techniken auszuführen, die hier beschrieben werden. Beispielsweise können die Authentifizierungsmodule **130** jeweils einen oder mehrere Mikroprozessoren, digitale Signalprozessoren (DSP), anwendungsspezifische integrierte Schaltkreise (ASIC), feldprogrammierbare Gate-Arrays (FPGA) oder eine andere äquivalente integrierte oder diskrete Logikschaltungsanordnung sowie beliebige Kombinationen solcher Komponenten aufweisen. Wenn die Authentifizierungsmodule **130** Software oder Firmware aufweisen, weisen die Authentifizierungsmodule **130** ferner erforderliche Hardware zum Speichern und Ausführen der Software oder Firmware in der Art eines oder mehrerer Prozessoren oder Verarbeitungseinheiten auf.

[0028] Im Allgemeinen kann eine Verarbeitungseinheit einen oder mehrere Mikroprozessoren, DSP, ASIC, FPGA oder eine andere gleichwertige integrierte oder diskrete Logikschaltungsanordnung so-

wie beliebige Kombinationen solcher Komponenten aufweisen. Wenngleich dies in **Fig.** 1 nicht dargestellt ist, können die Authentifizierungsmodule **130** einen Speicher aufweisen, der dafür ausgelegt ist, Daten zu speichern. Der Speicher kann beliebige flüchtige oder nicht flüchtige Medien in der Art eines Direktzugriffsspeichers (RAM), Nurlesespeichers (ROM), nicht flüchtigen RAM (NVRAM), elektrisch löschbaren, programmierbaren ROM (EEPROM), Flash-Speichers und dergleichen einschließen. Bei einigen Beispielen kann sich der Speicher außerhalb von Authentifizierungsmodulen **130** befinden, beispielsweise außerhalb einer Baugruppe, worin die Authentifizierungsmodule **130** aufgenommen sind.

[0029] Beim Betrieb können die Authentifizierungsmodule **130A** und **130B**, wie im US-Patent 8 630 411 von Lim u.a. beschrieben ist, gemeinsam ein Aufforderung-Antwort-Protokoll zum Authentifizieren von Vorrichtungen **102** und zum Gewährleisten der Integrität der über die Verbindung **116A** ausgetauschten Daten implementieren. Beispielsweise kann die Vorrichtung **102B** während einer bestimmten Kommunikationssitzung Daten über die Verbindung **116A** zur Vorrichtung **102A** senden. Damit die Vorrichtung **102A** verifizieren kann, dass die über die Verbindung **116A** empfangenen Daten ungeändert angekommen sind und tatsächlich von der Vorrichtung **102B** ausgegangen sind, kann das Authentifizierungsmodul **130B** der Vorrichtung **102B** eine erste Instanz eines Sitzungsschlüssels für die bestimmte Kommunikationssitzung zwischen den Vorrichtungen **102** ableiten. Die erste Instanz des Sitzungsschlüssels kann für jede Kommunikationssitzung (beispielsweise periodisch usw.) vom Authentifizierungsmodul **130B** wiederhergestellt werden.

[0030] Auf der Grundlage der abgeleiteten ersten Instanz des Sitzungsschlüssels kann das Authentifizierungsmodul **130B** dann ein erstes Nachrichtenauthentifierungscode(MAC)-Tag für die bestimmte Kommunikationssitzung erzeugen und das erste MAC-Tag in die Daten aufnehmen, welche die Vorrichtung **102A** an die Verbindung **116A** ausgibt. Beispielsweise kann das Authentifizierungsmodul **130B** den Sitzungsschlüssel in die MAC-Funktion eingeben, welche ein erstes MAC-Tag ausgibt, welches das Authentifizierungsmodul **130B** dann verwendet, um die Daten vor der Übertragung zu markieren.

[0031] Nach dem Empfang von Daten von der Verbindung **116A** kann das Authentifizierungsmodul **130A** der Vorrichtung **102A** das erste MAC-Tag mit den über die Verbindung **116A** empfangenen Daten analysieren, um zu bestimmen, ob die Vorrichtung **102B** die Daten tatsächlich übertragen hat, und ferner, ob die Daten gegenüber ihrer ursprünglichen Form ungeändert sind. Beispielsweise kann das Authentifizierungsmodul **130A** der Vorrichtung **102A** eine zweite Instanz des Sitzungsschlüssels für die bestimmte Kommunikationssitzung zwischen den Vorrichtungen **102** ableiten. Die zweite Instanz des Sitzungsschlüssels kann für jede Kommunikationssitzung (beispielsweise periodisch usw.) vom Authentifizierungsmodul **130A** wiederhergestellt werden.

[0032] Bei einigen Beispielen können die ersten und zweiten Instanzen der Sitzungsschlüssel auf der Grundlage der zwischen Vorrichtungen übertragenen Datenmenge wiederhergestellt werden. Beispielsweise können die ersten und zweiten Instanzen der Sitzungsschlüssel von den Vorrichtungen **102** wiederhergestellt werden, nachdem eine bestimmte Byteanzahl (beispielsweise 1024 Bytes oder eine andere Datenanzahl) über die Verbindung **116** gelaufen ist. Bei anderen Beispielen verwenden die Vorrichtungen **102** die Zeit als eine Variable zum Bestimmen, wann aktualisierte Sitzungsschlüssel abzuleiten sind. Beispielsweise können die Vorrichtungen **102** aktualisierte Sitzungsschlüssel bestimmen, nachdem ein bestimmter Zeitraum (beispielsweise eine Sekunde, eine Stunde oder ein anderes Zeitinkrement) verstrichen ist, seit die Sitzungsschlüssel zuletzt abgeleitet wurden.

[0033] Auf der Grundlage der abgeleiteten zweiten Instanz des Sitzungsschlüssels kann das Authentifizierungsmodul **130A** dann ein zweites MAC-Tag für die bestimmte Kommunikationssitzung erzeugen und bestimmen, ob das zweite MAC-Tag, welches das Authentifizierungsmodul **130A** erzeugt, mit dem ersten MAC-Tag übereinstimmt, das in den über die Verbindung **116A** empfangenen Daten empfangen wurde. Beispielsweise kann das Authentifizierungsmodul **130A** den Sitzungsschlüssel in eine MAC-Funktion eingeben, welche ein zweites MAC-Tag ausgibt, welches das Authentifizierungsmodul **130A** dann verwendet, um zu verifizieren, ob die über die Verbindung **116A** empfangenen Daten authentisch sind oder nicht. Das Authentifizierungsmodul **130A** kann bestimmen, dass die über die Verbindung **116A** empfangenen Daten authentisch sind, wenn das vom Authentifizierungsmodul **130A** erzeugte zweite MAC-Tag mit dem innerhalb der empfangenen Daten empfangenen ersten MAC-Tag übereinstimmt.

[0034] Zum Verhindern eines Ausspionierens der in den über die Verbindung **116A** ausgetauschten Daten enthaltenen Informationen können die Authentifizierungsmodule **130A** und **130B** die Daten vor der Übertragung und anschließend an den Empfang codieren und entschlüsseln. Anders als einige Vorrichtungen, welche vor einem unerlaubten Ausspionieren schützen, indem sie komplexe kryptographische Algorithmen und komplizierte Operationen zum Codieren und Entschlüsseln von Daten ausführen, leiten die Authentifizierungsmodule **130A** und **130B** kryptographische Schlüssel jedoch auf der Grundlage derselben bereits für Authentifizierungszwecke erzeugten Sitzungsschlüssel für das Codieren und

Entschlüsseln der Daten ab. Mit anderen Worten verwenden die Authentifizierungsmodule **130A** und **130B** die abgeleiteten Sitzungsschlüssel mit oder ohne Ausführen geringer Variationen wieder, um kryptographische Schlüssel für das Chiffrieren von Daten vor der Übertragung und das Dechiffrieren von Daten nach dem Empfang zu erzeugen. Bei einigen Beispielen können die Authentifizierungsmodule **130A** und **130B** einen getrennten Satz abgeleiteter Sitzungsschlüssel, die nicht für die MAC-Tag-Verwendung vorgesehen sind, wiederherstellen. In anderen Fällen leiten die Authentifizierungsmodule **130A** und **130B** zweite Sitzungsschlüssel ab und verwenden sie zusammen mit den vorhergehenden Sitzungsschlüsseln. Die zweiten Sitzungsschlüssel werden für das Chiffrieren der Daten vor der Übertragung und für das Dechiffrieren von Daten nach dem Empfang verwendet. Das MAC-Tag kann vor oder nach dem Chiffrieren oder Dechiffrieren der Daten ausgeführt werden. In anderen Fällen können weitere Sitzungsschlüsselpaare für Daten mit Chiffrierung und Dechiffrierung mit vielen Schlüsseln präpariert werden.

[0035] Beispielsweise kann das Authentifizierungsmodul **130B** codierte Daten **112A** zur Übertragung zur Vorrichtung **102A** durch Ausführen einer Exklusiv-ODER-Operation (oder einer anderen Chiffriertechnik) zwischen Rohdaten **110B** und einem kryptographischen Schlüssel erzeugen, welcher demselben Sitzungsschlüssel entspricht oder zumindest darauf beruht, welchen das Authentifizierungsmodul **130B** für die Erzeugung des ersten MAC abgeleitet hat, das für die bestimmte Kommunikationssitzung verwendet wird. Bei anderen Beispielen repräsentiert der kryptographische Schlüssel einen Hash-Wert des Sitzungsschlüssels und eines Startwerts (beispielsweise einer Zufallszahl, einer Zahl auf der Grundlage der Tageszeit usw.), der zwischen den Vorrichtungen **102** geteilt wird.

[0036] Bei einigen Beispielen codiert das Authentifizierungsmodul **130B** sowohl Rohdaten **110B** als auch den zugehörigen MAC, um codierte Daten **112A** zu erzeugen. Bei anderen Beispielen codiert das Authentifizierungsmodul **130B** lediglich Rohdaten **110B**, um codierte Daten **112A** zu erzeugen.

[0037] In jedem Fall gibt die Vorrichtung **102B** codierte Daten **112A** an Stelle von Rohdaten **110B** an die Verbindung **116A** aus. Weil codierte Daten **112A** eine verwürfelte Version der Rohdaten **110B** sind, kann die nicht autorisierte Vorrichtung **122** nicht in der Lage sein, die innerhalb der codierten Daten **112A** enthaltenen Informationen zu interpretieren.

[0038] Das Authentifizierungsmodul **130A** kann über die Verbindung **116B** empfangene codierte Daten **112A** durch Ausführen einer Exklusiv-ODER-Operation (oder einer anderen Dechiffriertechnik, welche die vom Authentifizierungsmodul **130B** ausgeführte Chiffrierung umkehrt) zwischen codierten Daten **112A** und dem kryptographischen Schlüssel in Rohdaten **110A** entwürfeln, wobei der kryptographische Schlüssel demselben Sitzungsschlüssel entspricht oder zumindest darauf beruht, welchen das Authentifizierungsmodul **130A** für den zweiten MAC abgeleitet hat, welcher für die bestimmte Kommunikationssitzung verwendet wird. Bei anderen Beispielen repräsentiert der kryptographische Schlüssel einen Hash-Wert des Sitzungsschlüssels und eines Startwerts (beispielsweise einer Zufallszahl, einer Zahl auf der Grundlage der Tageszeit usw.), der zwischen den Vorrichtungen **102** geteilt wird. Das Authentifizierungsmodul **130A** kann die entwürfelte Version der an der Vorrichtung **102A** codierten Daten **112A** als Rohdaten **110A** speichern.

[0039] Auf diese Weise können Vorrichtungen, welche Daten nach den hier beschriebenen Techniken codieren und entschlüsseln, vor einem unerlaubten Ausspionieren schützen, ohne komplexe kryptographische Algorithmen ausführen zu müssen oder komplizierte Operationen für das Codieren von Daten vor der Übertragung und das Entschlüsseln der Daten beim Empfang auszuführen. Durch Erzeugen kryptographischer Schlüssel für das Codieren und Entschlüsseln von Daten zumindest teilweise auf der Grundlage von Sitzungsschlüsseln, die bereits für Authentifizierungszwecke abgeleitet wurden, können die in dieser Offenbarung beschriebenen Techniken kostengünstige oder weniger komplizierte Systeme ermöglichen, welche Informationen austauschen, ohne dass sie für ein Ausspionieren anfällig sind.

[0040] Bei einigen Beispielen können die Vorrichtungen **102** Teil einer unbemannten Luftfahrzeuganwendung sein. Beispielsweise kann die Vorrichtung **102A** ein unbemanntes Luftfahrzeug sein und kann die Vorrichtung **102B** eine Steuereinrichtung oder eine Bodenstation zum Steuern des unbemannten Luftfahrzeugs sein. Die Vorrichtung **102B** kann Steuerbefehle senden, welche diese Vorrichtung **102A** verwendet, um einen Gleitweg zu einem Zielort zu fliegen. Durch Chiffrieren und Dechiffrieren der Steuerbefehle vor und nach der Übertragung können die Vorrichtungen **102** gewährleisten, dass die Steuerbefehle die Operationen anderer unbemannter Luftfahrzeuge im Gebiet nicht stören. Bei anderen Beispielen können die zwischen dem unbemannten Luftfahrzeug **102A** und der Steuereinrichtung **102B** geteilten Informationen Daten aufweisen, welche Aufnahme- und Abladestellen für vom unbemannten Luftfahrzeug **102A** ausgelieferte Waren angeben. Bei anderen Beispielen können die Informationen Daten aufweisen, welche die Steueroperationen oder das Umleiten oder das Stornieren der Lieferung der Waren angeben.

[0041] Bei einigen Beispielen kann die Vorrichtung **102A** ein Sender sein, der einem Absender der Waren zugeordnet ist, welcher ein unbemanntes Luftfahrzeug verwendet, und kann die Vorrichtung **102B** ein Empfänger sein, welcher einer Empfangsstelle der Waren zugeordnet ist, welche durch das unbemannte Luftfahrzeug ausgeliefert werden. Das unbemannte Luftfahrzeug kann ein passwortgeschütztes oder Sperrabteil aufweisen, das die Waren aufweist. Unter Verwendung der hier beschriebenen Techniken können die Absender der Waren das Passwort zum Entsperren des Abteils unter Verwendung der Vorrichtung **102A** übertragen und kann die Empfangsstelle das Passwort unter Verwendung der Vorrichtung **102B** dechiffrieren, wenn das unbemannte Luftfahrzeug an seinem Ort landet.

[0042] Es existieren viele andere Anwendungen für die Vorrichtungen **102**. Beispielsweise können die Vorrichtungen **102** bei anderen Beispielen Teil eines Authentifizierungsprozesses zwischen einer Rechenvorrichtung und einer Austauschkomponente oder einem Austauschgerät in der Art einer Batterie sein. Unter Verwendung der beschriebenen Techniken können die Rechenvorrichtung und die Batterie verwürfelte Daten austauschen, um die Authentizität der Batterie zu prüfen, und kann ein Benutzer der Rechenvorrichtung den Authentifizierungsprozess nicht stören (beispielsweise um die Rechenvorrichtung dazu zu verführen, dass sie denkt, dass die Batterie echt ist, selbst wenn die Batterie tatsächlich eine gefälschte und möglicherweise gefährliche Komponente sein kann).

[0043] Bei einigen anderen Beispielen können die Vorrichtungen **102** Teil einer Anwendung zum Schützen eines zum Herunterladen (beispielsweise vom Internet) verfügbaren proprietären Quellcodes einer Firma sein. Beispielsweise kann ein gewisser Quellcode nur für das Herunterladen verfügbar sein, nachdem ein Benutzer seine Identität bei der Firma registriert hat. Zum Schützen der Identität des Benutzers können die hier beschriebenen Verschlüsselungs- und Entschlüsselungstechniken der Firma ermöglichen, die Benutzeridentität vertraulich zu halten. Zusätzlich kann die Firma vor dem Herunterladen den Code mit einem MAC-Tag markieren, welches es dem Benutzer an seiner Vorrichtung ermöglicht, die Authentizität des Codes nach dem Herunterladen zu verifizieren (beispielsweise um zu gewährleisten, dass kein Malware- oder anderer Drittparteieingriff in den Code aufgetreten ist).

[0044] **Fig.** 2 ist ein Konzeptdiagramm, welches das System **200** als ein zusätzliches Beispielsystem für das Austauschen codierter Daten zwischen zwei authentifizierten Vorrichtungen **202A** und **202B** gemäß Techniken dieser Offenbarung zeigt. Das System **200** weist die Vorrichtung **202A** und die Vorrichtung **202B** (gemeinsam "Vorrichtungen **202**") auf. Die Vorrichtungen **202** sind über einen Kommunikationskanal oder eine Verbindung **216** kommunikativ gekoppelt. Beispiele der Verbindung **216** umfassen eine Form eines verdrahteten oder drahtlosen Kommunikationsmediums für das Austauschen von Daten zwischen zwei oder mehr Vorrichtungen in der Art der Vorrichtungen **202**. Die Vorrichtung **202A** weist ein Authentifizierungsmodul **230A** und einen Datenspeicher **250A** auf, während die Vorrichtung **202B** ein Authentifizierungsmodul **230B** und einen Datenspeicher **250B** aufweist.

[0045] Der Datenspeicher **250A** und der Datenspeicher **250B** (gemeinsam "Datenspeicher **250**") repräsentieren ein beliebiges geeignetes Speichermedium für das Speichern von Informationen vor und nach der Übertragung über die Verbindung **216**. Die am Datenspeicher **250A** gespeicherten Informationen können durch das Modul **230A** zugänglich sein, und die am Datenspeicher **250B** gespeicherten Informationen können durch das Modul **230B** zugänglich sein. Beispielsweise können ein oder mehrere Prozessoren der Vorrichtung **202A** Befehle in Zusammenhang mit dem Authentifizierungsmodul **230A** ausführen, welche das Modul **230A** veranlassen, Lese-/Schreibvorgänge am Datenspeicher **250A** auszuführen, um Informationen vor der Übertragung zur Vorrichtung **202B** oder nach dem Empfang von der Vorrichtung **202B** zu verarbeiten. Ähnlich kann ein ASIC der Vorrichtung **202B** Operationen in Zusammenhang mit dem Authentifizierungsmodul **230B** ausführen, welche das Modul **230B** veranlassen, Lese-/Schreibvorgänge am Datenspeicher **250B** auszuführen, um Informationen vor der Übertragung zur Vorrichtung **202A** oder nach dem Empfang von der Vorrichtung **202A** zu verarbeiten.

[0046] Die Authentifizierungsmodule **230A** und **230B** (gemeinsam "Authentifizierungsmodule **230**") können die Vorrichtungen **202** in die Lage versetzen, ein Aufforderung-Antwort-Protokoll für das Authentifizieren von Vorrichtungen **202** auszuführen und die Integrität der über die Verbindung **216** ausgetauschten Daten zu gewährleisten. Die Authentifizierungsmodule **230** können jeweilige Instanzen eines von der Ausführung des Aufforderung-Antwort-Protokolls abgeleiteten Sitzungsschlüssels verwenden, um die über die Verbindung **216** ausgetauschten Daten zu codieren und zu entschlüsseln. Die Authentifizierungsmodule **230** können unter Verwendung einer Vielzahl von Technologien und auf viele verschiedene Arten implementiert werden. Beispielsweise können die Authentifizierungsmodule **230** bei einigen Beispielen eine Kombination von Hardware, Software und/oder Firmware aufweisen, welche dafür ausgelegt ist, hier beschriebene Operationen für das Authentifizieren und Verschlüsseln/Entschlüsseln von Daten auszuführen. Bei einigen Beispielen repräsentieren die Authentifizierungsmodule **230** allein stehende integrierte Schaltungen oder weisen einen oder

mehrere Prozessoren auf, die dafür ausgelegt sind, hier beschriebene Operationen für das Authentifizieren und Verschlüsseln/Entschlüsseln von Daten auszuführen. Bei einigen Beispielen repräsentieren die Authentifizierungsmodule **230** individuelle Halbleiterchips und weisen einen Speicher auf. Bei einigen Beispielen können die Funktionalität und die Merkmale der Authentifizierungsmodule **230** als eine oder mehrere System-on-chip-Komponenten implementiert werden (beispielsweise um die Größe und/oder die Kosten der Vorrichtungen **202** zu verringern).

[0047] Das Authentifizierungsmodul **230A** weist ein Schlüsselerzeugungsmodul **234A** und ein Chiffrier-/Dechiffriermodul **238A** auf. Das Schlüsselerzeugungsmodul **234A** weist ein MAC-Funktionsmodul **236A** auf. Das Authentifizierungsmodul **230B** weist ein Schlüsselerzeugungsmodul **234B**, ein MAC-Funktionsmodul **236B** und ein Chiffrier-/Dechiffriermodul **238B** auf. Das Schlüsselerzeugungsmodul **234B** weist das MAC-Funktionsmodul **236B** auf.

[0048] Die Schlüsselerzeugungsmodule **234A** und **234B** (gemeinsam "Schlüsselerzeugungsmodule **234**") bestimmen jeweils MAC-Tags **244A** und **244B** für das Authentifizieren zwischen den Vorrichtungen **202** übertragener Nachrichten, und sie bestimmten auch jeweilige kryptographische Schlüssel **246A** und **246B** für das Chiffrieren und Dechiffrieren der Nachrichten.

[0049] Für das Authentifizieren zwischen den Vorrichtungen **202** übertragener Nachrichten kann das Schlüsselerzeugungsmodul **234A** einen Sitzungsschlüssel **240A** für das Erzeugen des MAC-Tags **244A** in Zusammenhang mit einer Kommunikationssitzung zwischen der Vorrichtung **202A** und der Vorrichtung **202B** bestimmen und kann das Schlüsselerzeugungsmodul **234B** einen Sitzungsschlüssel **240B** für das Erzeugen des MAC-Tags **244B** in Zusammenhang mit der Kommunikationssitzung zwischen der Vorrichtung **202A** und der Vorrichtung **202B** bestimmen. Die Sitzungsschlüssel **240A** und **240B** repräsentieren zwei getrennte Instanzen desselben Sitzungsschlüssels. Die MAC-Tags **244A** und **244B** repräsentieren zwei getrennte Instanzen desselben MAC-Tags. Jeder der Sitzungsschlüssel **240A** und **240B** und jedes der MAC-Tags **244A** und **244B** werden unabhängig jeweils durch die Schlüsselerzeugungsmodule **234A** und **234B** abgeleitet.

[0050] Bei einigen Beispielen leiten die Schlüsselerzeugungsmodule **234** die Sitzungsschlüssel **240A** und **240B** einer Sitzung als Nebenprodukt eines Aufforderung-Antwort-Protokolls ab. Beispielsweise kann das Protokoll eine asymmetrische Elliptische-Kurve-Authentifizierung verwenden. Eine elliptische Kurve E über einem finiten Feld K ist der Lösungssatz (x, y) in K x K einer kubischen Gleichung $y^2 + a1xy + a3y = x^3 + a2x^2 + a4x + a6$ ohne singuläre Punkte, wobei a1, a2, a3, a4 und a6 Elemente des finiten Felds K sind. Durch Hinzufügen des Punkts bei der Unendlichkeit O als Nullelement bilden die Punkte der elliptischen Kurve eine finite abelsche Gruppe. Das Gruppengesetz ist durch die algebraische Tatsache definiert, dass jede Linie durch zwei Punkte P und Q von E die Kurve bei einem dritten nicht notwendigerweise verschiedenen Punkt R schneidet und die Summe P + Q + R = O das Nullelement ist. (Falls P = Q, schneidet die Tangente die Kurve bei R.)

[0051] Analog zu Vektorräumen ist die Skalarmultiplikation k·P definiert, wo k eine natürliche Zahl ist und P ein Punkt von E ist. Dann bezeichnet k·P die k-fache Addition von P. Für kryptographisch starke elliptische Kurven ist die Skalarmultiplikation k·P = S eine Einwegfunktion, wobei es beispielsweise möglich ist, k·P in einem Zeitpolynom in der Länge der Parameter zu berechnen, wobei jedoch bei gegebenen Werten P und S nur Algorithmen mit einer exponentiellen Laufzeit für die Berechnung des Skalars k bekannt sind. Diese Einwegfunktion kann die Basis für die Sicherheit kryptographischer Protokolle unter Verwendung elliptischer Kurven sein.

[0052] Beispielsweise kann das Schlüsselerzeugungsmodul **234A** zum Erzeugen der MAC-Tags **244A** und zum Veranlassen der Vorrichtung **202B**, das MAC-Tag **244B** zu erzeugen (beispielsweise zum Authentifizieren zwischen den Vorrichtungen **202** übertragener Nachrichten), einen Zufallswert 'λ bestimmen und den Zufallswert 'λ für die Erzeugung einer Aufforderung x_A verwenden, welche das Schlüsselerzeugungsmodul **234A** zum Schlüsselerzeugungsmodul **234B** sendet. Bei einigen Beispielen weist die Aufforderung x_A die affine x-Koordinate eines Punkts A auf einer Kurve auf, welcher ein skalares Vielfaches eines Basispunkts P einer Kurve ist, welcher durch seine affine x-Koordinate x_p mit dem gewählten Zufallswert 'λ repräsentiert ist. Gemäß anderen Ausführungsformen kann die Aufforderung anhand des Zufallswerts 'λ sowie zusätzlicher Daten erzeugt werden. Die durch x_A repräsentierte Aufforderung A kann vom Schlüsselerzeugungsmodul **234A** zum Schlüsselerzeugungsmodul **234B** übertragen werden.

[0053] Zu Beginn der Authentifizierung hält die Vorrichtung **202A** den öffentlichen Authentifizierungsschlüssel (PAK) **248A** und hält die Vorrichtung **202B** einen entsprechenden geheimen Authentifizierungsschlüssel (SAK) **249B**. Umgekehrt kann die Vorrichtung **202B** einen PAK **248B** halten und kann die Vorrichtung **202A** einen entsprechenden SAK **249A** halten. PAK **248A** und SAK **249B** bilden beide ein Authentifizierungsschlüsselpaar für das Authentifizieren von Nachrichten, wenn die Vorrichtung **202A** als ein Host wirkt und die Vorrichtung **202B** als ein Slave wirkt, und PAK **248B** und SAK **249A** bilden ein an-

deres Authentifizierungspaar für das Authentifizieren von Nachrichten, wenn die Vorrichtung **202B** als ein Host wirkt und die Vorrichtung **202A** als ein Slave wirkt.

[0054] Nach dem Empfang der Aufforderung x_A und ansprechend auf den Empfang der Aufforderung x_A kann das Schlüsselerzeugungsmodul **234B** den Sitzungsschlüssel **240B** erzeugen. Beispielsweise kann das Schlüsselerzeugungsmodul **234B** projektive Koordinaten X_B und Z_B für einen Punkt B auf der Kurve bestimmen und dann eine Funktion f anwenden, um den Sitzungsschlüssel **240B** = f (X_B, Z_B) zu erhalten.

[0055] Insbesondere kann bei einigen Beispielen das Schlüsselerzeugungsmodul **234B** X_B und Z_B durch die Funktion f bestimmen, welche eine Skalarmultiplikation der Aufforderung x_A und des SAK **249B** ist. Das Schlüsselerzeugungsmodul **234B** kann eine Anzahl von Bits für die Skalarmultiplikation mit einer Länge L aus einer der Koordinaten auswählen, um den Sitzungsschlüssel **240B** zu bilden. Bei diesem Beispiel kann die Koordinate X_B verwendet werden, gemäß anderen Ausführungsformen kann Z_B jedoch stattdessen verwendet werden. Die Anzahl der Bits und daher die natürliche Zahl können auch gemäß Ausführungsformen variieren.

[0056] Das Schlüsselerzeugungsmodul **234B** kann den Sitzungsschlüssel **240B** für nachfolgende Datenauthentifizierungen in ein Register oder einen Speicher in Zusammenhang mit der Vorrichtung **202B** (beispielsweise beim Datenspeicher **250B**) oder eine andere Speicherstelle innerhalb des Authentifizierungsmoduls **230B** schreiben. Bei einigen Beispielen kann das Schlüsselerzeugungsmodul **234** den Sitzungsschlüssel **240B** für jede Authentifizierungsprozedur wiederherstellen.

[0057] Als nächstes kann das Schlüsselerzeugungsmodul **234B** eine Funktion g auf die projektiven Koordinaten X_B und Z_B anwenden, um Daten w = g(X_B, Z_B) zu erhalten, welche ausreichen, damit das Schlüsselerzeugungsmodul **234A** die tatsächliche projektive Repräsentation des vom Schlüsselerzeugungsmodul **234B** verwendeten Punkts B identifiziert und berechnet. Insbesondere kann das Schlüsselerzeugungsmodul **234B** bei einem Beispiel ein MAC-Funktionsmodul **236** aufrufen, um einen MAC-Algorithmus auszuführen, der die projektive Koordinate X_B und die Nachrichtendaten (beispielsweise Informationen), die zu übertragen sind (MAK), als Eingaben nimmt und das MAC-Tag **244B** als Ausgabe ausgibt. Auf diese Weise kann das Schlüsselerzeugungsmodul **234B** auf der Grundlage des Sitzungsschlüssels **240B** das MAC-Tag **244B** bestimmen, welches eine Instanz des MAC-Tags in Zusammenhang mit der Kommunikationssitzung repräsentiert.

[0058] Das Authentifizierungsmodul **230B** kann das MAC-Tag **244B** und die projektive Koordinate Z_B (oder X_B bei Ausführungsformen, bei denen Z_B als Quelle des Sitzungsschlüssels **240B** verwendet wurde) zum Schlüsselerzeugungsmodul **234A** senden, so dass das Schlüsselerzeugungsmodul **234A** das MAC-Tag **244A** und die Authentizität der mit dem MAC-Tag **244B** übertragenen Daten bestimmen kann. Mit anderen Worten kann das Schlüsselerzeugungsmodul **234B** ein MAC-Funktionsmodul **236B** aufrufen, welches als eine Art Authentifizierungsstempel wirkt, wodurch gewährleistet wird, dass zwischen den Vorrichtungen **202** ausgetauschte Daten während der Übertragung nicht manipuliert werden.

[0059] Das Schlüsselerzeugungsmodul **234A** kann dann den Sitzungsschlüssel **240A** bestimmen. Beispielsweise kann das Schlüsselerzeugungsmodul **234A** in einem ersten Schritt die affine Koordinate x_C eines Punkts C auf der Kurve durch Multiplikation des gewählten Zufallswerts 'λ mit der affinen x-Koordinate des öffentlichen Authentifizierungsschlüssels **248A** als ein erwarteter Antwortwert berechnen. Dann kann die Vorrichtung **202A** eine Funktion h auf den erwarteten Antwortwert x_C und die von der Vorrichtung **202B** empfangenen Daten w anwenden, was zur Erzeugung eines Sitzungsschlüssels **240A** = h (x_C, w) führt. Falls demgemäß die Authentifizierung zwischen den Vorrichtungen **202A** und **202B** gelingt, sollte der Sitzungsschlüssel **240A** an diesem Punkt gleich dem Sitzungsschlüssel **240B** sein.

[0060] Insbesondere kann die Vorrichtung **202A** bei einem Beispiel die affine Koordinate x_C eines Punkts C auf der Kurve durch Multiplikation des gewählten Zufallswerts 'λ mit der affinen x-Koordinate von PAK **248A** berechnen oder hat sie bereits berechnet. Die Vorrichtung **202A** kann dann x_C mit dem von der Vorrichtung **202B** empfangenen Wert Z_B multiplizieren, um die projektive Koordinate X_B zu bestimmen. Die Vorrichtung **202A** kann als nächstes L Bits von X_B nehmen, um den Sitzungsschlüssel **240A** zu bestimmen, und schreibt den Sitzungsschlüssel **240A** in den Speicher **218** (beispielsweise ein RAM, ein Datenspeicher **250A** oder ein anderer nicht flüchtiger Speicher der Vorrichtung **202A**), um ihn bei anschließenden Datenauthentifizierungen zu verwenden.

[0061] Unter Verwendung des Sitzungsschlüssels **240A** kann die Vorrichtung **202A** versuchen, die zuvor von der Vorrichtung **202B** über die Verbindung **216** empfangenen Daten zu authentifizieren. Beispielsweise kann das Authentifizierungsmodul **230A** verifizieren, dass das MAC-Tag **244A** mit dem MAC-Tag **244B** in Zusammenhang mit den von der Vorrichtung **202B** empfangenen Daten übereinstimmt. Bei folgenden Empfängen von Daten zwischen den Vorrichtungen **202A** und **202B** braucht die Vorrichtung **202A** angesichts der Tatsache, dass die Sitzungs-

schlüssel **240A** und **240B** bereits bestimmt und authentifiziert wurden, lediglich die von der Vorrichtung **202B** empfangenen Daten in den Speicher am Datenspeicher **250A** zu schreiben.

[0062] Zu einer späteren Zeit können die Vorrichtungen **202A** und **202B** den Authentifizierungsprozess wiederholen, um die Sitzungsschlüssel **240A** und **240B** wieder aufzufrischen (beispielsweise um die Sitzungsschlüssel **240A** und **240B** zu schützen und die Authentifizierung beizubehalten). Der Zeitraum zwischen Auffrischungen von Sitzungsschlüsseln kann variieren und auf der Stärke der MAC-Funktion oder Fingerabdruckoperationen, die von den MAC-Funktionen **236A** und **236B** ausgeführt werden, beruhen.

[0063] Gemäß Techniken dieser Offenbarung für das Chiffrieren und Dechiffrieren zwischen Vorrichtungen **202** übertragener Nachrichten kann das Schlüsselerzeugungsmodul **234A** den Sitzungsschlüssel **240A**, wie vorstehend bestimmt, für das Erzeugen des kryptographischen Schlüssels **246A** in Zusammenhang mit einer Kommunikationssitzung zwischen der Vorrichtung **202A** und der Vorrichtung **202B** wieder verwenden und kann das Schlüsselerzeugungsmodul **234B** den Sitzungsschlüssel **240B**, wie vorstehend bestimmt, für das Erzeugen des kryptographischen Schlüssels **246B** in Zusammenhang mit der Kommunikationssitzung zwischen der Vorrichtung **202A** und der Vorrichtung **202B** wieder verwenden.

[0064] Die kryptographischen Schlüssel **246A** und **246B** repräsentieren zwei getrennte Instanzen desselben kryptographischen Schlüssels zum Codieren (beispielsweise Codieren und/oder Entschlüsseln) einer Nachricht in Zusammenhang mit den Vorrichtungen **202**. Jeder der kryptographischen Schlüssel **246A** und **246B** wird unabhängig durch die jeweiligen Schlüsselerzeugungsmodule **234A** und **234B** abgeleitet. Durch Ableiten einer getrennten Instanz desselben kryptographischen Schlüssels können die Vorrichtungen **202** Datennachrichten codieren und entschlüsseln, ohne Informationen über die Verbindung **216** zu teilen, die einem Angreifer einer dritten Partei Hinweise für das Entschlüsseln der Daten bereitstellen können.

[0065] Beim Betrieb kann das Schlüsselerzeugungsmodul **234B** den Sitzungsschlüssel **240B** als Teil des Prozesses bestimmen, den das Schlüsselerzeugungsmodul **234B** durchmacht, um das MAC-Tag **244B** in Zusammenhang mit einer Kommunikationssitzung zwischen der Vorrichtung **202B** und der Vorrichtung **202A** zu erzeugen. Als nächstes kann das Schlüsselerzeugungsmodul **234B** zumindest teilweise auf der Grundlage des Sitzungsschlüssels **244B** den kryptographischen Schlüssel **246B** für das Codieren einer für die Vorrichtung **202A** vorgesehenen Nachricht bestimmen.

[0066] Das Schlüsselerzeugungsmodul **234B** kann den kryptographischen Schlüssel **246B** unter Verwendung des MAC-Funktionsmoduls **236B** erzeugen. Beispielsweise kann das Authentifizierungsmodul **230B** in einigen Fällen vom Authentifizierungsmodul **230A** der Vorrichtung **202A** eine Angabe eines Startwerts N (beispielsweise einer zufällig ausgewählten Zahl) zur Bestimmung des kryptographischen Schlüssels **246B** empfangen und den Startwert N zusammen mit dem Sitzungsschlüssel **244B** als Eingaben für das MAC-Funktionsmodul **236B** zur Bestimmung des kryptographischen Schlüssels **246B** verwenden. Beim Beispiel aus **Fig.** 2 ist der Startwert N als "Startwert **242**" dargestellt.

[0067] Bei einigen Beispielen wird der Startwert N zur Verbesserung der Sicherheit aktualisiert. Beispielsweise kann der Startwert N nie wiederholt werden (wobei beispielsweise nie der gleiche Wert zwei Mal verwendet wird), und falls das Schlüsselerzeugungsmodul **234B** bestimmt, dass der Startwert N der gleiche zuvor verwendete Wert ist, kann das Schlüsselerzeugungsmodul **234B** vom Authentifizierungsmodul **230A** einen aktualisierten Startwert anfordern (beispielsweise eine erneute Aufforderung).

[0068] Bei einigen Beispielen ist der Startwert N keine "zufällige" Zahl, sondern kann vielmehr ein "geteiltes Geheimnis" sein, welches die Vorrichtungen **202** jeweils unabhängig ableiten. Beispielsweise kann der Startwert N auf einem Hash-Wert gemeinsamer Daten (beispielsweise Zeit, Datum usw.) beruhen oder vorprogrammiert sein (beispielsweise von einem Administrator).

[0069] In jedem Fall kann das MAC-Funktionsmodul **236B** den Startwert N sowie die projektive Koordinate X_B oder eine Ableitung davon (beispielsweise den Sitzungsschlüssel **240B** oder andere L Bits der projektiven Koordinate X_B) empfangen und den kryptographischen Schlüssel **246B** bestimmen. Der auch als Strom des Nachrichtenchiffrierblocks (MCB) bezeichnete kryptographische Schlüssel **246B** kann gleich der Ausgabe von MAC (X_B, N) sein.

[0070] Während das Schlüsselerzeugungsmodul **234B** den kryptographischen Schlüssel **246B** unter Verwendung des MAC-Funktionsmoduls **236B** erzeugt, erzeugt das Schlüsselerzeugungsmodul **234A** der Vorrichtung **202A** den kryptographischen Schlüssel **246A** unter Verwendung des MAC-Funktionsmoduls **236B** und des Startwerts **242**. Beispielsweise kann das Schlüsselerzeugungsmodul **234A** den Sitzungsschlüssel **240A** (oder eine andere Ableitung von X_B) und den Startwert **242** als Eingabe in das MAC-Funktionsmodul **236A** bereitstellen, um

als Ausgabe den kryptographischen Schlüssel **246A** (auch als MCB' bezeichnet) zu erzeugen.

[0071] Nach der Erzeugung der kryptographischen Schlüssel **246A** und **246B** sind die Vorrichtungen **202** bereit, Nachrichten zu codieren und zu entschlüsseln. Das Authentifizierungsmodul **230B** kann eine Nachricht (auch als "Daten" bezeichnet) zur Übertragung zur Vorrichtung **202A** erzeugen, welche einen Teil der im Datenspeicher **250B** gespeicherten Daten enthält. Bei einigen Beispielen enthält die vom Authentifizierungsmodul **230B** erzeugte Nachricht eine Angabe des MAC-Tags in Zusammenhang mit der Kommunikationssitzung (beispielsweise MAC-Tag **244B**) und zusätzliche Informationen (beispielsweise proprietärer Code, Befehls- und Steuerfunktionen für ein unbemanntes Luftfahrzeug oder andere Nachrichtendaten, die einen Schutz benötigen).

[0072] Das Authentifizierungsmodul **230B** kann sich auf das Chiffrier-/Dechiffriermodul **238B** verlassen, um die Nachricht auf der Grundlage des kryptographischen Schlüssels **246B** zu codieren. Beispielsweise kann das Chiffrier-/Dechiffriermodul **238B** eine Exklusiv-ODER-(XOR)-Operation zwischen einem nicht codierten Abschnitt der Nachricht und dem kryptographischen Schlüssel **246B** ausführen, um verwürfelte Daten als Ausgabe zu erzeugen. Beispielsweise kann das Chiffrier-/Dechiffriermodul **238B** bei einigen Beispielen chiffrierte Daten CpDaten erzeugen, die gleich MCB ^ Daten sind.

[0073] Bei einigen Beispielen kann sich das Chiffrier-/Dechiffriermodul **238B** auf Zyklische-Redundanzprüfung-(CRC)-Operationen oder Hash-Funktionen an Stelle der Exklusiv-ODER-Operation für das Verwürfeln einer Nachricht auf der Grundlage des kryptographischen Schlüssels **246B** verlassen. CRC ist ein Fehlererkennungscode, der üblicherweise in digitalen Netzen und Speichervorrichtungen verwendet wird, um versehentliche Änderungen an Rohdaten zu erkennen. An Datenblöcke, welche in diese Systeme eintreten, wird ein kurzer Prüfwert auf der Grundlage des Rests einer Polynomdivision ihres Inhalts angehängt. Beim Zurückgewinnen wird die Umkehrberechnung ausgeführt, um die unverwürfelten Daten zu bestimmen. Eine kryptographische Hash-Funktion kann es dem Chiffrier-/Dechiffriermodul **238B** ermöglichen, eine Kombination des kryptographischen Schlüssels **246B** und der Nachrichtendaten auf einen bestimmten Hash-Wert abzubilden. Nach dem Empfang können die ursprünglichen Daten durch Ausführen der Umkehr-Hash-Funktion des bestimmten Hash-Werts dechiffriert werden. Beim Beispiel aus **Fig.** 2 kann das Chiffrier-/Dechiffriermodul **238B** den kryptographischen Schlüssel **246B** und die Nachrichtendaten als Eingabe empfangen und unter Verwendung von CRS-Operationen oder Hash-Funktionen verwürfelte Daten als Ausgabe erzeugen.

[0074] Nach der Codierung der Nachricht auf der Grundlage des kryptographischen Schlüssels **246B** kann das Authentifizierungsmodul **230B** der Vorrichtung **202B** zur Vorrichtung **202A** die codierte Nachricht über die Verbindung **216** übertragen. Das Authentifizierungsmodul **230A** der Vorrichtung **202A** kann von der Vorrichtung **202B** die codierte Nachricht über die Verbindung **216** empfangen. Auf der Grundlage des kryptographischen Schlüssels **246A** kann das Authentifizierungsmodul **230A** die über die Verbindung **216** empfangene Nachricht entschlüsseln.

[0075] Beispielsweise kann das Authentifizierungsmodul **230A** die codierte Nachricht dem Chiffrier-/Dechiffriermodul **238A** bereitstellen. Falls eine Exklusiv-ODER-Operation verwendet wurde, um die Nachricht zu codieren, kann das Chiffrier-/Dechiffriermodul **238A** die Nachricht auf der Grundlage des kryptographischen Schlüssels **246A** entschlüsseln, indem es gleichermaßen die Exklusiv-ODER-Operation zwischen der Nachricht und dem kryptographischen Schlüssel **246A** ausführt. Andernfalls kann das Chiffrier-/Dechiffriermodul **238A**, falls eine CRC-Operation oder eine Hash-Funktion vom Chiffrier-/Dechiffriermodul **238B** verwendet wurde, um die über die Verbindung **216** empfangene Nachricht zu codieren, die über die Verbindung **216** empfangene Nachricht unter Verwendung des kryptographischen Schlüssels **246A** und der Umkehr-CRC-Operation oder Hash-Funktion entschlüsseln.

[0076] Das Chiffrier-/Dechiffriermodul **238A** kann die nicht codierten Daten am Datenspeicher **250A** speichern, damit sie von anderen Komponenten der Vorrichtung **202A** verwendet werden können. Falls die Vorrichtung **202A** beispielsweise ein unbemanntes Luftfahrzeug ist, kann ein Prozessor oder eine andere Komponente der Vorrichtung **202A** die am Datenspeicher **250A** gespeicherten uncodierten Daten als Eingabe einer Steuerfunktion (beispielsweise zum Steuern des unbemannten Luftfahrzeugs) bereitstellen.

[0077] Bei einigen Beispielen kann das Authentifizierungsmodul **230A** anschließend an das Entschlüsseln der Nachricht auf der Grundlage des MAC-Tags **244A** die Nachricht authentifizieren. Mit anderen Worten kann das Authentifizierungsmodul **230A** vor dem Speichern der nicht codierten Nachrichtendaten am Datenspeicher **250A** Authentifizierungsoperationen an einem eingebetteten MAC-Tag, das in den Daten vorgefunden wird, unter Verwendung des MAC-Tags **244A** ausführen, wie vorstehend beschrieben wurde.

[0078] Beispielsweise kann das Authentifizierungsmodul **230A** bestimmen, ob das MAC-Tag **244A** dem MAC-Tag **244B** entspricht (wie anhand der über die Verbindung **216** empfangenen nicht codierten Nachrichtendaten abgeleitet). Bei einigen Beispielen kann

das Authentifizierungsmodul **230A** ansprechend auf die Bestimmung, dass das MAC-Tag **244A** dem MAC-Tag **244B** entspricht, bestimmen, dass die über die Verbindung **216** empfangene Nachricht authentisch ist. Mit anderen Worten kann das Authentifizierungsmodul **230A** bestimmen, dass die über die Verbindung **216** empfangene Nachricht tatsächlich von der Vorrichtung **202B** ausgegangen ist und nicht während der Übertragung (beispielsweise durch eine dritte Partei) geändert wurde. Bei einigen Beispielen kann das Authentifizierungsmodul **230A** ansprechend auf die Bestimmung, dass das MAC-Tag **244A** nicht dem MAC-Tag **244B** entspricht, bestimmen, dass die über die Verbindung **216** empfangene Nachricht nicht authentisch ist. Mit anderen Worten kann das Authentifizierungsmodul **230A** bestimmen, dass die über die Verbindung **216** empfangene Nachricht nicht tatsächlich von der Vorrichtung **202B** herrühren kann oder während der Übertragung geändert worden sein kann (beispielsweise durch eine dritte Partei, durch Wetteranomalien oder eine andere Störung in Zusammenhang mit der Übertragung).

[0079] Die **Fig.** 3A und **Fig.** 3B sind Flussdiagramme, welche durch Beispielvorrichtungen zum Codieren von Daten ausgeführte Beispieloperationen **300A** und **300B** gemäß einem oder mehreren Aspekten der vorliegenden Offenbarung zeigen. Die **Fig.** 3A und **Fig.** 3B werden nachstehend in Zusammenhang mit dem System **100** aus **Fig.** 1 beschrieben. Beispielsweise kann wenigstens ein Prozessor der Vorrichtung **102A** Operationen **300A** ausführen und kann wenigstens ein Prozessor der Vorrichtung **102B** Operationen **300B** ausführen. Bei anderen Beispielen kann das Authentifizierungsmodul **130A** eine ASIC aufweisen, die dafür ausgelegt ist, Operationen **300A** auszuführen, und kann das Authentifizierungsmodul **130B** eine ASIC aufweisen, die dafür ausgelegt ist, Operationen **300B** auszuführen. Bei wieder anderen Beispielen kann die Vorrichtung **102A** einen Speicher oder ein anderes nicht flüchtiges computerlesbares Speichermedium aufweisen, das Befehle aufweist, die, wenn sie von wenigstens einem Prozessor der Vorrichtung **102A** ausgeführt werden, den wenigstens einen Prozessor veranlassen, die Operationen **300A** auszuführen, und kann die Vorrichtung **102B** einen Speicher oder ein anderes nicht flüchtiges computerlesbares Speichermedium aufweisen, das Befehle aufweist, die, wenn sie von wenigstens einem Prozessor der Vorrichtung **102B** ausgeführt werden, den wenigstens einen Prozessor veranlassen, die Operationen **300B** auszuführen.

[0080] Die Vorrichtung **102B** kann eine Aufforderungsantwort erzeugen und zur Vorrichtung **102A** senden (**302B**), und die Vorrichtung **102A** kann die Aufforderungsantwort von der Vorrichtung **102B** empfangen (**302A**). Beispielsweise kann die Vorrichtung **102A** von der Vorrichtung **102B** ein anfängliches Signal, eine anfängliche Nachricht oder einen Datenabschnitt über die Verbindung **116A** empfangen, wodurch eine Aufforderung x_A angegeben wird, welche die affine x-Koordinate eines Punkts A auf einer Kurve aufweist, welcher die Skalarmultiplikation eines Basispunkts P einer durch seine affine x-Koordinate x_p repräsentierten Kurve mit einem gewählten Zufallswert 'λ ist. Gemäß anderen Ausführungsformen kann die Aufforderung anhand des Zufallswerts 'λ sowie zusätzlicher Daten erzeugt werden. Die Aufforderung A, die durch x_A repräsentiert ist, kann vom Authentifizierungsmodul **130B** zum Authentifizierungsmodul **130A** übertragen werden.

[0081] Die Vorrichtung **102A** kann einen Sitzungsschlüssel für das Erzeugen eines Nachrichtenauthentifierungscode(MAC)-Tags bestimmen (**304A**). Beispielsweise kann das Authentifizierungsmodul **130A** projektive Koordinaten X_B und Z_B für einen Punkt B auf der Kurve bestimmen und dann eine Funktion f anwenden, um einen Sitzungsschlüssel zu erhalten, der gleich $f(X_B, Z_B)$ ist.

[0082] Die Vorrichtung **102A** kann das MAC-Tag für das Authentifizieren der Nachricht in Zusammenhang mit der Vorrichtung **102B** auf der Grundlage des Sitzungsschlüssels bestimmen (**306A**). Beispielsweise kann das Authentifizierungsmodul **130A** die von der Vorrichtung **102B** empfangene Aufforderung zusammen mit dem abgeleiteten Sitzungsschlüssel in eine MAC-Funktion eingeben und als Ausgabe eine erste Instanz des MAC-Tags empfangen, das für das Authentifizieren von Daten zu verwenden ist, die während der Kommunikationssitzung zwischen den Vorrichtungen **102A** und **102B** übertragen werden.

[0083] Ähnlich kann die Vorrichtung **102B** einen Sitzungsschlüssel für das Erzeugen eines Nachrichtenauthentifierungscode(MAC)-Tags bestimmen (**304B**). Beispielsweise kann das Authentifizierungsmodul **130B** projektive Koordinaten X_B und Z_B für einen Punkt B auf der Kurve bestimmen und dann eine Funktion f anwenden, um einen Sitzungsschlüssel zu erhalten, der gleich $f(X_B, Z_B)$ ist.

[0084] Die Vorrichtung **102B** kann das MAC-Tag für das Authentifizieren der Nachricht in Zusammenhang mit der Vorrichtung **102A** auf der Grundlage des Sitzungsschlüssels bestimmen (**306B**). Beispielsweise kann das Authentifizierungsmodul **130A** die von der Vorrichtung **102B** empfangene Aufforderung zusammen mit dem abgeleiteten Sitzungsschlüssel in eine MAC-Funktion eingeben und als Ausgabe eine erste Instanz des MAC-Tags empfangen, das für das Authentifizieren von Daten zu verwenden ist, die während der Kommunikationssitzung zwischen den Vorrichtungen **102A** und **102B** übertragen werden.

[0085] Die Vorrichtung **102B** kann einen Startwert zum Bestimmen eines kryptographischen Schlüssels zum Codieren einer Nachricht in Zusammenhang mit

der Vorrichtung **102A** auf der Grundlage des Sitzungsschlüssels senden (**308B**), und die Vorrichtung **102A** kann den Startwert zum Bestimmen eines kryptographischen Schlüssels zum Codieren einer Nachricht in Zusammenhang mit der Vorrichtung **102B** auf der Grundlage des Sitzungsschlüssels empfangen (**308A**). Beispielsweise kann die Vorrichtung **102A** eine anschließende Nachricht von der Vorrichtung **102B** empfangen, welche einen Startwert N zur Eingabe in eine MAC-Funktion aufweist, welche das Authentifizierungsmodul **130A** verwendet, um eine erste Instanz eines von den Vorrichtungen **102** geteilten kryptographischen Schlüssels abzuleiten.

[0086] Die Vorrichtung **102B** kann den kryptographischen Schlüssel für das Codieren der Nachricht in Zusammenhang mit der Vorrichtung **102A** auf der Grundlage des Sitzungsschlüssels bestimmen (**310B**), und die Vorrichtung **102A** kann den kryptographischen Schlüssel für das Codieren der Nachricht in Zusammenhang mit der Vorrichtung **102B** auf der Grundlage des Sitzungsschlüssels bestimmen (**310A**). Beispielsweise kann das Authentifizierungsmodul **130A** den von der Vorrichtung **102B** empfangenen Startwert zusammen mit dem zuvor abgeleiteten Sitzungsschlüssel in die MAC-Funktion eingeben (beispielsweise dem Sitzungsschlüssel, der zuvor für das Bestimmen des MAC-Tags in Zusammenhang mit der Kommunikationssitzung verwendet wurde).

[0087] Bei einigen Beispielen kann das Authentifizierungsmodul **130A** an Stelle der Verwendung des von der Vorrichtung **102B** empfangenen Startwerts den Startwert auf der Grundlage des Sitzungsschlüssels ableiten. Beispielsweise kann das Authentifizierungsmodul **130A** eine Hash-Funktion verwenden, welche den Startwert nach Gl. 1 bestimmt:

$$\text{abgeleiteter Startwert (z.B. Sitzungsschlüssel 2)} = a\cdot(\text{Sitzungsschlüssel})^2 + b\cdot(\text{Sitzungsschlüssel}) \quad \text{Gl. 1}$$

[0088] Unter Verwendung der Ausgabe von Gl. 1 kann das Authentifizierungsmodul **130A** den Sitzungsschlüssel und den empfangenen oder abgeleiteten Startwert in die MAC-Funktion eingeben, die zuvor für die Bestimmung des MAC-Tags verwendet wurde, um den kryptographischen Schlüssel für die aktuelle Kommunikationssitzung zu bestimmen.

[0089] Die Vorrichtung **102A** kann die Nachricht in Zusammenhang mit der Vorrichtung **102B** auf der Grundlage des kryptographischen Schlüssels codieren oder entschlüsseln (**312A**), und die Vorrichtung **102B** kann die Nachricht in Zusammenhang mit der Vorrichtung **102A** auf der Grundlage des kryptographischen Schlüssels codieren oder entschlüsseln (**312B**). Falls beispielsweise codierte Daten von der Vorrichtung **102A** empfangen werden, kann das Authentifizierungsmodul **130A** den kryptographischen Schlüssel und die empfangenen Nachrichtendaten in ein Dechiffriermodul eingeben, das bei manchen Beispielen eine Exklusiv-ODER-Operation verwendet, um die nicht codierten Daten zu bestimmen. Falls die Vorrichtung **102A** umgekehrt codierte Daten zur Vorrichtung **102B** sendet, kann das Authentifizierungsmodul **130A** den kryptographischen Schlüssel und die nicht codierten Nachrichtendaten in ein Chiffriermodul eingeben, das bei manchen Beispielen eine Exklusiv-ODER-Operation verwendet, um die codierten Daten zu bestimmen.

[0090] Die Vorrichtung **102A** kann die Nachricht in Zusammenhang mit der Vorrichtung **102B** auf der Grundlage des MAC-Tags authentifizieren (**314A**), und die Vorrichtung **102B** kann die Nachricht in Zusammenhang mit der Vorrichtung **102A** auf der Grundlage des MAC-Tags authentifizieren (**314B**). Wenn beispielsweise codierte Nachrichten zur Vorrichtung **102B** gesendet werden, kann die Vorrichtung **102A** das für diese bestimmte Kommunikationssitzung abgeleitete MAC-Tag an den codierten Nachrichtenstrom anhängen, so dass die Vorrichtung **102B** Authentifizierungstechniken ausführen kann, um die Integrität der Daten zu verifizieren. Bei einigen Beispielen ist das MAC-Tag in den codierten Daten codiert oder auf andere Weise verwürfelt. Bei anderen Beispielen ist das MAC-Tag nicht verwürfelt. Wenn umgekehrt codierte Nachrichten empfangen werden, die dechiffriert werden müssen, kann die Vorrichtung **102A** das MAC-Tag, das in die codierten Daten eingebettet oder angehängt ist, vergleichen, um zu bestimmen, ob das MAC-Tag, welches die Vorrichtung **102A** zuvor abgeleitet hat, mit dem MAC-Tag übereinstimmt, das mit den Daten empfangen wurde. Falls die MAC-Tags übereinstimmen, kann die Vorrichtung **102A** bestimmen, dass die von der Vorrichtung **102B** empfangenen codierten Daten authentisch sind (was beispielsweise bedeutet, dass die Daten tatsächlich von der Vorrichtung **102B** ausgegangen sind und nicht während der Übertragung von einer dritten Partei geändert wurden).

[0091] **Fig.** 4 ist ein Konzeptdiagramm, das einen zwischen zwei authentifizierten Vorrichtungen übertragenen Beispieldatenstrom **400** gemäß einem oder mehreren Aspekten der vorliegenden Offenbarung zeigt. **Fig.** 4 wird nachstehend in Zusammenhang mit dem System **100** aus **Fig.** 1 beschrieben.

[0092] **Fig.** 4 zeigt einen Versatz, der durch ein Authentifizierungsmodul in der Art der Authentifizierungsmodule **130** der Vorrichtungen **102** in eine Nachricht eingefädelt wird, um den nächsten Nachrichtenchiffrierblock oder kryptographischen Schlüssel zu erzeugen, der während einer nachfolgenden Nachricht zu verwenden ist. Beispielsweise kann die Vorrichtung **102**, nachdem ein Zeitraum seit der Erzeugung eines aktuellen kryptographischen Schlüs-

sels verstrichen ist, nachdem eine bestimmte Menge codierter Daten unter Verwendung des aktuellen kryptographischen Schlüssels zwischen den Vorrichtungen **102** übertragen wurde, nachdem der aktuelle kryptographische Schlüssel beeinträchtigt wurde oder nachdem der aktuelle kryptographische Schlüssel auf andere Weise verbraucht wurde, einen neu erzeugten Nachrichtenchiffrierblock aufnehmen, um ein kontinuierliches Daten-Parsen zu ermöglichen.

[0093] Bei einigen Techniken zum Ausführen von Datenintegritätsprüfungen kann eine Prüfsumme an einen Datenstrom angehängt werden, um zu prüfen, ob die Daten gegenüber ihrer ursprünglichen Form geändert wurden. **Fig.** 4 zeigt, dass als eine Erweiterung eines langen Datenstroms ein letztes Datenwort oder Byte als erste Daten mit einem nonce-Versatz N_off angefügt werden kann, so dass ein nächster Nachrichtenchiffrierblock (kryptographischer Schlüssel) MCB(m) durch die Vorrichtungen **102** als MAC (X_B, N + N_off) bestimmt werden kann, wobei MCB (m) mehrere MCB definiert. Zusätzlich zeigt **Fig.** 4, dass die Bitstelle der Daten, welche den X_B-Wert repräsentiert, und der Startwert N im Datenstrom beispielsweise unter Verwendung eines gemeinsamen Geheimnisses oder durch Hinzufügen eines gemeinsamen Geheimnisses zu X_B und/oder N oder bei anderen Beispielen als Funktion des N- und N_off-Verfahrens verwürfelt werden kann.

[0094] Fig. 5 ist ein Konzeptdiagramm, welches das System **500** als ein zusätzliches Beispielsystem zum Austauschen codierter Daten zwischen den Vorrichtungen **502A**–**502C** (gemeinsam "Vorrichtungen" **502**) zeigt, wobei die Vorrichtung **502A** eine einzige Host-Vorrichtung ist und die Vorrichtungen **502B** und **502C** zwei getrennte Slave-Vorrichtungen sind, gemäß Techniken dieser Offenbarung. Die Vorrichtungen **502A**–**502C** ähneln den Vorrichtungen **102** und **202** aus den **Fig.** 1 und **Fig.** 2. Beim Beispiel aus **Fig.** 5 ist die Vorrichtung **502A** als eine Host-Vorrichtung ausgelegt und sind die Vorrichtungen **502B** und **502C** als getrennte Slave-Vorrichtungen ausgelegt.

[0095] Die Vorrichtungen **502** weisen jeweilige Authentifizierungsmodule **530A**–**530C** und jeweilige Chiffrier-/Dechiffriermodule **538A**–**538C** auf. Die Vorrichtung **502A** weist ferner ein Schlüsselerzeugungsmodul **534** und Datenspeicher **560A** und **562A** auf. Die Vorrichtung **502B** weist einen Datenspeicher **560B** auf, und die Vorrichtung **502C** weist einen Datenspeicher **560C** auf. Nachdem die Vorrichtungen **502A** und **502B** über Verbindungen **516A** codierte Daten ausgetauscht haben, entsprechen die im Datenspeicher **560A** enthaltenen Informationen den im Datenspeicher **560B** enthaltenen Informationen. Ähnlich entsprechen die im Datenspeicher **562A** enthaltenen Informationen nach einem Informationsaustausch zwischen den Vorrichtungen **502A** und **502C** über die Verbindung **516B** den am Datenspeicher **562C** gespeicherten Informationen.

[0096] Beim Beispiel aus **Fig.** 5 teilen sich die Vorrichtungen **502A** und **502B** einen ersten Satz kryptographischer Schlüssel **546B** und **546B'** auf der Grundlage eines ersten Satzes von (X_B, X_B') und teilen sich die Vorrichtungen **502A** und **502C** einen zweiten Satz kryptographischer Schlüssel **546C** und **546C'** auf der Grundlage eines zweiten Satzes von (X_{B2}, X_{B2}'). Mit anderen Worten kann sich beim Beispiel aus **Fig.** 5 die Vorrichtung **502A**, die als Host des Systems **500** wirkt, getrennte kryptographische Schlüsselpaare mit den Vorrichtungen **502B** und der Slave-Vorrichtung **502C** teilen. Auf diese Weise kann die Vorrichtung **502A** eine unabhängige, sichere Kommunikationssitzung über die Verbindungen **516A** und **516B** beibehalten.

[0097] Bei anderen Beispielen können sich die Vorrichtungen **502A** und **502B** zwei getrennte Sätze kryptographischer Schlüssel teilen, Der erste Satz kryptographischer Schlüssel **546B** und **546B'** auf der Grundlage eines ersten Satzes von (X_B, X_B') kann verwendet werden, wenn die Vorrichtung **502A** Daten zur Vorrichtung **502B** sendet. Der zweite Satz kryptographischer Schlüssel kann auf einem zweiten Satz von (X_B, X_B') beruhen und verwendet werden, wenn die Vorrichtung **502B** Daten zur Vorrichtung **502A** sendet. Auf diese Weise können die Vorrichtungen **502A** und **502B** verschiedene kryptographische Schlüssel abhängig davon verwenden, welche Vorrichtung sendet und welche empfängt.

[0098] Fig. 6 ist ein Konzeptdiagramm, das einen Authentifizierungsablauf für das Austauschen codierter Daten zwischen den Vorrichtungen **602A** und **602B** des Systems **600** als Beispiele zweier authentifizierter Vorrichtungen gemäß Techniken dieser Offenbarung zeigt. Die Vorrichtung **602A** weist einen Authentifizierungs-ASIC **630A** auf, und die Vorrichtung **602B** weist einen Authentifizierungs-ASIC **630B** auf. Die Authentifizierungs-ASIC **630A** und **630B** sind ASIC, welche Operationen ähnlich jenen Operationen ausführen, die von den Authentifizierungsmodulen **130** aus **Fig.** 1 ausgeführt werden.

[0099] Beim Beispiel aus **Fig.** 6 wirkt die Vorrichtung **602B** als ein Host und weist einen öffentlichen Schlüssel auf. Unter Verwendung der vorstehend mit Bezug auf die Berechnung elliptischer Kurven beschriebenen Techniken kann das Authentifizierungsmodul **630B** eine Aufforderung auf der Grundlage des öffentlichen Schlüssels erzeugen und die Aufforderung zur Slave-Vorrichtung **602A** senden. Diese Aufforderung kann eine "Klartext"- oder "codierte" Aufforderung sein. Nach einer erfolgreichen Authentifizierung zwischen den Vorrichtungen **602A** und **602B** auf der Grundlage der Aufforderung tauschen die Vorrichtungen **602A** und **602B** codierte Daten wäh-

rend eines Datentransaktionszeitfensters **690A** aus. **Fig.** 6 zeigt, dass anschließende Aufforderungen für nachfolgende Datentransaktionszeitfenster **690B** und **690C** erzeugt werden.

[0100] Fig. 7 ist ein Konzeptdiagramm, welches ein System **700** für das Austauschen codierter Daten zwischen zwei authentifizierten Vorrichtungen **702A** und **702B** gemäß Techniken dieser Offenbarung zeigt. Das System **700** weist die Vorrichtung **702A** auf, welche über eine Verbindung **716A** mit der Vorrichtung **702B** kommuniziert. Die Vorrichtungen **702A** und **702B** können codierte Daten **712A** über die Verbindung **716A** gemäß Techniken der vorliegenden Offenbarung austauschen. Die Vorrichtung **702A** weist einen Prozessor **760A**, ein Authentifizierungsmodul **730A** und einen Speicher **710A** auf, der ein Programm **770A** und eine Nachricht **750A** aufweist. Die Vorrichtung **702B** weist ein Authentifizierungsmodul **730B**, einen Speicher **710B** und eine Nachricht **750B** auf.

[0101] Bei einigen Beispielen kann die Vorrichtung **702A** eine Host-Vorrichtung sein, welche die Vorrichtung **702B** auffordert. Bei anderen Beispielen kann die Vorrichtung **702A** auf eine Aufforderung von der Vorrichtung **702B** antworten. In jedem Fall kann die Vorrichtung **702B** die Nachricht **750B** als codierte Daten **712A** zur Vorrichtung **702A** senden, welche die codierten Daten **712A** als Nachricht **750A** speichert.

[0102] Nach dem Empfang der Nachricht **750A** kann die Vorrichtung **702A** die Nachricht **750A** zum Ausführen des Programms **770A** verwenden. Beispielsweise kann die Vorrichtung **702A** Befehle in Zusammenhang mit dem Programm **770A** unter Verwendung des Prozessors **760A** ausführen. Während der Ausführung des Programms **770A** am Prozessor **760A** kann sich die Vorrichtung **702A** auf in der Nachricht **750A** enthaltene Informationen verlassen, um die Ausführung des Programms **770A** abzuschließen.

[0103] Bei einigen Beispielen kann die Vorrichtung **702A** die Nachricht **750A** durch verschiedene und eindeutige Informationen auf der Grundlage einer anschließenden Nachricht **750B** ersetzen, die empfangen wird, wenn eine andere Vorrichtung **702B** mit der Verbindung **716A** verbunden wird. Während der Ausführung des Programms **770A** kann sich die Vorrichtung **702A** auf in der Nachricht **750A** enthaltene Informationen verlassen, um während der Ausführung eines Teils des Programms **770A** zu indexieren. Bei anderen Beispielen kann sich die Vorrichtung **702A** auf in der Nachricht **750A** enthaltene Informationen verlassen, um einen Wert eines Parameters für eine mathematische Berechnung oder Steuerfunktion, die als Teil der Ausführung des Programms **770A** ausgeführt wird, zu bestimmen. Bei einigen Beispielen sind die in der Nachricht **750A** enthaltenen Informationen sicher durch einen Prozessor **760A** zugänglich, so dass die Nachricht nicht an anderen Speicherstellen der Vorrichtung **702A** repliziert werden kann. Bei einigen Beispielen kann die Vorrichtung **702A** bestimmen, wann eine Verbindung zwischen den Vorrichtungen **702A** und **702B** endet, und die Vorrichtung **702B** kann ansprechend auf die Beendigung der Verbindung mit der Vorrichtung **702B** die Nachricht **750A** aus dem Speicher **710A** entfernen.

[0104] Bei einigen Beispielen repräsentiert das Programm **770A** einen Steueralgorithmus und weist die Nachricht **750A** einen Wert eines Parameters auf, der erforderlich ist, um den Steueralgorithmus auszuführen. Beispielsweise kann die Vorrichtung **702A** ein Fahrzeug (beispielsweise ein UAV) sein und kann die Vorrichtung **702B** eine Nutzlast oder eine andere austauschbare Komponente des Fahrzeugs sein. Die Vorrichtung **702A** kann das Programm **770A** als einen Steueralgorithmus ausführen, der auf andere Weise von der spezifischen Vorrichtung **702B** abhängt. Beispielsweise kann eine Version der Vorrichtung **702B** eine Größen- oder Gewichtsabmessung aufweisen, die von anderen Versionen der Vorrichtung **702B** verschieden ist. Wenn die Vorrichtung **702B** über die Verbindung **716A** mit der Vorrichtung **702A** gekoppelt wird, kann die Vorrichtung **702A** die Größen- oder Gewichtsabmessung über die Nachricht **750A** herausfinden und die Steuerung der Vorrichtung **702A** entsprechend einstellen.

[0105] Fig. 8 ist ein Konzeptdiagramm, das einen Beispielpseudocode **800** zur Ausführung durch die Vorrichtung **702A** aus **Fig.** 7 zur Ausführung von Operationen zum Codieren von Daten gemäß einem oder mehreren Aspekten der vorliegenden Offenbarung zeigt. Beim Beispiel aus **Fig.** 8 repräsentiert das Programm **770A** ein "Master"- oder "Haupt"-Programm und können in der Nachricht **750A** enthaltene Informationen erforderlich sein, um die Ausführung des Programms **770A** abzuschließen. Bei anderen Beispielen kann die Nachricht **750A** jedoch selbst ein Master- oder Hauptprogramm sein und kann das Programm **770A** tatsächlich aus Informationen bestehen, die für das Abschließen der Ausführung der Nachricht **750A** erforderlich sind. Wie in **Fig.** 8 dargestellt ist, wird der Pseudocode **800** in keiner bestimmten Reihenfolge in Zeilen oder Befehle 1–17 unterteilt. Der Pseudocode **800** wird in weiteren Einzelheiten in Zusammenhang mit Operationen **900** aus **Fig.** 9 beschrieben. Die Vorrichtung **702A** kann den Pseudocode **800** in kompilierter oder vorkompilierter Form am Speicher **710A** speichern.

[0106] Fig. 9 ist ein Flussdiagramm, das von der Vorrichtung **702A** aus **Fig.** 7 ausgeführte Beispieloperationen **900** zum Codieren von Daten zeigt, wenn der Pseudocode **800** aus **Fig.** 8 ausgeführt wird, gemäß einem oder mehreren Aspekten der vorliegenden Offenbarung. Der Prozessor **760A** und das

Authentifizierungsmodul **730A** der Vorrichtung **702A** aus **Fig.** 7 können verwendet werden, um Operationen **900** auszuführen.

[0107] Beim Beispiel aus **Fig.** 9 kann die Vorrichtung **702A** eine Nachricht von einer zweiten Vorrichtung auf der Grundlage eines abgeleiteten kryptographischen Schlüssels entschlüsseln (**902**). Beispielsweise kann das Authentifizierungsmodul **730A** der Vorrichtung **702A** Operationen ähnlich den Operationen **302A**–**312A** aus **Fig.** 3 ausführen, um eine sichere Kommunikationssitzung mit der Vorrichtung **702B** einzurichten, einen kryptographischen Schlüssel für das Entschlüsseln der codierten Daten **712A** abzuleiten und mit dem abgeleiteten kryptographischen Schlüssel die codierten Daten **712A** zur Nachricht **750A** zu entschlüsseln.

[0108] Bei einigen Beispielen kann die Nachricht **750A** Informationen aufweisen, die vom an der Vorrichtung **702A** ausgeführten Programm **770A** verwendet werden, um eine Aufgabe auszuführen. Beispielsweise kann das Programm **770A** ein Steueralgorithmus für das Steuern der Bewegung der Vorrichtung **702A** sein und kann die Nachricht **750A** einen Parameterwert in Zusammenhang mit der Vorrichtung **702B** aufweisen, welchen das Programm **770A** benötigt, um die Bewegung der Vorrichtung **702A** zu steuern.

[0109] Bei einigen Beispielen kann die Nachricht **750A** Informationen aufweisen, die vom an der Vorrichtung **702A** ausgeführten Programm **770A** benötigt werden, um die Aufgabe abzuschließen. Beispielsweise kann die Nachricht **750A** einen kritischen Parameterwert oder einen Satz von Befehlen aufweisen, welche das Programm **770A** benötigt, um an der Vorrichtung **702A** ausgeführt zu werden.

[0110] In jedem Fall kann das Authentifizierungsmodul **730A** nach dem Entschlüsseln codierter Daten **712A** zur Nachricht **750A** die decodierten Daten am Speicher **710A** speichern. Der Prozessor **760A** kann Befehle für das Ausführen des Programms **770A** aus dem Speicher **710A** abrufen und einen anfänglichen Abschnitt des Programms **770A** ausführen (**904**). Beispielsweise kann der anfängliche Abschnitt des Programms **770A** die Befehle auf den Zeilen 1 und 2 des Pseudocodes **800** aufweisen.

[0111] Der Prozessor **760A** kann weitere Befehle für das Ausführen des Programms **770A** aus dem Speicher **710A** abrufen und einen anschließenden Abschnitt des Programms **770A** ausführen (**906**). Beispielsweise kann der anschließende Abschnitt des Programms **770A** die Befehle auf den Zeilen 3–15 des Pseudocodes **800** aufweisen.

[0112] Bei der Ausführung des anschließenden Abschnitts des Programms **770A** kann sich der Prozessor **760A** auf Daten in Zusammenhang mit der Nachricht **750A** verlassen. Wenn beispielsweise die Befehle auf den Zeilen 4–7 des Codes **800** ausgeführt werden, kann der Prozessor **760A** eine Case-Anweisung auf der Grundlage eines Werts einer auf der Zeile N der Nachricht **750A** gespeicherten Variable auswerten. Mit anderen Worten können die Zeilen der Nachricht **750A** Daten aufweisen, welche den Wert der vom Prozessor **760A** benötigten Variable für den Abschluss der Ausführung des Codes **800** angeben.

[0113] Bei weiteren Ausführung des anschließenden Abschnitts des Programms **770A** kann sich der Prozessor **760A** auf zusätzliche Daten in Zusammenhang mit der Nachricht **750A** verlassen, um die Aufgaben X und Y abzuschließen. Beispielsweise kann ein Prozessor **760A**, wenn er die Befehle auf den Zeilen 8–10 des Codes **800** ausführt, um die Aufgabe X abzuschließen, eine erste Funktion ausführen (beispielsweise durch Ausführen einer mathematischen Operation, einer logischen Operation, einer arithmetischen Operation oder einer anderen Operation), welche von einem Wert einer auf der Zeile N1 der Nachricht **750A** gespeicherten Variable und einem Wert einer vom Programm **770A** gespeicherten Variable abhängt. Und wenn er die Befehle auf den Zeilen 11–14 des Codes **800** ausführt, um die Aufgabe Y abzuschließen, kann der Prozessor **760A** eine zweite Funktion (beispielsweise eine bedingte Operation oder eine andere Operation) ausführen, welche von einem Wert einer auf der Zeile N2 der Nachricht **750A** gespeicherten Variable abhängt.

[0114] Nach Abschluss der Ausführung des anschließenden Abschnitts des Programms **770A** kann der Prozessor **760A** beurteilen, ob die Nachricht **750A** aus dem Speicher beseitigt werden sollte oder nicht (beispielsweise zur Sicherheit). Der Prozessor **760A** kann feststellen, ob die Vorrichtung **702B** noch mit der Verbindung **716A** verbunden ist (**908**). Beispielsweise kann der Prozessor **760A** Zeile 16 des Codes **800** ausführen. Die Vorrichtung **702A** kann das Entfernen der Vorrichtung **702B** feststellen, indem sie eine elektrische Verbindungsunterbrechung in Zusammenhang mit der Verbindung **716A** nach einem Zeitablauf oder ansprechend auf den Empfang einer anschließenden Aufforderung/Antwort zur Ausführung einer Authentifizierung (beispielsweise von derselben Vorrichtung **702B** oder von einer anderen oder neuen Vorrichtung **702B**) feststellt.

[0115] Falls die Vorrichtung **702B** noch verbunden ist, kann der Prozessor **760A** die Operationen **902**–**906** für das Ausführen des Programms **770A** und das Codieren der Daten **712A** wiederholen. Andernfalls kann der Prozessor **760A**, falls die Kommunikation zwischen der Vorrichtung **702B** und der Vorrichtung **702A** verloren geht oder auf andere Weise endet, Zeile 17 des Codes **800** ausführen und einen Entfernungs-, Lösch- oder Beseitigungsvorgang

am Abschnitt des Speichers **710A**, welcher die Nachricht **750A** speichert, ausführen. Der Prozessor **760A** kann die Nachricht **750A** aus dem Speicher **710A** löschen (**910**). Durch Entfernen der Nachricht **750A** aus dem Speicher kann die Vorrichtung **702A** weiter die Sicherheit der Daten in Zusammenhang mit der Nachricht **750A** gewährleisten.

[0116] Wenngleich **Fig.** 8 vorstehend unter der Annahme beschrieben wurde, dass die Nachricht **750A** Daten aufweist, die Teil des Programms **770A** sind, kann die Nachricht **750A** bei anderen Beispielen ein Programm zur Ausführung am Prozessor **760A** sein, wobei Daten in Zusammenhang mit dem Programm **770A** verwendet werden. Mit anderen Worten kann die Vorrichtung **702B** ein Programm als codierte Daten **712** zur Vorrichtung **702A** senden und kann die Vorrichtung **702A** das von der Vorrichtung **702B** empfangene Programm unter Verwendung zuvor am Speicher **710** gespeicherter Daten ausführen.

[0117] Auf diese Weise können zwei Vorrichtungen Daten gemäß den hier beschriebenen Techniken in einer solchen Weise codieren, dass sie vor einem unerlaubten Ausspionieren geschützt werden, ohne komplexe kryptographische Algorithmen ausführen zu müssen oder komplizierte Operationen durchführen zu müssen, um zuerst Daten vor der Übertragung zu codieren und die Daten anschließend nach dem Empfang zu entschlüsseln. Durch die Erzeugung kryptographischer Schlüssel für das Codieren und Entschlüsseln von Daten zumindest teilweise auf der Grundlage von Sitzungsschlüsseln, die bereits für Authentifizierungszwecke abgeleitet wurden, können die in dieser Offenbarung beschriebenen Techniken kostengünstige oder weniger komplizierte Systeme für das Austauschen von Informationen ermöglichen, ohne dass sie für ein Ausspionieren anfällig wären. Bei den Techniken müssen weniger Operationen ausgeführt werden, um ein sicheres Kommunikationsschema zu implementieren, als die Anzahl der Operationen, die typischerweise von anderen Systemen ausgeführt werden müssen, welche auf komplexen kryptographischen Algorithmen beruhen. Durch das Ausführen von weniger Operationen können Vorrichtungen gemäß den beschriebenen Techniken weniger elektrische Leistung verbrauchen und daher wirksamer arbeiten als andere Systeme.

Klausel 1. Ein Verfahren, welches Folgendes umfasst: Bestimmen, durch eine erste Vorrichtung, eines Sitzungsschlüssels zum Erzeugen eines Nachrichtenauthentifierungscode(MAC)-Tags in Zusammenhang mit einer Kommunikationssitzung zwischen der ersten Vorrichtung und einer zweiten Vorrichtung, Bestimmen eines kryptographischen Schlüssels zum Codieren einer Nachricht in Zusammenhang mit der zweiten Vorrichtung zumindest teilweise auf der Grundlage des Sitzungsschlüssels durch die erste Vorrichtung und Codieren der Nachricht auf der Grundlage des kryptographischen Schlüssels durch die erste Vorrichtung.

Klausel 2. Das Verfahren nach Klausel 1, wobei das Codieren der Nachricht wenigstens eines der folgenden umfasst: Codieren der Nachricht auf der Grundlage des kryptographischen Schlüssels durch die erste Vorrichtung oder Entschlüsseln der Nachricht auf der Grundlage des kryptographischen Schlüssels durch die erste Vorrichtung.

Klausel 3. Das Verfahren nach einer der Klauseln 1–2, welches ferner Folgendes umfasst: Bestimmen einer Instanz des MAC-Tags in Zusammenhang mit der Kommunikationssitzung auf der Grundlage des Sitzungsschlüssels durch die erste Vorrichtung und vor dem Codieren der Nachricht Erzeugen der Nachricht auf der Grundlage des MAC-Tags in Zusammenhang mit der Kommunikationssitzung durch die erste Vorrichtung.

Klausel 4. Das Verfahren nach Klausel 3, welches ferner Folgendes umfasst: Erzeugen der Nachricht durch die erste Vorrichtung, wobei die Nachricht eine Angabe des MAC-Tags in Zusammenhang mit der Kommunikationssitzung und zusätzliche Informationen aufweist.

Klausel 5. Das Verfahren nach einer der Klauseln 1–4, welches ferner Folgendes umfasst: nach dem Codieren der Nachricht auf der Grundlage des kryptographischen Schlüssels, Senden der Nachricht zur zweiten Vorrichtung durch die erste Vorrichtung.

Klausel 6. Das Verfahren nach einer der Klauseln 1–5, welches ferner Folgendes umfasst: Empfangen der Nachricht von der zweiten Vorrichtung durch die erste Vorrichtung und anschließend an das Entschlüsseln der Nachricht auf der Grundlage des kryptographischen Schlüssels, Speichern der in der Nachricht enthaltenen Informationen durch die erste Vorrichtung.

Klausel 7. Das Verfahren nach einer der Klauseln 1–6, welches ferner Folgendes umfasst: Bestimmen einer Instanz des MAC-Tags in Zusammenhang mit der Kommunikationssitzung auf der Grundlage des Sitzungsschlüssels durch die erste Vorrichtung, Empfangen der Nachricht von der zweiten Vorrichtung durch die erste Vorrichtung und anschließend an das Entschlüsseln der Nachricht, Authentifizieren der Nachricht auf der Grundlage des MAC-Tags in Zusammenhang mit der Kommunikationssitzung durch die erste Vorrichtung.

Klausel 8. Das Verfahren nach Klausel 7, wobei die Instanz des MAC-Tags in Zusammenhang mit der Kommunikationssitzung eine erste Instanz des MAC-Tags in Zusammenhang mit der Kommunikationssitzung ist, wobei das Verfahren ferner Folgendes umfasst: Bestimmen einer zweiten Instanz des MAC-Tags in Zusammenhang mit der Kommunikationssitzung auf der Grundlage der Nachricht durch die erste Vorrichtung, wobei das Authentifizieren der Nachricht das Bestimmen

aufweist, ob die erste Instanz des MAC-Tags in Zusammenhang mit der Kommunikationssitzung der zweiten Instanz des MAC-Tags in Zusammenhang mit der Kommunikationssitzung entspricht.

Klausel 9. Das Verfahren nach Klausel 8, welches ferner Folgendes umfasst: ansprechend auf die Bestimmung, dass die erste Instanz des MAC-Tags in Zusammenhang mit der Kommunikationssitzung der zweiten Instanz des MAC-Tags in Zusammenhang mit der Kommunikationssitzung entspricht, Bestimmen, dass die von der zweiten Vorrichtung empfangene Nachricht authentisch ist, durch die erste Vorrichtung und ansprechend auf die Bestimmung, dass die erste Instanz des MAC-Tags in Zusammenhang mit der Kommunikationssitzung nicht der zweiten Instanz des MAC-Tags in Zusammenhang mit der Kommunikationssitzung entspricht, Bestimmen, dass die von der zweiten Vorrichtung empfangene Nachricht nicht authentisch ist, durch die erste Vorrichtung.

Klausel 10. Das Verfahren nach einer der Klauseln 1–9, wobei: das Codieren der Nachricht auf der Grundlage des kryptographischen Schlüssels das Ausführen einer Exklusiv-ODER-Operation zwischen einem nicht codierten Abschnitt der Nachricht und dem kryptographischen Schlüssel umfasst, und das Entschlüsseln der Nachricht auf der Grundlage des kryptographischen Schlüssels das Ausführen der Exklusiv-ODER-Operation zwischen einem codierten Abschnitt der Nachricht und dem kryptographischen Schlüssel umfasst.

Klausel 11. Das Verfahren nach einer der Klauseln 1–10, welches ferner Folgendes umfasst: Empfangen einer Angabe eines Startwerts zum Bestimmen des kryptographischen Schlüssels von der zweiten Vorrichtung durch die erste Vorrichtung, wobei der kryptographische Schlüssel ferner zumindest teilweise auf der Grundlage des Startwerts bestimmt wird.

Klausel 12. Das Verfahren nach einer der Klauseln 1–11, wobei: der Sitzungsschlüssel ein erster Sitzungsschlüssel ist, der erste Sitzungsschlüssel bestimmt wird, indem von der zweiten Vorrichtung durch die erste Vorrichtung wenigstens der erste Sitzungsschlüssel empfangen wird, wobei der erste Sitzungsschlüssel durch wenigstens einen Prozessor der zweiten Vorrichtung erzeugt wird, die Nachricht codiert wird, indem mit wenigstens einem Prozessor der ersten Vorrichtung die Nachricht wenigstens mit dem ersten Sitzungsschlüssel decodiert wird, und das Verfahren ferner Folgendes umfasst: Verarbeiten der Nachricht durch die erste Vorrichtung, wobei das Verarbeiten der Nachricht das Modifizieren wenigstens eines Teils der in der Nachricht enthaltenen Informationen aufweist, Codieren der verarbeiteten Nachricht durch die erste Vorrichtung mit einem anderen durch wenigstens einen Prozessor der zweiten Vorrichtung erzeugten Sitzungsschlüssel und Ausgeben der verarbeiteten Nachricht an die zweite Vorrichtung durch die erste Vorrichtung.

Klausel 13. Das Verfahren nach einer der Klauseln 1–12, wobei die Nachricht Informationen umfasst, die von einem Programm, das auf der ersten Vorrichtung ausgeführt wird, verwendet werden, um eine Aufgabe auszuführen.

Klausel 14. Das Verfahren nach Klausel 13, wobei die Informationen vom Programm, das an der ersten Vorrichtung ausgeführt wird, benötigt werden, um die Aufgabe abzuschließen.

Klausel 15. Das Verfahren nach einer der Klauseln 13–14, wobei die Nachricht eine erste Nachricht von mehreren Nachrichten ist, die jeweils Informationen aufweisen, die von einem Programm verwendet werden, welches auf der ersten Vorrichtung ausgeführt wird, um eine Aufgabe auszuführen.

Klausel 16. Das Verfahren nach Klausel 15, welches ferner Folgendes umfasst: Ausführen des Programms ansprechend auf das Entschlüsseln der Nachricht auf der Grundlage des kryptographischen Schlüssels durch die erste Vorrichtung.

Klausel 17. Das Verfahren nach einer der Klauseln 13–16, welches ferner Folgendes umfasst: ansprechend auf die Bestimmung, dass die Kommunikationssitzung zwischen der ersten Vorrichtung und der zweiten Vorrichtung beendet ist, Löschen der Nachricht aus einem Speicher der ersten Vorrichtung durch die erste Vorrichtung.

Klausel 18. Eine erste Vorrichtung umfasst wenigstens einen Prozessor, der in der Lage ist, Folgendes auszuführen: Bestimmen eines Sitzungsschlüssels zum Erzeugen eines Nachrichtenauthentifierungscode(MAC)-Tags in Zusammenhang mit einer Kommunikationssitzung zwischen der ersten Vorrichtung und einer zweiten Vorrichtung, Bestimmen eines kryptographischen Schlüssels zum Codieren oder Entschlüsseln einer Nachricht in Zusammenhang mit der zweiten Vorrichtung zumindest teilweise auf der Grundlage des Sitzungsschlüssels und Codieren der Nachricht auf der Grundlage des kryptographischen Schlüssels.

Klausel 19. Die erste Vorrichtung nach Klausel 18, wobei der wenigstens eine Prozessor ferner in der Lage ist, Folgendes auszuführen: Bestimmen einer Instanz des MAC-Tags in Zusammenhang mit der Kommunikationssitzung auf der Grundlage des Sitzungsschlüssels, und vor dem Codieren der Nachricht, Erzeugen der Nachricht auf der Grundlage des MAC-Tags in Zusammenhang mit der Kommunikationssitzung.

Klausel 20. Die erste Vorrichtung nach Klausel 19, wobei der wenigstens eine Prozessor ferner in der Lage ist, die Nachricht zu erzeugen, wobei die Nachricht eine Angabe des MAC-Tags in Zusammenhang mit der Kommunikationssitzung und zusätzliche Informationen aufweist.

Klausel 21. Die erste Vorrichtung nach einer der Klauseln 18–20, wobei der wenigstens eine Prozessor ferner in der Lage ist, die Nachricht nach dem Codieren der Nachricht auf der Grundlage des kryptographischen Schlüssels zur zweiten Vorrichtung zu senden.

Klausel 22. Die erste Vorrichtung nach einer der Klauseln 18–21, wobei der wenigstens eine Prozessor ferner in der Lage ist, Folgendes auszuführen: Empfangen der Nachricht von der zweiten Vorrichtung, und anschließend an das Entschlüsseln der Nachricht auf der Grundlage des kryptographischen Schlüssels, Speichern der in der Nachricht enthaltenen Informationen.

Klausel 23. Die erste Vorrichtung nach einer der Klauseln 18–22, wobei der wenigstens eine Prozessor ferner in der Lage ist, Folgendes auszuführen: Bestimmen einer Instanz des MAC-Tags in Zusammenhang mit der Kommunikationssitzung auf der Grundlage des Sitzungsschlüssels, Empfangen der Nachricht von der zweiten Vorrichtung, und anschließend an das Entschlüsseln der Nachricht, Authentifizieren der Nachricht auf der Grundlage des MAC-Tags in Zusammenhang mit der Kommunikationssitzung.

Klausel 24. Die erste Vorrichtung nach einer der Klauseln 18–23, wobei der wenigstens eine Prozessor einen anwendungsspezifischen integrierten Schaltkreis (ASIC) umfasst.

Klausel 25. Die erste Vorrichtung nach einer der Klauseln 18–24, wobei die erste Vorrichtung und die zweite Vorrichtung ein unbemanntes Luftfahrzeug und eine Steuervorrichtung, die dafür ausgelegt ist, das unbemannte Luftfahrzeug zu steuern, umfassen.

Klausel 26. Ein System, welches Folgendes umfasst: Mittel zum Bestimmen eines Sitzungsschlüssels, um ein Nachrichtenauthentifierungscode(MAC)-Tag in Zusammenhang mit einer Kommunikationssitzung zwischen einer ersten Vorrichtung und einer zweiten Vorrichtung zu erzeugen, Mittel zum Bestimmen eines kryptographischen Schlüssels zum Codieren oder Entschlüsseln einer Nachricht in Zusammenhang mit der zweiten Vorrichtung zumindest teilweise auf der Grundlage des Sitzungsschlüssels und Mittel zum Codieren der Nachricht auf der Grundlage des kryptographischen Schlüssels.

[0118] Bei einem oder mehreren Beispielen können die beschriebenen Operationen in Hardware, Software, Firmware oder einer Kombination davon implementiert werden. Falls sie in Software implementiert werden, können die Operationen als ein oder mehrere Befehle oder Code auf einem computerlesbaren Medium gespeichert oder darüber übertragen werden und durch eine Hardware-basierte Verarbeitungseinheit ausgeführt werden. Computerlesbare Medien können computerlesbare Speichermedien, welche einem gegenständlichen Medium in der Art von Datenspeichermedien entsprechen, oder Kommunikationsmedien, einschließlich eines Mediums, welches die Übertragung eines Computerprogramms von einem Ort zu einem anderen, beispielsweise entsprechend einem Kommunikationsprotokoll, erleichtert, einschließen. Auf diese Weise können computerlesbare Medien allgemein (1) gegenständlichen computerlesbaren Speichermedien, die nicht flüchtig sind, oder (2) einem Kommunikationsmedium in der Art eines Signals oder einer Trägerwelle entsprechen. Datenspeichermedien können beliebige verfügbare Medien sein, auf die durch einen oder mehrere Computer oder einen oder mehrere Prozessoren zugegriffen werden kann, um Befehle, Code und/oder Datenstrukturen zur Implementation der in dieser Offenbarung beschriebenen Techniken abzurufen. Ein Computerprogrammprodukt kann ein computerlesbares Medium aufweisen.

[0119] Als Beispiel und ohne Einschränkung können solche computerlesbaren Speichermedien einen RAM, einen ROM, einen EEPROM, eine CD-ROM oder einen anderen optischen Plattenspeicher, einen magnetischen Plattenspeicher oder andere magnetische Speichervorrichtungen, einen Flash-Speicher oder ein anderes Medium, das verwendet werden kann, um einen gewünschten Programmcode in Form von Befehlen oder Datenstrukturen zu speichern, und worauf durch einen Computer zugegriffen werden kann, umfassen. Auch wird eine beliebige Verbindung geeignet als ein computerlesbares Medium bezeichnet. Falls beispielsweise Befehle von einer Webseite, einem Server oder einer anderen fernen Quelle unter Verwendung eines Koaxialkabels, eines faseroptischen Kabels, eines verdrillten Paares, einer digitalen Teilnehmerleitung (DSL) oder drahtloser Technologien in der Art von Infrarot-, Funk- und Mikrowellentechnologien übertragen werden, sind das Koaxialkabel, das faseroptische Kabel, das verdrillte Paar, DSL oder drahtlose Technologien, wie Infrarot-, Funk- und Mikrowellentechnologien, in der Definition eines Mediums enthalten. Es ist jedoch zu verstehen, dass computerlesbare Speichermedien und Datenspeichermedien keine Verbindungen, Trägerwellen, Signale oder andere flüchtigen Medien einschließen, sondern vielmehr nicht flüchtige, gegenständliche Speichermedien betreffen. Platte und Scheibe umfassen hier eine Compact Disk (CD), eine Laser Disc, eine optische Scheibe, eine Digital Versatile Disc (DVD), eine Diskette und eine Bluray Disc, wobei Platten gewöhnlich Daten magnetisch wiedergeben, während Scheiben Daten optisch mit Lasern wiedergeben. Kombinationen der vorstehend erwähnten sollten auch in den Geltungsbereich computerlesbarer Medien aufgenommen werden.

[0120] Befehle können durch einen oder mehrere Prozessoren in der Art eines oder mehrerer DSP, Mikroprozessoren für allgemeine Zwecke, ASIC, FPGA oder anderer äquivalenter oder diskreter Logikschal-

tungsanordnungen ausgeführt werden. Dementsprechend kann sich der hier verwendete Begriff "Prozessor" auf eine beliebige vorstehend erwähnte Struktur oder auf eine andere Struktur beziehen, die für die Implementation der hier beschriebenen Techniken geeignet ist. Zusätzlich kann bei einigen Aspekten die hier beschriebene Funktionalität innerhalb zweckgebundener Hardware- und/oder Softwaremodule bereitgestellt werden. Auch könnten die Techniken vollständig in einer oder mehreren Schaltungen oder Logikelementen implementiert werden.

[0121] Die Techniken dieser Offenbarung können in einer breiten Vielzahl von Vorrichtungen oder Geräten, einschließlich einer Lichtmaschine, einer integrierten Schaltung (IC) oder eines IC-Satzes (beispielsweise eines Chipsatzes), implementiert werden. Verschiedene Komponenten, Module oder Einheiten werden in dieser Offenbarung beschrieben, um funktionelle Aspekte von Vorrichtungen hervorzuheben, die dafür ausgelegt sind, die offenbarten Techniken auszuführen, sie müssen jedoch nicht unbedingt durch verschiedene Hardwareeinheiten verwirklicht werden. Vielmehr können, wie vorstehend beschrieben wurde, verschiedene Einheiten in einer Hardwareeinheit kombiniert werden oder durch eine Sammlung zusammenwirkender Hardwareeinheiten bereitgestellt werden, einschließlich eines oder mehrerer Prozessoren, wie vorstehend beschrieben, in Zusammenhang mit geeigneter Software und/oder Firmware.

[0122] Verschiedene Beispiele wurden beschrieben. Diese und andere Beispiele liegen innerhalb des Schutzumfangs der folgenden Ansprüche.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- US 8630411 [0001, 0020, 0029]

Patentansprüche

1. Verfahren, welches Folgendes umfasst:
Bestimmen, durch eine erste Vorrichtung, eines Sitzungsschlüssels zum Erzeugen eines Nachrichtenauthentifizierungscode-Tags, welcher einer Kommunikationssitzung zwischen der ersten Vorrichtung und einer zweiten Vorrichtung zugeordnet ist,
Bestimmen eines kryptographischen Schlüssels zum Codieren einer der zweiten Vorrichtung zugeordneten Nachricht, zumindest teilweise auf der Grundlage des Sitzungsschlüssels, durch die erste Vorrichtung, und
Codieren der Nachricht auf der Grundlage des kryptographischen Schlüssels durch die erste Vorrichtung.

2. Verfahren nach Anspruch 1, wobei das Codieren der Nachricht wenigstens eines der Folgenden umfasst:
Verschlüsseln der Nachricht auf der Grundlage des kryptographischen Schlüssels durch die erste Vorrichtung oder
Entschlüsseln der Nachricht auf der Grundlage des kryptographischen Schlüssels durch die erste Vorrichtung.

3. Verfahren nach Anspruch 1 oder 2, welches ferner Folgendes umfasst:
Bestimmen einer Instanz des Nachrichtenauthentifizierungscode-Tags, welcher der Kommunikationssitzung zugeordnet ist, auf der Grundlage des Sitzungsschlüssels durch die erste Vorrichtung und vor dem Verschlüsseln der Nachricht, Erzeugen der Nachricht durch die erste Vorrichtung auf der Grundlage des Nachrichtenauthentifizierungscode-Tags, welcher der Kommunikationssitzung zugeordnet ist.

4. Verfahren nach Anspruch 3, welches ferner Folgendes umfasst:
Erzeugen der Nachricht durch die erste Vorrichtung, wobei die Nachricht eine Angabe des Nachrichtenauthentifizierungscode-Tags, welcher der Kommunikationssitzung zugeordnet ist, und zusätzliche Informationen umfasst.

5. Verfahren nach einem der Ansprüche 1–4, welches ferner Folgendes umfasst:
nach dem Verschlüsseln der Nachricht auf der Grundlage des kryptographischen Schlüssels, Senden der Nachricht zur zweiten Vorrichtung durch die erste Vorrichtung.

6. Verfahren nach einem der Ansprüche 1–4, welches ferner Folgendes umfasst:
Empfangen der Nachricht von der zweiten Vorrichtung durch die erste Vorrichtung und
anschließend an das Entschlüsseln der Nachricht auf der Grundlage des kryptographischen Schlüssels, Speichern der in der Nachricht enthaltenen Informationen durch die erste Vorrichtung.

7. Verfahren nach Anspruch 1 oder 2, welches ferner Folgendes umfasst:
Bestimmen einer Instanz des Nachrichtenauthentifizierungscode-Tags, welcher der Kommunikationssitzung zugeordnet ist, auf der Grundlage des Sitzungsschlüssels durch die erste Vorrichtung,
Empfangen der Nachricht von der zweiten Vorrichtung durch die erste Vorrichtung und
anschließend an das Entschlüsseln der Nachricht,
Authentifizieren der Nachricht auf der Grundlage des Nachrichtenauthentifizierungscode-Tags, welcher der Kommunikationssitzung zugeordnet ist, durch die erste Vorrichtung.

8. Verfahren nach Anspruch 7, wobei die Instanz des Nachrichtenauthentifizierungscode-Tags, welcher der Kommunikationssitzung zugeordnet ist, eine erste Instanz des Nachrichtenauthentifizierungscode-Tags, welcher der Kommunikationssitzung zugeordnet ist, ist, wobei das Verfahren ferner Folgendes umfasst:
Bestimmen einer zweiten Instanz des Nachrichtenauthentifizierungscode-Tags, welcher der Kommunikationssitzung zugeordnet ist, auf der Grundlage der Nachricht durch die erste Vorrichtung, wobei das Authentifizieren der Nachricht ein Bestimmen aufweist, ob die erste Instanz des Nachrichtenauthentifizierungscode-Tags, welcher der Kommunikationssitzung zugeordnet ist, der zweiten Instanz des Nachrichtenauthentifizierungscode-Tags, welcher der Kommunikationssitzung zugeordnet ist, entspricht.

9. Verfahren nach Anspruch 8, welches ferner Folgendes umfasst:
in Antwort auf das Bestimmen, dass die erste Instanz des Nachrichtenauthentifizierungscode-Tags, welcher der Kommunikationssitzung zugeordnet ist, der zweiten Instanz des Nachrichtenauthentifizierungscode-Tags, welcher der Kommunikationssitzung zugeordnet ist, entspricht, Bestimmen, dass die von der zweiten Vorrichtung empfangene Nachricht authentisch ist, durch die erste Vorrichtung, und
in Antwort auf das Bestimmen, dass die erste Instanz des Nachrichtenauthentifizierungscode-Tags, welcher der Kommunikationssitzung zugeordnet ist, nicht der zweiten Instanz des Nachrichtenauthentifizierungscode-Tags, welcher der Kommunikationssitzung zugeordnet ist, entspricht, Bestimmen, dass die von der zweiten Vorrichtung empfangene Nachricht nicht authentisch ist, durch die erste Vorrichtung.

10. Verfahren nach einem der Ansprüche 1–9, wobei:
das Codieren ein Verschlüsseln der Nachricht auf der Grundlage des kryptographischen Schlüssels umfasst, welches ein Ausführen einer Exklusiv-ODER-

Operation zwischen einem nicht codierten Abschnitt der Nachricht und dem kryptographischen Schlüssel umfasst, und/oder
das Codieren ein Entschlüsseln der Nachricht auf der Grundlage des kryptographischen Schlüssels umfasst, welches ein Ausführen der Exklusiv-ODER-Operation zwischen einem codierten Abschnitt der Nachricht und dem kryptographischen Schlüssel umfasst.

11. Verfahren nach einem der Ansprüche 1–10, welches ferner Folgendes umfasst:
Empfangen einer Angabe eines Startwerts zum Bestimmen des kryptographischen Schlüssels von der zweiten Vorrichtung durch die erste Vorrichtung, wobei der kryptographische Schlüssel ferner zumindest teilweise auf der Grundlage des Startwerts bestimmt wird.

12. Verfahren nach einem der Ansprüche 1–11, wobei:
der Sitzungsschlüssel ein erster Sitzungsschlüssel ist, der erste Sitzungsschlüssel bestimmt wird, indem von der zweiten Vorrichtung durch die erste Vorrichtung wenigstens der erste Sitzungsschlüssel empfangen wird, wobei der erste Sitzungsschlüssel durch wenigstens einen Prozessor der zweiten Vorrichtung erzeugt wird,
die Nachricht codiert wird, indem mit wenigstens einem Prozessor der ersten Vorrichtung die Nachricht wenigstens mit dem ersten Sitzungsschlüssel decodiert wird, und
das Verfahren ferner Folgendes umfasst:
Verarbeiten der Nachricht durch die erste Vorrichtung, wobei das Verarbeiten der Nachricht das Modifizieren wenigstens eines Teils von in der Nachricht enthaltenen Informationen aufweist,
Verschlüsseln der verarbeiteten Nachricht durch die erste Vorrichtung mit einem anderen durch den wenigstens einen Prozessor der zweiten Vorrichtung erzeugten Sitzungsschlüssel und
Ausgeben der verarbeiteten Nachricht an die zweite Vorrichtung durch die erste Vorrichtung.

13. Verfahren nach einem der Ansprüche 1–12, wobei die Nachricht Informationen umfasst, die von einem Programm, das auf der ersten Vorrichtung ausgeführt wird, verwendet werden, um eine Aufgabe auszuführen.

14. Verfahren nach Anspruch 13, wobei die Informationen vom Programm, das an der ersten Vorrichtung ausgeführt wird, benötigt werden, um die Aufgabe abzuschließen.

15. Verfahren nach Anspruch 13 oder 14, wobei die Nachricht eine erste Nachricht von mehreren Nachrichten ist, die jeweils Informationen aufweisen, die von einem Programm verwendet werden, welches auf der ersten Vorrichtung ausgeführt wird, um eine Aufgabe auszuführen.

16. Verfahren nach Anspruch 15, welches ferner Folgendes umfasst:
Ausführen des Programms in Antwort auf das Entschlüsseln der Nachricht auf der Grundlage des kryptographischen Schlüssels durch die erste Vorrichtung.

17. Verfahren nach einem der Ansprüche 13–16, welches ferner Folgendes umfasst:
in Antwort auf ein Bestimmen, dass die Kommunikationssitzung zwischen der ersten Vorrichtung und der zweiten Vorrichtung beendet ist, Löschen der Nachricht aus einem Speicher der ersten Vorrichtung durch die erste Vorrichtung.

18. Erste Vorrichtung, welche wenigstens einen Prozessor umfasst, der betreibbar ist, Folgendes auszuführen:
Bestimmen eines Sitzungsschlüssels zum Erzeugen eines Nachrichtenauthentifizierungscode-Tags, welcher der Kommunikationssitzung zugeordnet ist, zwischen der ersten Vorrichtung und einer zweiten Vorrichtung,
Bestimmen eines kryptographischen Schlüssels zum Codieren einer Nachricht, die der zweiten Vorrichtung zugeordnet ist, zumindest teilweise auf der Grundlage des Sitzungsschlüssels und
Codieren der Nachricht auf der Grundlage des kryptographischen Schlüssels.

19. Erste Vorrichtung nach Anspruch 18, wobei der wenigstens eine Prozessor einen anwendungsspezifischen integrierten Schaltkreis (ASIC) umfasst.

20. Erste Vorrichtung nach Anspruch 18 oder 19, wobei die erste Vorrichtung und die zweite Vorrichtung ein unbemanntes Luftfahrzeug und eine Steuervorrichtung, die dafür ausgelegt ist, das unbemannte Luftfahrzeug zu steuern, umfassen.

21. Erste Vorrichtung nach einem der Ansprüche 18–20, wobei die erste Vorrichtung, insbesondere der Prozessor, zur Durchführung des Verfahrens nach einem der Ansprüche 1–17 betreibbar ist.

22. System, welches Folgendes umfasst:
Mittel zum Bestimmen eines Sitzungsschlüssels, um ein Nachrichtenauthentifizierungscode-Tag, welcher der Kommunikationssitzung zugeordnet ist, zwischen einer ersten Vorrichtung und einer zweiten Vorrichtung zu erzeugen,
Mittel zum Bestimmen eines kryptographischen Schlüssels zum Verschlüsseln oder Entschlüsseln einer Nachricht in Zusammenhang mit der zweiten Vorrichtung zumindest teilweise auf der Grundlage des Sitzungsschlüssels und

Mittel zum Codieren der Nachricht auf der Grundlage des kryptographischen Schlüssels.

Es folgen 10 Seiten Zeichnungen

Anhängende Zeichnungen

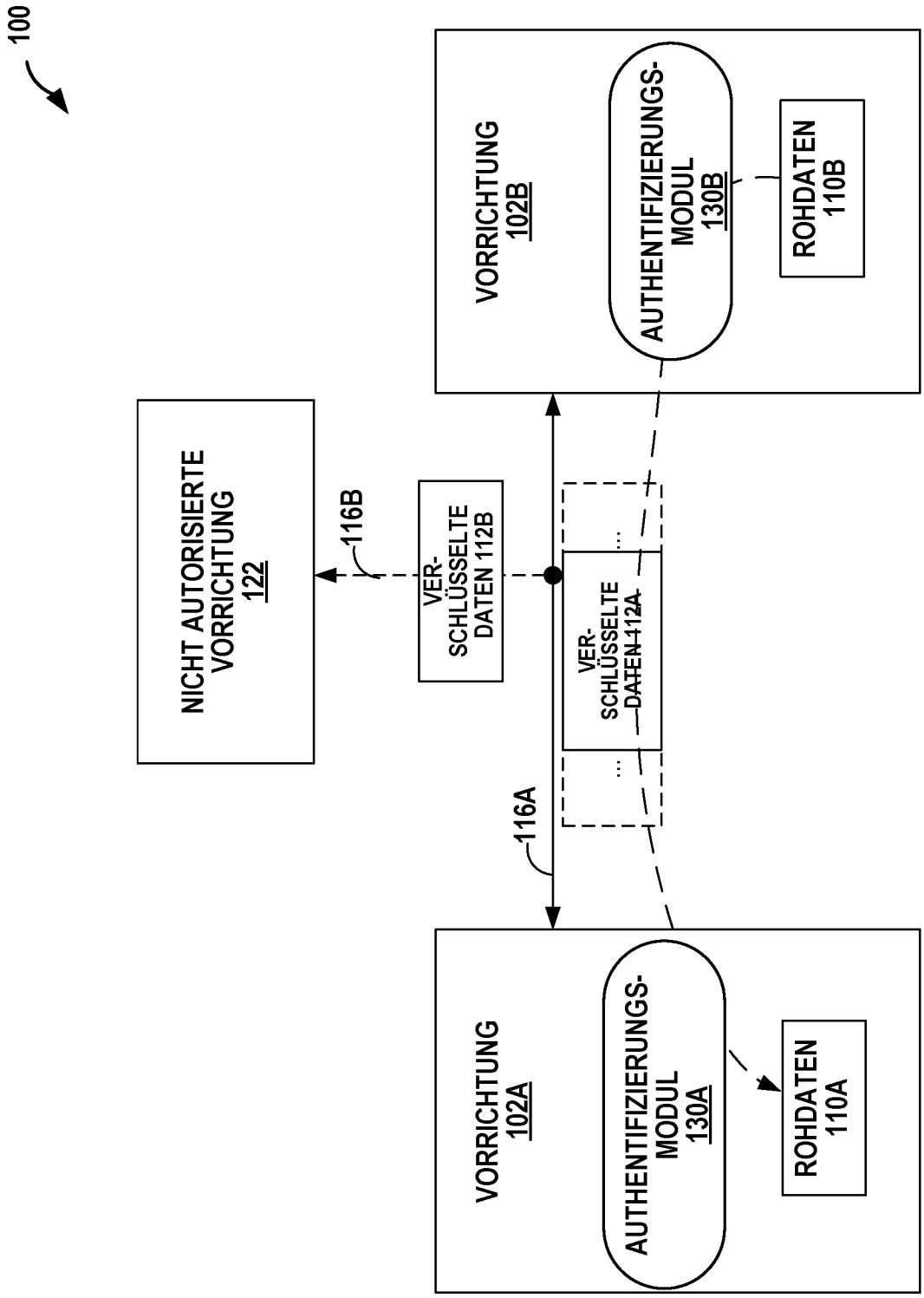


FIG. 1

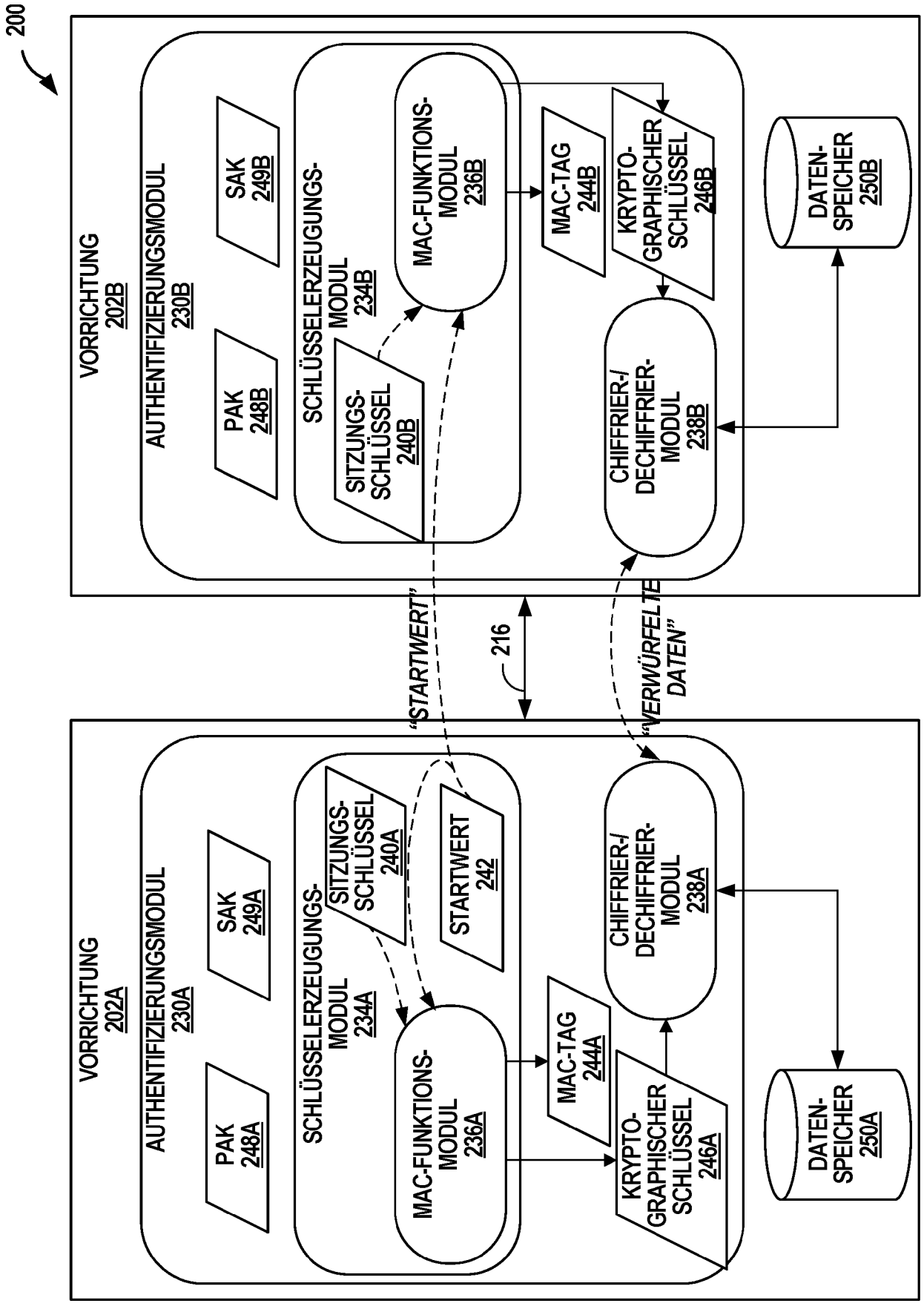

200
VORRICHTUNG 202B
AUTHENTIFIZIERUNGSMODUL 230B
PAK 248B
SAK 249B
SCHLÜSSELERZEUGUNGS-MODUL 234B
SITZUNGS-SCHLÜSSEL 240B
MAC-FUNKTIONS-MODUL 236B
MAC-TAG 244B
KRYPTO-GRAPHISCHER SCHLÜSSEL 246B
CHIFFRIER-/DECHIFFRIER-MODUL 238B
DATEN-SPEICHER 250B
"STARTWERT"
216
"VERWÜRFELTE DATEN"
VORRICHTUNG 202A
AUTHENTIFIZIERUNGSMODUL 230A
PAK 248A
SAK 249A
SCHLÜSSELERZEUGUNGS-MODUL 234A
SITZUNGS-SCHLÜSSEL 240A
STARTWERT 242
MAC-FUNKTIONS-MODUL 236A
MAC-TAG 244A
KRYPTO-GRAPHISCHER SCHLÜSSEL 246A
CHIFFRIER-/DECHIFFRIER-MODUL 238A
DATEN-SPEICHER 250A

FIG. 2

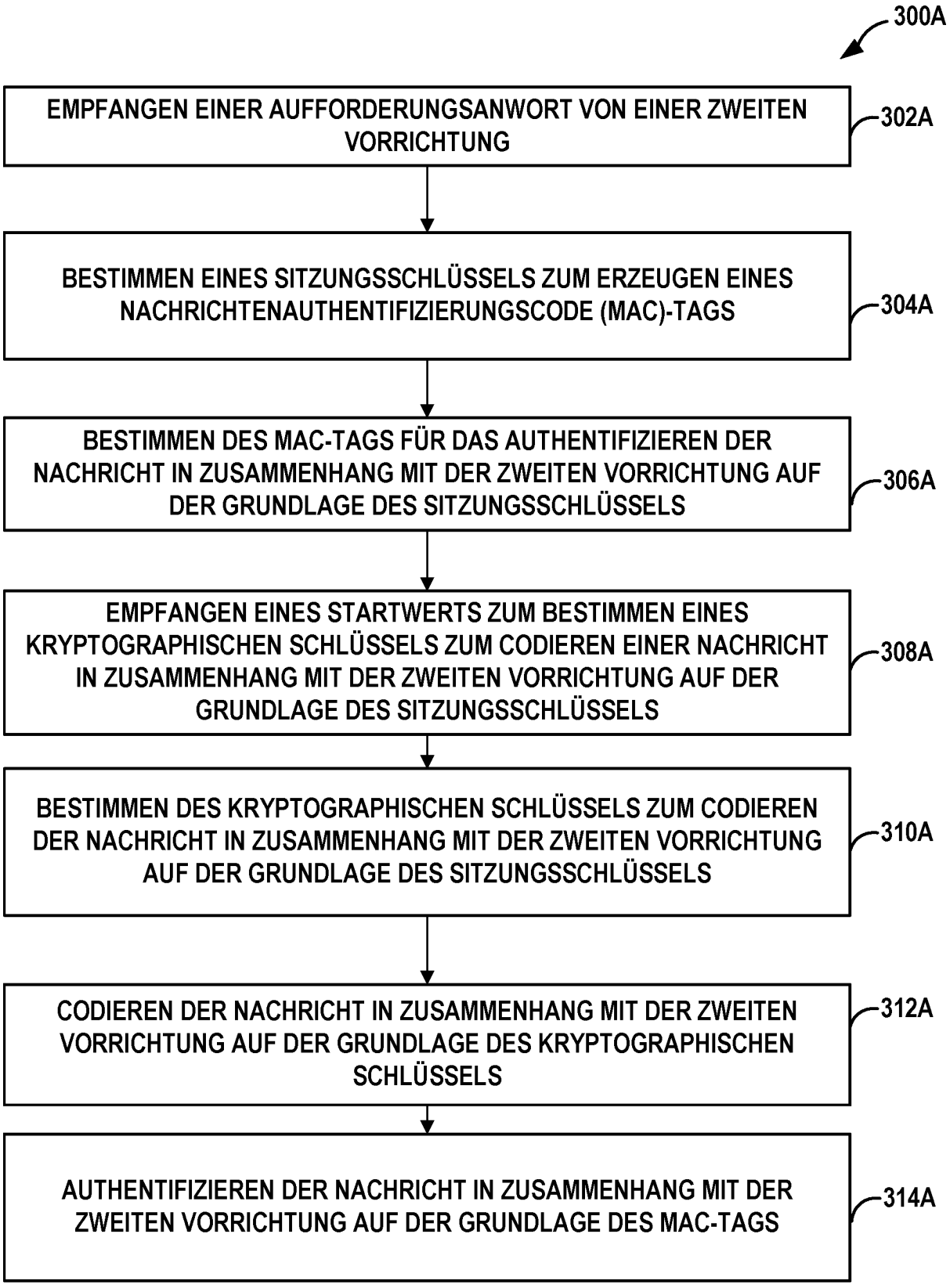

300A
EMPFANGEN EINER AUFFORDERUNGSANWORT VON EINER ZWEITEN VORRICHTUNG
302A
BESTIMMEN EINES SITZUNGSSCHLÜSSELS ZUM ERZEUGEN EINES NACHRICHTENAUTHENTIFIZIERUNGSCODE (MAC)-TAGS
304A
BESTIMMEN DES MAC-TAGS FÜR DAS AUTHENTIFIZIEREN DER NACHRICHT IN ZUSAMMENHANG MIT DER ZWEITEN VORRICHTUNG AUF DER GRUNDLAGE DES SITZUNGSSCHLÜSSELS
306A
EMPFANGEN EINES STARTWERTS ZUM BESTIMMEN EINES KRYPTOGRAPHISCHEN SCHLÜSSELS ZUM CODIEREN EINER NACHRICHT IN ZUSAMMENHANG MIT DER ZWEITEN VORRICHTUNG AUF DER GRUNDLAGE DES SITZUNGSSCHLÜSSELS
308A
BESTIMMEN DES KRYPTOGRAPHISCHEN SCHLÜSSELS ZUM CODIEREN DER NACHRICHT IN ZUSAMMENHANG MIT DER ZWEITEN VORRICHTUNG AUF DER GRUNDLAGE DES SITZUNGSSCHLÜSSELS
310A
CODIEREN DER NACHRICHT IN ZUSAMMENHANG MIT DER ZWEITEN VORRICHTUNG AUF DER GRUNDLAGE DES KRYPTOGRAPHISCHEN SCHLÜSSELS
312A
AUTHENTIFIZIEREN DER NACHRICHT IN ZUSAMMENHANG MIT DER ZWEITEN VORRICHTUNG AUF DER GRUNDLAGE DES MAC-TAGS
314A

FIG. 3A

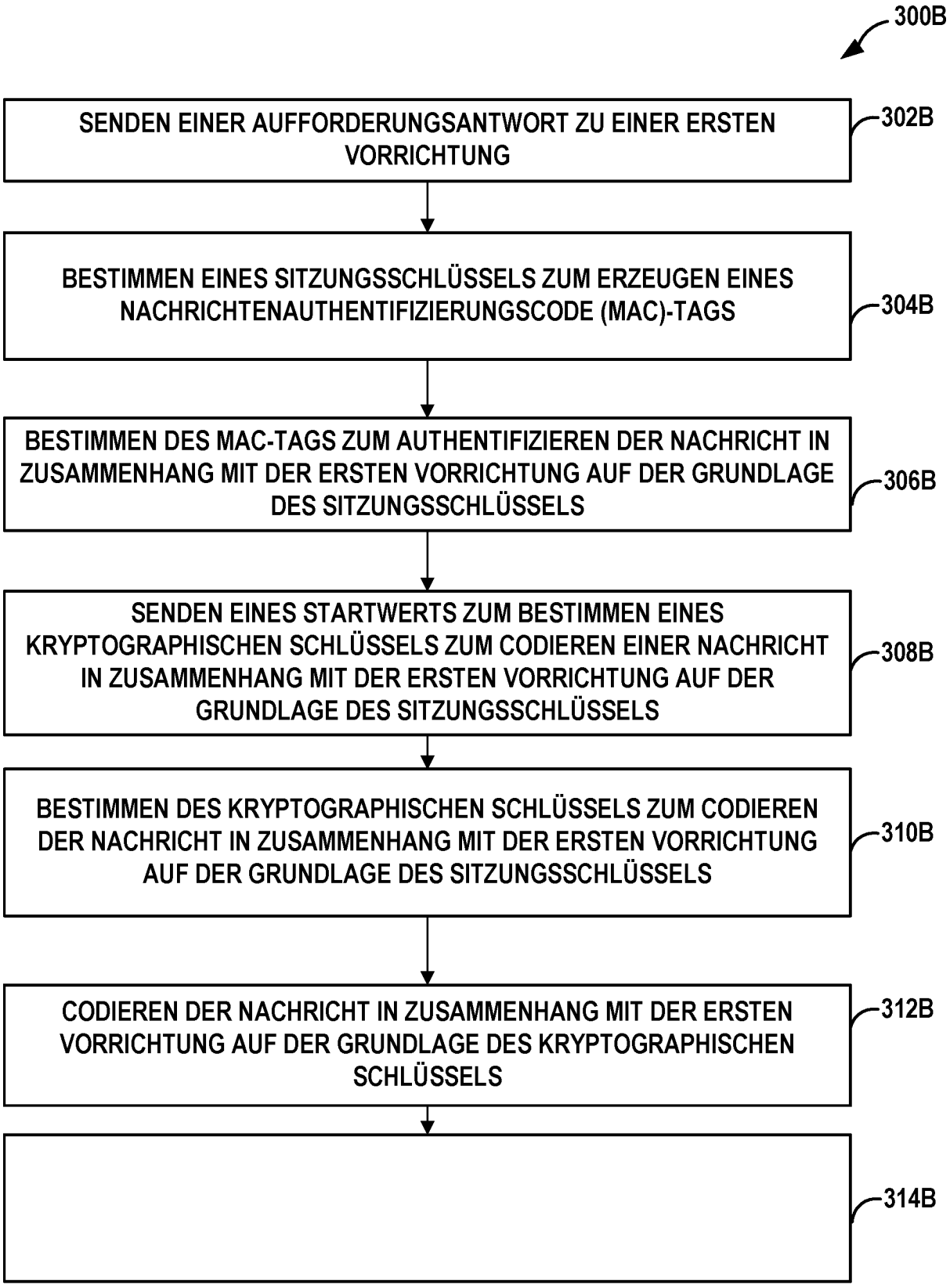

300B
SENDEN EINER AUFFORDERUNGSANTWORT ZU EINER ERSTEN VORRICHTUNG
302B
BESTIMMEN EINES SITZUNGSSCHLÜSSELS ZUM ERZEUGEN EINES NACHRICHTENAUTHENTIFIZIERUNGSCODE (MAC)-TAGS
304B
BESTIMMEN DES MAC-TAGS ZUM AUTHENTIFIZIEREN DER NACHRICHT IN ZUSAMMENHANG MIT DER ERSTEN VORRICHTUNG AUF DER GRUNDLAGE DES SITZUNGSSCHLÜSSELS
306B
SENDEN EINES STARTWERTS ZUM BESTIMMEN EINES KRYPTOGRAPHISCHEN SCHLÜSSELS ZUM CODIEREN EINER NACHRICHT IN ZUSAMMENHANG MIT DER ERSTEN VORRICHTUNG AUF DER GRUNDLAGE DES SITZUNGSSCHLÜSSELS
308B
BESTIMMEN DES KRYPTOGRAPHISCHEN SCHLÜSSELS ZUM CODIEREN DER NACHRICHT IN ZUSAMMENHANG MIT DER ERSTEN VORRICHTUNG AUF DER GRUNDLAGE DES SITZUNGSSCHLÜSSELS
310B
CODIEREN DER NACHRICHT IN ZUSAMMENHANG MIT DER ERSTEN VORRICHTUNG AUF DER GRUNDLAGE DES KRYPTOGRAPHISCHEN SCHLÜSSELS
312B
314B

FIG. 3B

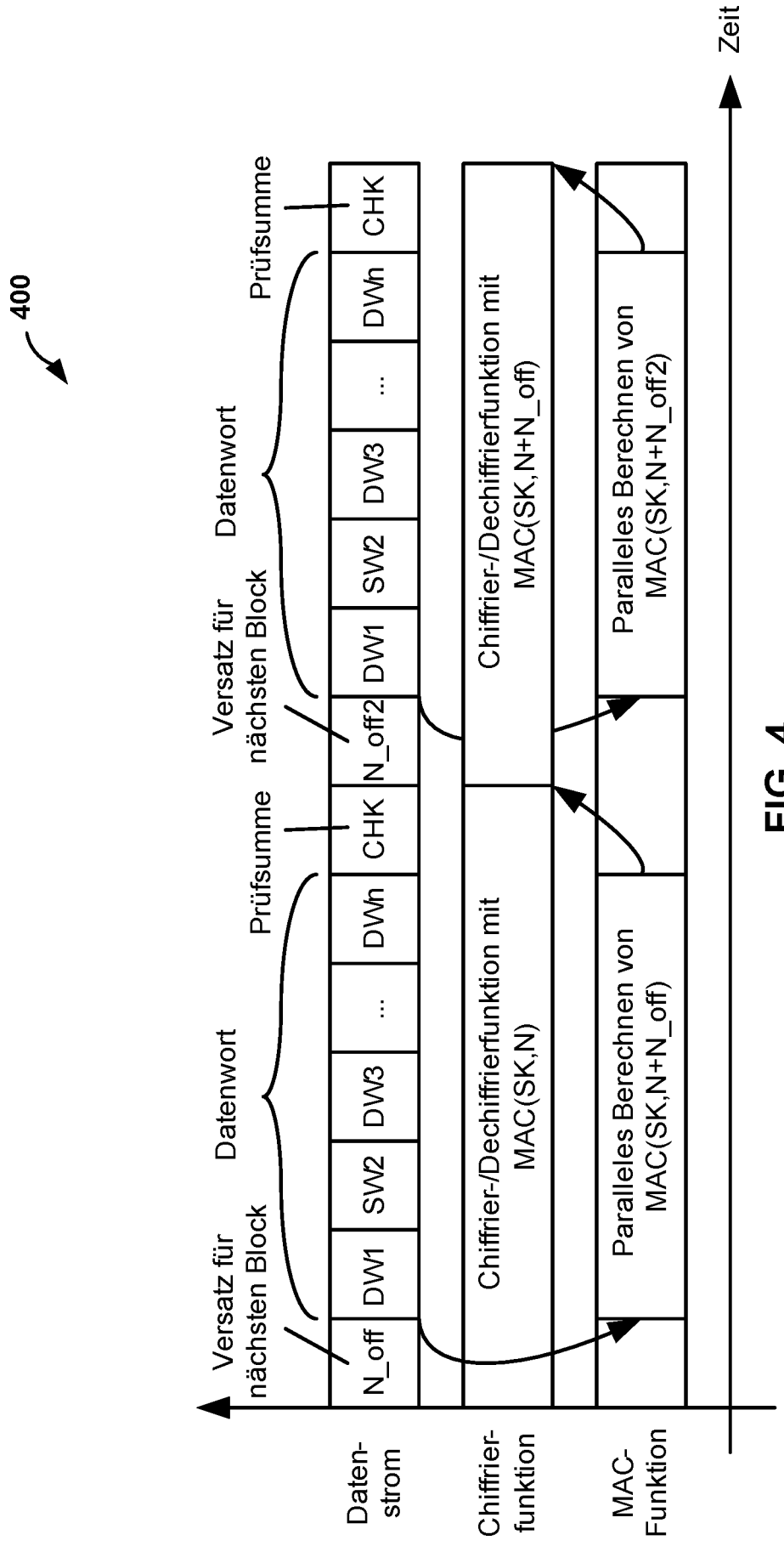

400
Zeit
Daten-strom
Chiffrier-funktion
MAC-Funktion
Versatz für nächsten Block
Datenwort
Prüfsumme
N_off
DW1
SW2
DW3
...
DWn
CHK
N_off2
Chiffrier-/Dechiffrierfunktion mit MAC(SK,N)
Chiffrier-/Dechiffrierfunktion mit MAC(SK,N+N_off)
Paralleles Berechnen von MAC(SK,N+N_off)
Paralleles Berechnen von MAC(SK,N+N_off2)

FIG. 4

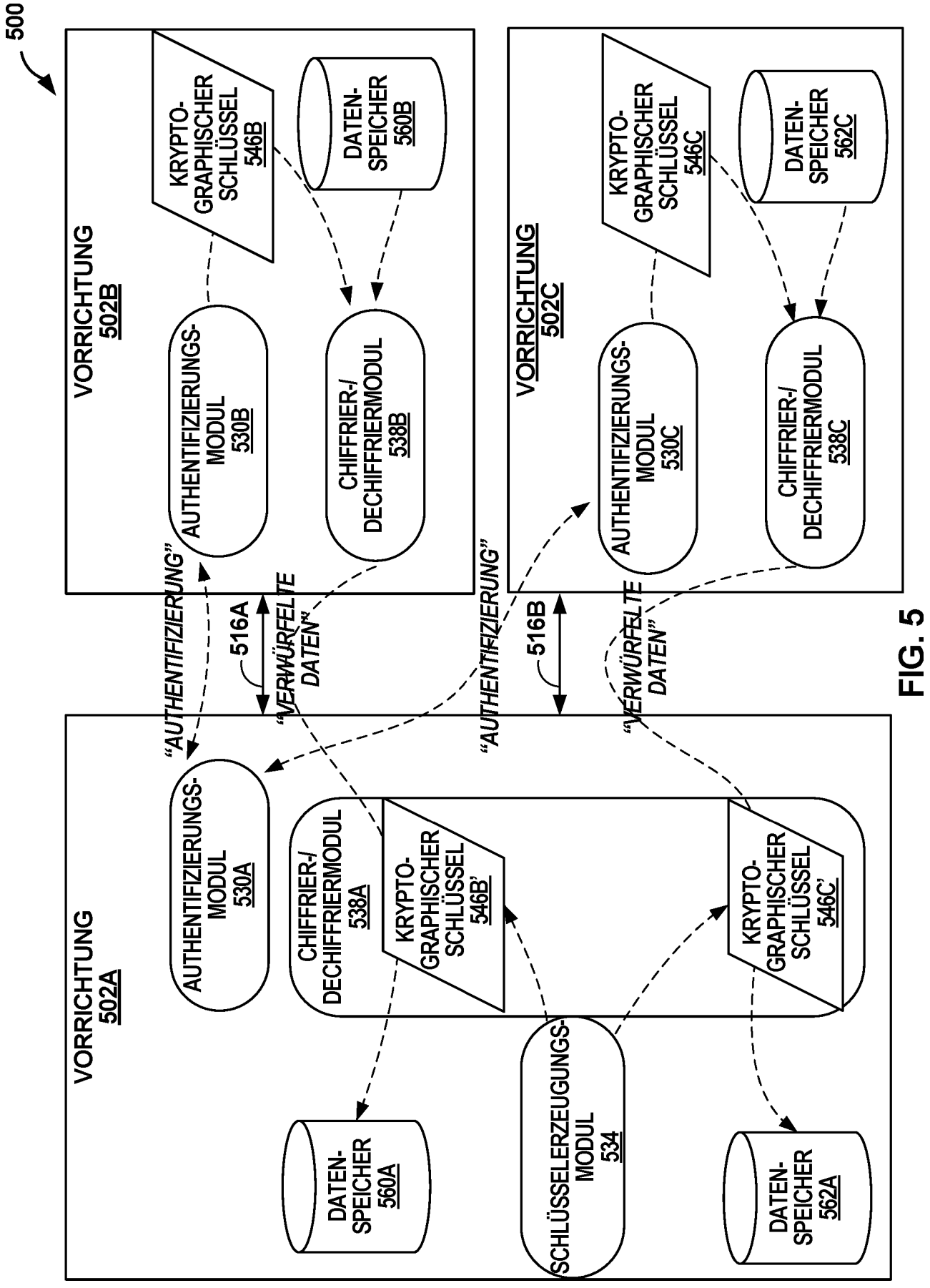

500
VORRICHTUNG 502A
VORRICHTUNG 502B
VORRICHTUNG 502C
AUTHENTIFIZIERUNGS-MODUL 530A
AUTHENTIFIZIERUNGS-MODUL 530B
AUTHENTIFIZIERUNGS-MODUL 530C
CHIFFRIER-/DECHIFFRIERMODUL 538A
CHIFFRIER-/DECHIFFRIERMODUL 538B
CHIFFRIER-/DECHIFFRIERMODUL 538C
KRYPTO-GRAPHISCHER SCHLÜSSEL 546B'
KRYPTO-GRAPHISCHER SCHLÜSSEL 546B
KRYPTO-GRAPHISCHER SCHLÜSSEL 546C
KRYPTO-GRAPHISCHER SCHLÜSSEL 546C'
SCHLÜSSELERZEUGUNGS-MODUL 534
DATEN-SPEICHER 560A
DATEN-SPEICHER 560B
DATEN-SPEICHER 562A
DATEN-SPEICHER 562C
516A
516B
"AUTHENTIFIZIERUNG"
"VERWÜRFELTE DATEN"
"AUTHENTIFIZIERUNG"
"VERWÜRFELTE DATEN"

FIG. 5

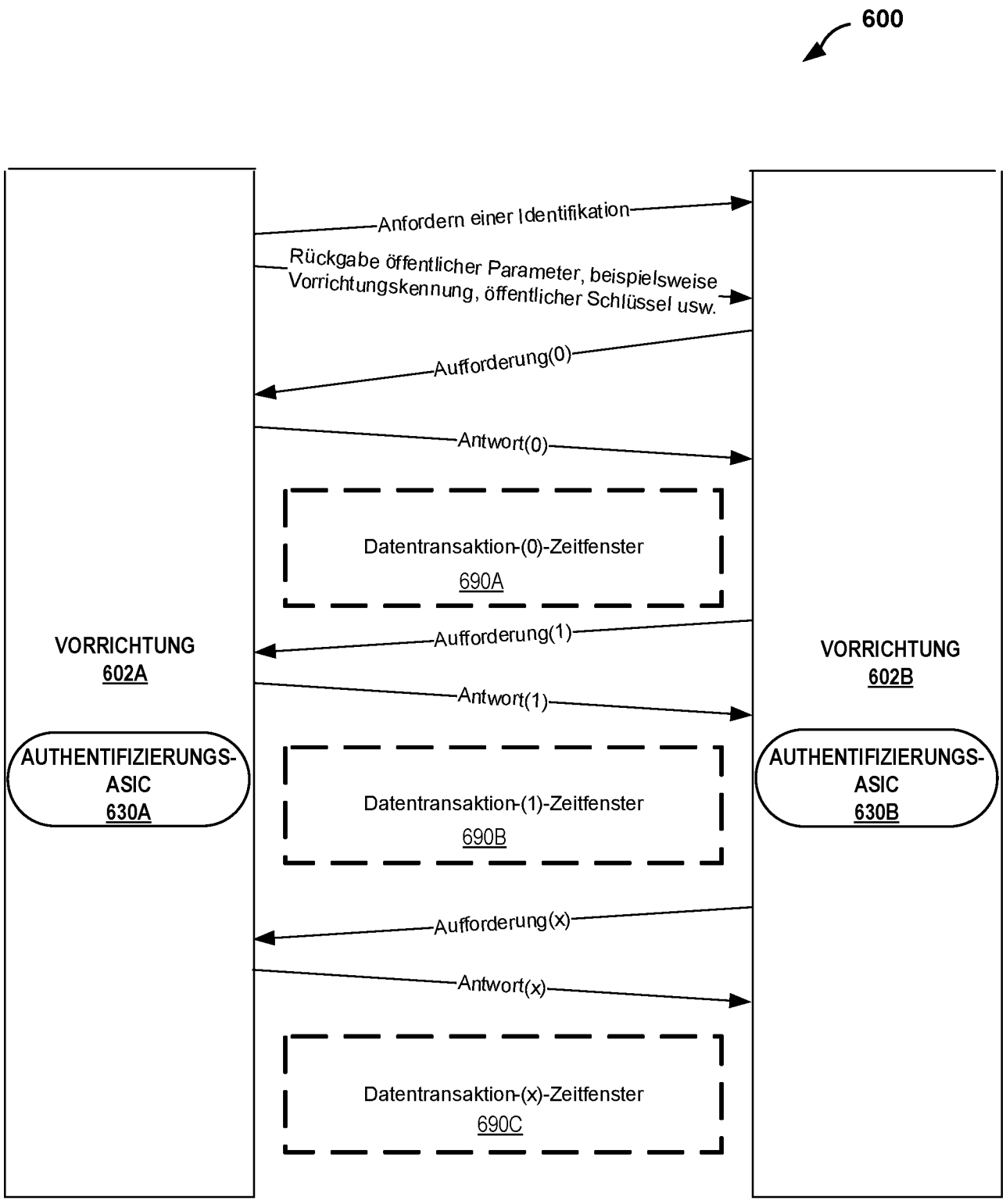

600
VORRICHTUNG
602A
AUTHENTIFIZIERUNGS-
ASIC
630A
VORRICHTUNG
602B
AUTHENTIFIZIERUNGS-
ASIC
630B
Anfordern einer Identifikation
Rückgabe öffentlicher Parameter, beispielsweise Vorrichtungskennung, öffentlicher Schlüssel usw.
Aufforderung(0)
Antwort(0)
Datentransaktion-(0)-Zeitfenster
690A
Aufforderung(1)
Antwort(1)
Datentransaktion-(1)-Zeitfenster
690B
Aufforderung(x)
Antwort(x)
Datentransaktion-(x)-Zeitfenster
690C

FIG. 6

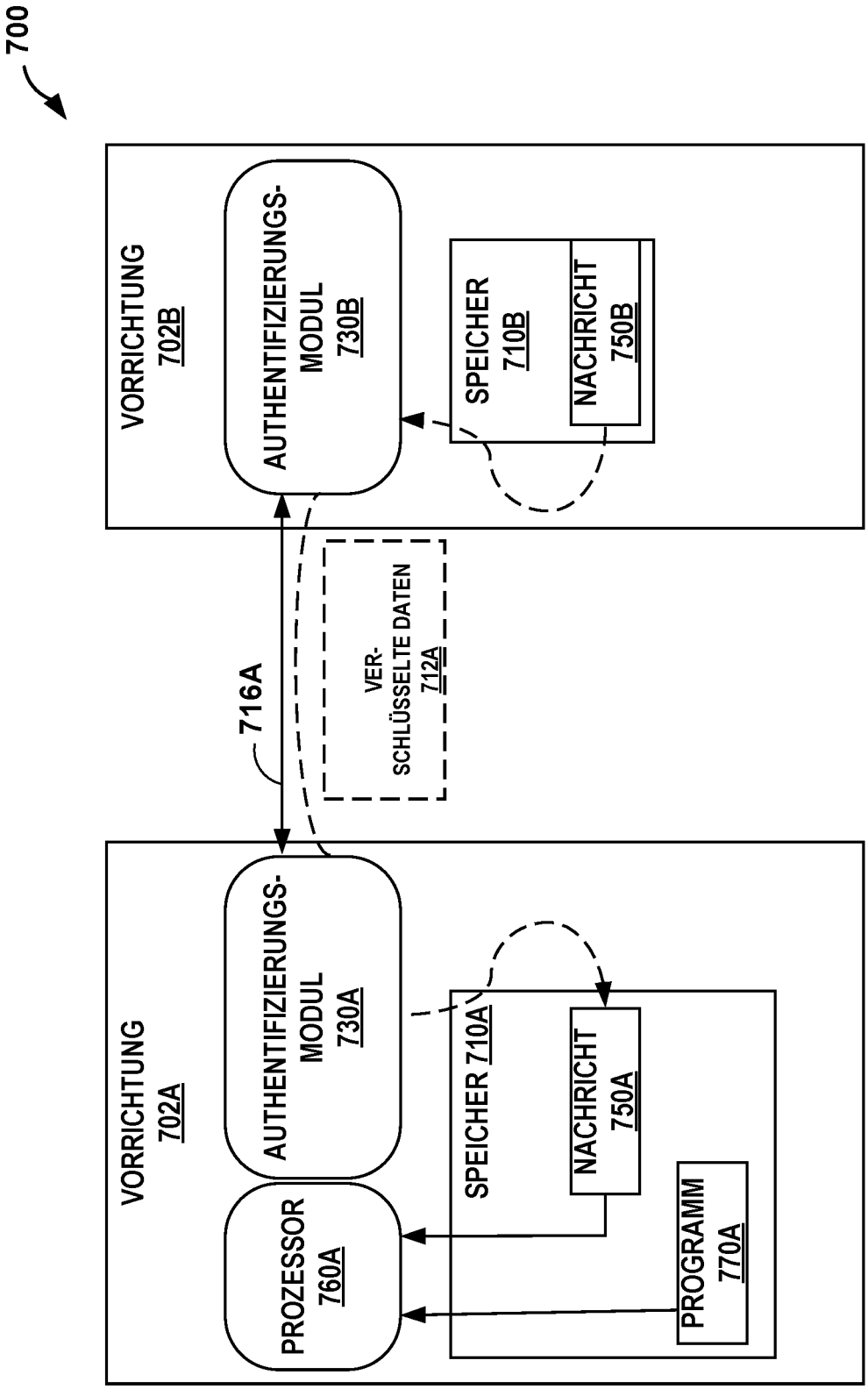

700
VORRICHTUNG 702B
AUTHENTIFIZIERUNGS-MODUL 730B
SPEICHER 710B
NACHRICHT 750B
716A
VER-SCHLÜSSELTE DATEN 712A
VORRICHTUNG 702A
AUTHENTIFIZIERUNGS-MODUL 730A
PROZESSOR 760A
SPEICHER 710A
NACHRICHT 750A
PROGRAMM 770A

FIG. 7

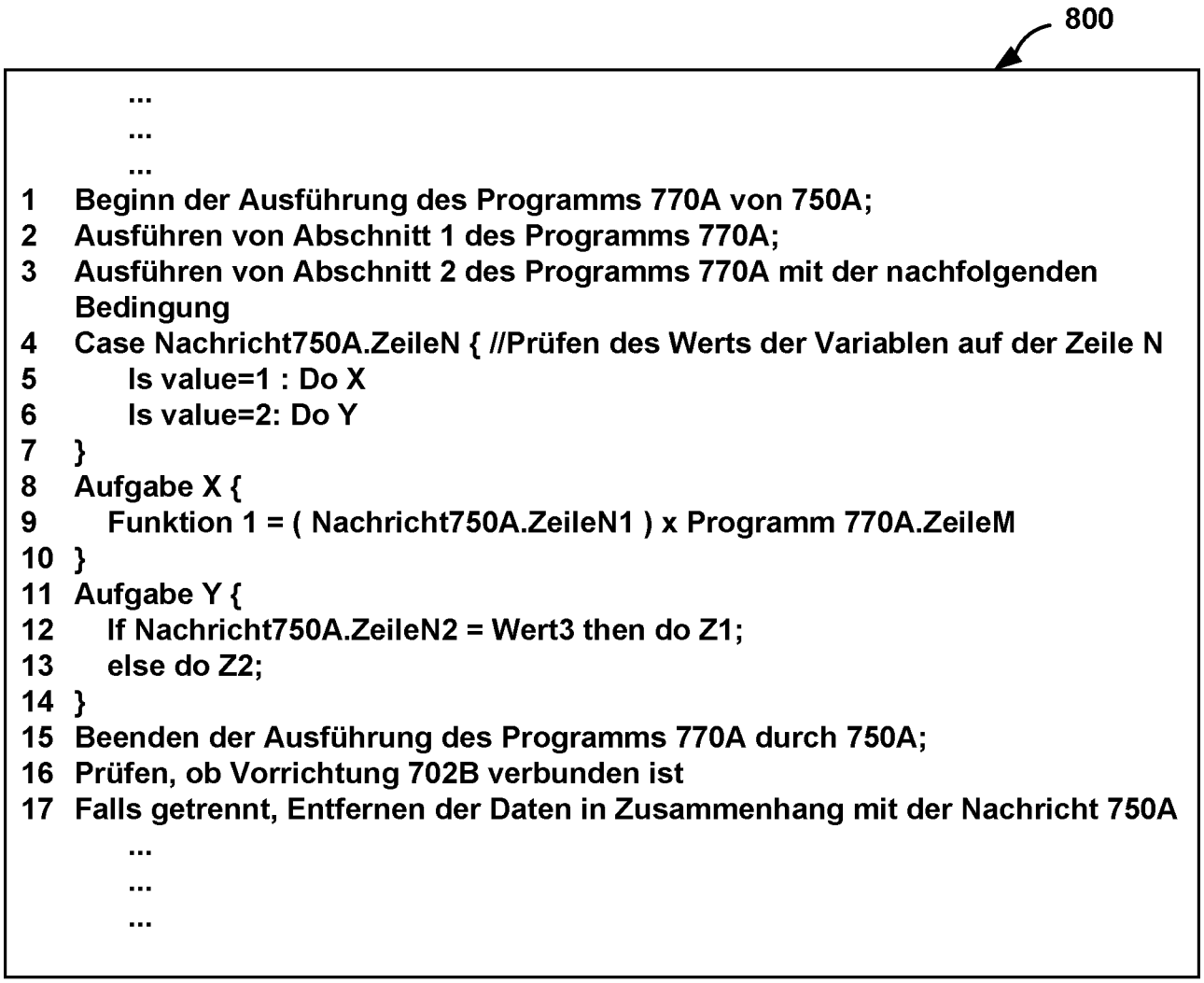

800
...
...
...
1 Beginn der Ausführung des Programms 770A von 750A;
2 Ausführen von Abschnitt 1 des Programms 770A;
3 Ausführen von Abschnitt 2 des Programms 770A mit der nachfolgenden Bedingung
4 Case Nachricht750A.ZeileN { //Prüfen des Werts der Variablen auf der Zeile N
5 Is value=1 : Do X
6 Is value=2: Do Y
7 }
8 Aufgabe X {
9 Funktion 1 = (Nachricht750A.ZeileN1) x Programm 770A.ZeileM
10 }
11 Aufgabe Y {
12 If Nachricht750A.ZeileN2 = Wert3 then do Z1;
13 else do Z2;
14 }
15 Beenden der Ausführung des Programms 770A durch 750A;
16 Prüfen, ob Vorrichtung 702B verbunden ist
17 Falls getrennt, Entfernen der Daten in Zusammenhang mit der Nachricht 750A
...
...
...

FIG. 8

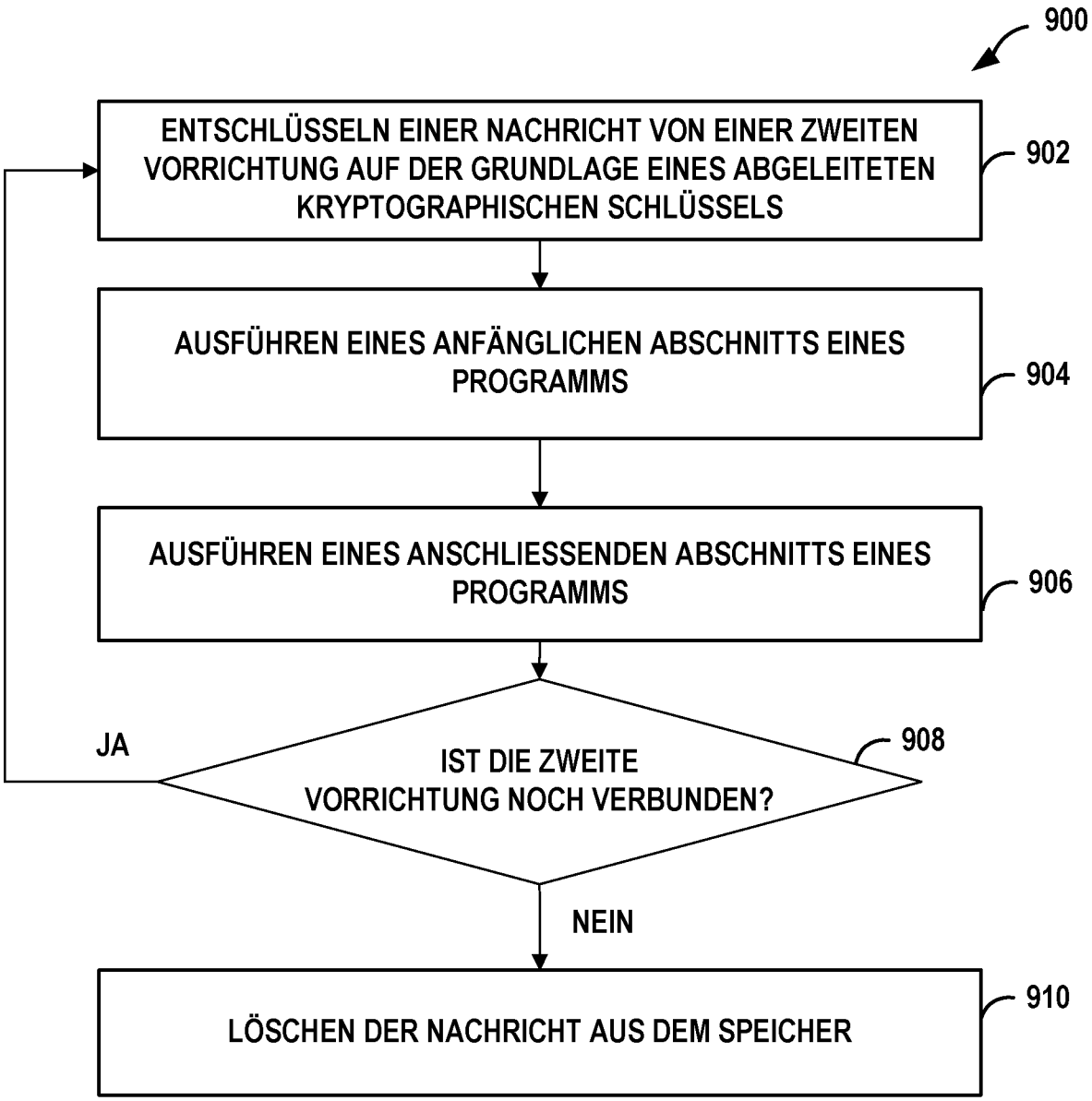

900
ENTSCHLÜSSELN EINER NACHRICHT VON EINER ZWEITEN VORRICHTUNG AUF DER GRUNDLAGE EINES ABGELEITETEN KRYPTOGRAPHISCHEN SCHLÜSSELS
902
AUSFÜHREN EINES ANFÄNGLICHEN ABSCHNITTS EINES PROGRAMMS
904
AUSFÜHREN EINES ANSCHLIESSENDEN ABSCHNITTS EINES PROGRAMMS
906
IST DIE ZWEITE VORRICHTUNG NOCH VERBUNDEN?
908
JA
NEIN
LÖSCHEN DER NACHRICHT AUS DEM SPEICHER
910

FIG. 9