(19) Deutsches Patent- und Markenamt

(10) **DE 10 2010 011 022 A1** 2012.02.16

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2010 011 022.1**
(22) Anmeldetag: **11.03.2010**
(43) Offenlegungstag: **16.02.2012**

(51) Int Cl.: ***H04L 9/30*** (2006.01)

(71) Anmelder:
Siemens Aktiengesellschaft, 80333, München, DE

(72) Erfinder:
Falk, Rainer, Dr., 85435, Erding, DE; Fries, Steffen, 85598, Baldham, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

US 72 78 582 B1

Brackin, S.: "Automatically Detecting Most Vulnerabilities in Cryptographic Protocols". In: IEEE, Proceedings of DARPA Information Survivability Conference and Exposition, 2000. 25.-27 .01.2000, Vol. 1, Seiten 222-236

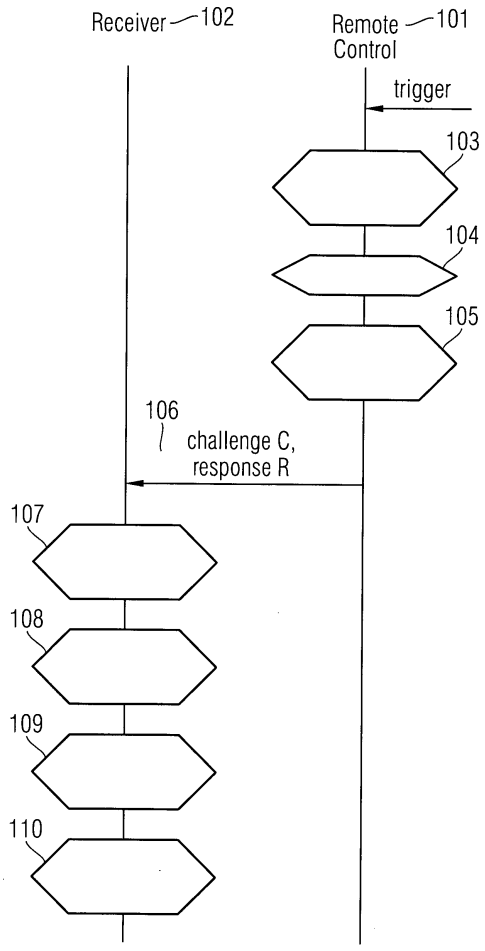
Clark, J., Jacob, J.: "A Survey of Authentication Protocol Literature: Version 1.0", 17.11.1997. Am 26.10.2010 im Internet gefunden unter folgendem Link http://www.eis.mdx.ac.uk/staffpages /m_cheng/Link/clarkjacob.pdf

Menezes, A., van Oorschot, P., Vanstone, S.: Handbook of Applied Cryptogrphy", CRC Press, 1997, Seiten 385-435

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren zur sicheren unidirektionalen Übertragung von Signalen**



(57) Zusammenfassung: Unidirektionale Übertragungen von Signalen werden beispielsweise bei Fernbedienungen zum Aussenden eines Steuerkommandos verwendet, da in diesen Fällen üblicherweise keine Antwortnachricht benötigt wird. Auch bei einer unidirektionalen Übertragung besteht jedoch in den meisten Anwendungsfällen die Anforderung einer sicheren und manipulationsgeschützten Übertragung der Signale. Die Erfindung schlägt ein Verfahren zur sicheren unidirektionalen Übertragung eines Signals unter Verwendung eines asymmetrischen Kryptographieverfahrens vor.

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren, einen Sender und einen Empfänger zur sicheren unidirektionalen Übertragung eines Signals unter Verwendung eines asymmetrischen Kryptographieverfahrens.

[0002] Unidirektionale Übertragungen von Signalen werden beispielsweise bei Fernbedienungen zum Aussenden eines Steuerkommandos verwendet, da in diesen Fällen üblicherweise keine Antwortnachricht benötigt wird. Beispiele für derartige Fernbedienungen sind Funkschlüssel zum Ver- und Entriegeln von Autos, drahtlose Garagentoröffner oder Fernbedienungen im Unterhaltungselektronikbereich. Weiterhin werden beispielsweise Statusinformationen, wie Temperatur oder Erschütterung, von drahtlosen Sensoren unidirektional übertragen. Eine solche unidirektionale Übertragung ist energiesparend, da lediglich eine einzelne Nachricht ausgesendet wird und vorab keine Verbindung aufgebaut werden muss. Zudem kann üblicherweise auf ein Empfangsteil verzichtet werden, was die entsprechenden Systeme preiswert in der Herstellung macht.

[0003] Auch bei einer unidirektionalen Übertragung besteht jedoch in den meisten Anwendungsfällen die Anforderung einer sicheren und manipulationsgeschützten Übertragung der Signale. Zur sicheren unidirektionalen Übertragung ist das so genannte Keeloq-Protokoll bekannt. In diesem Protokoll wird ein symmetrischer Schlüssel zur Verschlüsselung der gesendeten Signale verwendet. In einem symmetrischen Verschlüsselungsverfahren müssen Sender und Empfänger über den gleichen Schlüssel verfügen, damit der Sender die Nachricht mit diesem verschlüsseln und der Empfänger die Nachricht mit diesem entschlüsseln kann. Um einen neuen Sender bei einem Empfänger bekannt zu machen, müssen daher in einem geeigneten Verfahren ein spezifischer symmetrischer Schlüssel zwischen Sender um Empfänger vereinbart werden. In der Praxis werden Verfahren verwendet, bei dem ein symmetrischer Systemschlüssel beim Empfänger durch den Hersteller gespeichert wird. Anhand einer senderspezifischen Information, wie beispielsweise einer Seriennummer, kann dann ein senderspezifischer Schlüssel durch den Empfänger berechnet werden. Hierzu überträgt der Sender in einer Anlernphase beispielsweise seine Seriennummer an den Empfänger, welcher daraufhin mit Hilfe des Systemschlüssels den senderspezifischen Schlüssel ermittelt. Auf Seiten des Senders ist der senderspezifische Schlüssel bereits durch den Hersteller gespeichert. Somit verfügen sowohl der Sender als auch der Empfänger nach dieser Anlernphase über einen gemeinsamen Schlüssel, mit dem die Nachrichten verschlüsselt beziehungsweise entschlüsselt werden können.

[0004] Problematisch bei einem solchen Verfahren ist jedoch, dass auf jedem Empfänger der Systemschlüssel hinterlegt ist. Ein Angreifer, der im Besitz nur eines Empfängers ist, kann den Systemschlüssel auslesen und mit diesem Wissen die Schlüssel eines beliebigen Senders nachbilden.

[0005] In einem weiteren Verfahren wird zur Vereinbarung eines symmetrischen Schlüssels zwischen Sender und Empfänger der Senderschlüssel in einer Anlernphase unverschlüsselt übertragen. Auch diese birgt jedoch die Gefahr, dass ein Angreifer in einer manipulierten Anlernphase den Senderschlüssel abhört.

[0006] Hiervon abgesehen ist in beiden Verfahren eine Anlernphase zu durchlaufen, die durch den Benutzer zu initiieren ist. Dies ist mit einem zusätzlichen Aufwand für den Benutzer verbunden, so dass die beschriebenen Verfahren durch die zusätzlich erforderliche Anlernphase fehleranfälliger und benutzerunfreundlicher werden.

[0007] Der vorliegenden Erfindung liegt somit die Aufgabe zugrunde, ein Verfahren zur unidirektionalen Übertragung von Signalen anzugeben, welches sicherer und benutzerfreundlicher als bisher bekannte Verfahren ist.

[0008] Diese Aufgabe wird durch ein Verfahren, einen Sender und einen Empfänger mit den Merkmalen der Ansprüche 1, 9 und 11 gelöst. Vorteilhafte Weiterbildungen der Erfindung sind in den abhängigen Ansprüchen angegeben.

[0009] Das erfindungsgemäße Verfahren zur Übertragung eines Signals mit einer unidirektionalen Kommunikationsverbindung wird durch ein asymmetrisches Kryptographieverfahren geschützt. Hierzu wird durch einen Sender ein Zählerwert bei einem Sendevorgang inkrementiert. Anschließend wird durch den Sender eine Challenge auf Basis des Zählerwertes und eines Steuerkommandos ermittelt und auf Basis der ermittelten Challenge wird wiederum eine Response ermittelt. Die Challenge und die Response werden von dem Sender an einen Empfänger übertragen. Erfindungsgemäß werden durch den Sender sowohl die Challenge als auch die zugehörigen Response ermittelt. Auf diese Weise kann ein asymmetrisches Kryptographieverfahren eingesetzt werden, welches üblicherweise für bidirektionale Kommunikationsverbindungen konzipiert wird. Bei dem Zähler handelt es sich z. B. um einen 16 Bit, 32 Bit oder 64 Bit Zähler. Die Response wird mittels eines asymmetrischen kryptographischen Verfahrens wie z. B. RSA, ECC (Elliptic Curve Cryptography) wie z. B. ECC-DSA, oder Diffie-Hellman unter Verwendung eines privaten asymmetrischen Schlüssels ermittelt. Unter Inkrementieren des Zählerwertes wird insbesondere ein erhöhen um den Wert 1 verstanden. Es kann

jedoch auch analog ein anderes Rechensystem zugrunde gelegt werden, bei dem z. B. rückwärts gezählt wird (also der Zählerwert um den Wert 1 verringert wird). Entsprechend ist es ebenso möglich, um andere Werte zu erhöhen (z. B. +2, +5, +7) oder um andere Werte zu verringern (z. B. –2, –5, –7). Auch können andere Rechenoperationen verwendet werden, z. B. ein Multiplizieren mit einem Wert (z. B. 2, 3, 5, 7), um den nächsten Zählerwert zu bestimmen. In einer anderen Variante wird als Zählerwert ein Zufallswert verwendet, wobei beim inkrementieren des Zählers ein neuer Zufallswert berechnet wird (z. B. durch eine Pseudozufallszahlenfolgengenerator).

[0010] In einer Weiterbildung der vorliegenden Erfindung wird die Nachricht umfassend die Challenge mehrmals übertragen, damit auch bei Übertragungsfehlern das Steuerkommando zuverlässig übermittelt wird. Dabei kann der Zählerwert mit jeder Nachricht erhöht werden oder mit jeder wiederholten Übertragung unverändert bleiben. Der Empfänger akzeptiert diesen gleichen Zählerwert, solange mit einer gewissen Häufigkeit Nachrichten mit diesem Zählerwert empfangen werden. Der Empfänger speichert in einer Variante einen Zähler-Referenzwert. Bei Empfang einer Nachricht prüft der Empfänger, ob der dabei verwendete Zählerwert gegenüber dem gespeicherten Zähler-Referenzwert inkrementiert ist. Nur bei einem einfach oder alternativ mehrfach inkrementierten Zählerwert wird ein in der Nachricht codiertes Steuerkommando ausgeführt. Dabei wird der Zähler-Referenzwert auf den in der Nachricht verwendeten Zählerwert gesetzt. Sobald für eine gewisse Zeitspanne keine Steuernachricht mit diesem Zählerwert empfangen wird, wird dieser Zählerwert ungültig. Zudem kann durch den Empfänger überprüft werden, ob das gleiche Steuerkommando mit diesem Zählerwert übertragen wird. Das in der Nachricht codierte Steuerkommando wird dabei für einen konstanten Zählerwert vorzugsweise nur einmal ausgeführt.

[0011] In einer weiteren Ausgestaltung der vorliegenden Erfindung speichert zur Initialisierung ein Empfänger eine Identifizierungsinformation eines Senders, wobei die Identifizierungsinformation zumindest eine Seriennummer des Empfängers umfasst. Die Identifizierungsinformation des Senders kann über eine Administrationsschnittstelle, wie beispielsweise eine serielle Schnittstelle, übertragen werden. Vorteilhafterweise kann der Empfänger mit Hilfe der empfangenen Identifizierungsinformation einen öffentlichen Schlüssel des Senders ermitteln. Auf Basis dieses öffentlichen Schlüssels ist es dem Empfänger möglich, eine von dem Sender empfangene Response sicher zu verifizieren. Folglich benötigt der Empfänger in vorteilhafter Weise kein geheimes Schlüsselmaterial, um die Nachrichten des Senders sicher zu überprüfen. Auch wenn ein Angreifer die Identifizierungsinformation oder den öffentlichen Schlüssel des Senders ermitteln würde, könnte er damit jedoch nicht Nachrichten des Senders nachbilden. Dazu würde der dem öffentlichen Schlüssel des Senders zugeordnete private Schlüssel des Senders benötigt.

[0012] In einer weiteren Ausgestaltung der vorliegenden Erfindung wird auf Basis der ermittelten Response ein Integritätsschlüssel durch den Sender abgeleitet, und zum Schutz der Integrität der Challenge eine kryptographische Prüfsumme mit dem Integritätsschlüssel über die Challenge ermittelt. Dies hat die vorteilhafte Wirkung, dass auch die Integrität der Challenge bei der unidirektionalen Übertragung gewährleistet wird. Die kryptographische Prüfsumme kann über die gesamte Challenge oder über einen Teil der Challenge berechnet werden.

[0013] In dem erfindungsgemäßen Verfahren zur Überprüfung eines derart geschützten übertragenen Signals werden durch einen Empfänger die übertragene Challenge und die zugehörige Response empfangen. Die empfangene Challenge wird daraufhin überprüft, ob der in der Challenge verwendete Zählerwert größer als ein bisher von dem übertragenen Sender gespeicherter Zählerwert ist. Die empfangene Response wird auf Basis der Challenge überprüft. Nach erfolgreicher Überprüfung von Challenge und Response wird das in der Challenge übermittelte Steuerkommando ausgeführt.

[0014] Der erfindungsgemäße Sender weist Mittel zum Durchführen des erfindungsgemäßen Verfahrens zur Übertragung eines Signals mit einer unidirektionalen Kommunikationsverbindung geschützt durch ein asymmetrisches Kryptographieverfahren auf.

[0015] In einer Weiterbildung weist der Sender ein Sicherheitsmodul zur effizienten und sicheren Ausführung kryptographischer Operationen auf. Das Sicherheitsmodul umfasst Mittel zum Schutz sowohl gegen softwaretechnische als auch gegen physikalische Angriffe oder Seitenkanalangriffe.

[0016] Der erfindungsgemäße Empfänger umfasst Mittel geeignet zum Durchführen eines Verfahrens zur Überprüfung eines unidirektional übertragenen Signals geschützt durch ein asymmetrisches Kryptographieverfahren.

[0017] Im Folgenden werden bevorzugte Ausführungsformen des erfindungsgemäßen Verfahrens und des erfindungsgemäßen Senders und Empfängers unter Bezugnahme auf die beigefügten Figuren zur Erläuterung erfindungswesentlicher Merkmale beschrieben. Es zeigen

[0018] Fig. 1 ein Ablaufdiagramm eines erfindungsgemäßen Verfahrens zur sicheren unidirektionalen Übertragung eines Signals,

[0019] Fig. 2 ein Ablaufdiagramm einer Variante mit einem Sicherheitsmodul eines erfindungsgemäßen Verfahrens zur sicheren unidirektionalen Übertragung eines Signals,

[0020] Fig. 3 ein Ablaufdiagramm einer weiteren Variante mit einem zusätzlichen Integritätsschutz der übertragenen. Challenge eines erfindungsgemäßen Verfahrens zur sicheren unidirektionalen Übertragung eines Signals.

[0021] Die Fig. 1 zeigt in einem Ablaufdiagramm ein erfindungsgemäßes Verfahren zur sicheren Übertragung eines Signals. Die Übertragung erfolgt hierbei nur in eine Richtung, also unidirektional, von einem Sender **101** zu einem Empfänger **102**.

[0022] Der Sender **101** ermittelt in einem ersten Schritt **103** eine Challenge, welche einen Zählerwert und ein Steuerkommando Umfasst. Der Zählerwert wird bei jedem Sendevorgang inkrementiert und dient zur Verhinderung von Replayattacken, bei denen eine abgehörte Nachricht durch einen Angreifer gesendet wird. Das Steuerkommando ist beispielsweise bei einer Fernbedienung für einen Fernseher ein Kommando zum Ein- oder Ausschalten des Gerätes oder ein Kommando zum Verändern der Lautstärke. Bei drahtlosen Sensoren ist das Steuerkommando beispielsweise ein Sensorwert wie Temperatur oder Druck.

[0023] Im nächsten Schritt **104** wird der Zählerwert des Senders inkrementiert. Anschließend ermittelt der Sender **101** auf Basis der ermittelten Challenge eine Response **105**. Die ermittelte Challenge sowie die ermittelte Response werden anschließend vom Sender **101** an den Empfänger **102** übertragen **106**.

[0024] Der Empfänger **102** überprüft nun in einem ersten Schritt **107**, ob die erhaltene Response zur erhaltenen Challenge passt. In einem nächsten Schritt überprüft der Sender **102**, ob die erhaltene Challenge gültig ist **108**. Hierbei wird beispielsweise geprüft, ob der von der Challenge umfasste Zählerwert des Senders größer ist als der bisher von diesem Sender empfangene Zählerwert. Ist sowohl die Überprüfung der Response als auch die Überprüfung der Challenge erfolgreich, wird die im Empfänger **102** hinterlegte Referenzinformation des Senders **101** angepasst **109**. Dazu wird beispielsweise der für diesen Sender gespeicherte Zählerwert inkrementiert. Schließlich wird das von der Challenge umfasste Steuerkommando ausgeführt **110**.

[0025] Sollte die Überprüfung der Response oder der Challenge jedoch erfolglos sein, wird die Referenzinformation des betreffenden Senders nicht angepasst und das entsprechende Steuerkommando nicht ausgeführt.

[0026] Es liegt selbstverständlich im Ermessen eines Fachmanns, die dargestellten Verfahrensschritte in einer anderen Reihenfolge oder zumindest teilweise parallel durchzuführen.

[0027] Die Sicherheit von asymmetrischen Kryptographieverfahren basiert auf der Verwendung eines privaten und eines öffentlichen Schlüssels. Der private, geheime Schlüssel steht dabei nur dem Prüfling zur Verfügung, während der öffentliche Schlüssel im Prinzip jedermann zugänglich sein kann. In dem beschriebenen Verfahren basiert die Sicherheit also darauf, dass die Response aus der Challenge lediglich mit Kenntnis des privaten Schlüssels ermittelt werden kann. Kenntnis von dem privaten Schlüssel hat jedoch nur der Sender. Mit dem öffentlichen Schlüssel hingegen kann lediglich überprüft werden, ob eine Response zu einer Challenge passt und somit der Sender Kenntnis von dem privaten Schlüssel hatte. Mit dem öffentlichen Schlüssel ist es jedoch nicht möglich, auf Basis einer Challenge eine dazugehörige Response zu ermitteln. Daher wäre es völlig unproblematisch, wenn der im Besitz des Empfängers befindliche öffentliche Schlüssel durch einen Angreifer ermittelt würde.

[0028] In einer weiteren Ausgestaltung der vorliegenden Erfindung wird die Nachricht umfassend die Challenge mehrmals übertragen, damit auch bei Übertragungsfehlern das Steuerkommando zuverlässig vom Empfänger erkannt werden kann. Dabei kann der Zählerwert mit jeder Nachricht erhöht werden oder beim wiederholten Senden der Nachricht unverändert bleiben.

[0029] Beim wiederholten Senden einer Nachricht mit unverändertem Zählerwert akzeptiert der Empfänger diesen gleichen Zählerwert, solange mit einer gewissen vorgebbaren Häufigkeit Nachrichten mit diesem Zählerwert empfangen werden. Sobald für eine vorgebbare Zeitspanne keine Nachricht mit diesem Zählerwert empfangen wird, wird dieser Zählerwert ungültig. Zusätzlich kann überprüft werden, ob das gleiche Steuerkommando mit diesem Zählerwert übertragen wird.

[0030] Um einen Empfänger mit einem Sender vertraut zu machen, wird in einer Anlernphase eine Identifizierungsinformation des Senders an den Empfänger übermittelt. Die Identifizierungsinformation ist beispielsweise eine Seriennummer, ein digitales Zertifikat umfassend den öffentlichen Schlüssel oder der öffentliche Schlüssel selbst.

[0031] Die Identifizierungsinformation des Senders kann beim Anlernen über eine Administrationsschnittstelle, beispielsweise über einen Personalcomputer mit einer seriellen Schnittstelle, eingegeben werden. In einem automatisierten Anlernverfahren wird der Empfänger in einen Anlernmodus ver-

setzt und speichert in diesem Zeitraum Identifizierungsinformationen derjenigen Sender, die ein Steuerkommando übertragen. Zum Initiieren des Anlernmodus dient beispielsweise eine spezielle Taste oder ein mechanischer Schlüsselschalter am Empfänger.

[0032] Die Identifizierungsinformation des Senders wird vom Empfänger direkt abgespeichert oder erst nach einer Gültigkeitsprüfung, beispielsweise eines digitalen Zertifikats.

[0033] Die Fig. 2 zeigt in einem Ablaufdiagramm ein erfindungsgemäßes Verfahren zur sicheren Übertragung eines Signals mit einem Sicherheitsmodul. Die Übertragung erfolgt hierbei nur in eine Richtung, also unidirektional, von einem Sender **201** zu einem Empfänger **202**.

[0034] Zur Vermeidung von Wiederholungen wird im Folgenden bei gleichen Verfahrensschritten in der Fig. 2 auf die entsprechenden Beschreibungsteile in der Fig. 1 verwiesen. Zur Kennzeichnung sind gleiche Verfahrensschritte in Fig. 2 mit den gleichen Bezugszeichen wie in Fig. 1 versehen.

[0035] Im Unterschied zu dem in Fig. 1 gezeigten Verfahren wird in dem Verfahren gemäß Fig. 2 zur Ermittlung der Response im Sender ein Sicherheitsmodul **203** verwendet. Das Sicherheitsmodul **203** ist zur effizienten und sicheren Ausführung kryptographischer Operationen ausgelegt und weist Mittel zum Schutz sowohl gegen softwaretechnische als auch gegen physikalische Angriffe oder Seitenkanalangriffe auf.

[0036] Hierzu wird nach einer Inkrementierung des Zählerwertes **104** die ermittelte Challenge dem Sicherheitsmodul **203** zur Verfügung gestellt. Anschließend ermittelt das Sicherheitsmodul **203** des Senders **201** auf Basis der ermittelten Challenge eine Response **205**. Die ermittelte Response wird wiederum durch das Sicherheitsmodul **203** dem Sender zur Verfügung gestellt **206**.

[0037] Die ermittelte Challenge sowie die ermittelte Response werden schließlich vom Sender **201** an den Empfänger **202** übertragen **106**. Der übrige Verfahrenablauf entspricht dann wieder dem aus Fig. 1 bekannten Verfahrensablauf. Es ist auch möglich, das Sicherheitsmodul mit einem entsprechenden Zählerwert zu initialisieren und die Inkrementierung direkt im Sicherheitsmodul vorzunehmen. Die hat den Vorteil, dass der Zählerwert nicht manipuliert werden kann.

[0038] Die Fig. 3 zeigt in einem Ablaufdiagramm ein erfindungsgemäßes Verfahren zur sicheren Übertragung eines Signals mit einem zusätzlichen Integritätsschutz für die übertragene Challenge. Die Übertragung erfolgt hierbei nur in eine Richtung, also unidirektional, von einem Sender **301** zu einem Empfänger **302**.

[0039] Zur Vermeidung von Wiederholungen wird im Folgenden bei gleichen Verfahrensschritten in der Fig. 3 auf die entsprechenden Beschreibungsteile in der Fig. 1 verwiesen. Zur Kennzeichnung sind gleiche Verfahrensschritte in Fig. 3 mit den gleichen Bezugszeichen wie in Fig. 1 versehen.

[0040] In dieser Ausgestaltung des erfindungsgemäßen Verfahrens wird die Challenge unter Verwendung des Responsewertes geschützt übertragen. Dazu wird aus dem Responsewert ein symmetrischer Schlüssel abgeleitet oder der Responsewert direkt als symmetrischer Schlüssel verwendet **303**. Die Ableitung kann dabei beispielsweise durch eine Hashfunktion erfolgen. Mit diesem ermittelten symmetrischen Schlüssel wird eine kryptographische Prüfsumme berechnet **304**, welche den Zählerwert und das Steuerkommando umfasst. Beispiele für eine Hashfunktion sind MD6, SHA-1, SHA-256. Die Prüfsumme kann z. B. mittels einer HMAC-MD5, HMAC-SHA1, HMAC256, oder AES-CBC-MAC Funktion berechnet werden.

[0041] Die Challenge und die Prüfsumme werden durch den Sender an den Empfänger übermittelt **305**. Der Empfänger speichert nun die Challenge samt Prüfsumme und ermittelt ein Zeitfenster für einen gültigen Empfangszeitraum der zugehörigen Response **306**. Der Sender **301** startet eine Zeitmessung **307** und übermittelt die Response an den Empfänger in dem gültigen Zeitfenster **308**. Um die Sicherheit weiter zu erhöhen, wird also in diesem Ausführungsbeispiel zuerst die Challenge und Prüfsumme gesendet und erst zu einem späteren Zeitpunkt die Response.

[0042] Der Empfänger **302** überprüft nun in einem ersten Schritt **309**, ob die erhaltene Challenge gültig ist. Hierbei wird beispielsweise geprüft, ob der von der Challenge umfasste Zählerwert des Senders größer ist als der bisher von diesem Sender empfangene Zählerwert. Weiterhin ermittelt der Empfänger **302** nun seinerseits auf Grundlage der erhaltenen Response den symmetrischen Schlüssel. Hiernach überprüft der Empfänger anhand des symmetrischen Schlüssels ob die empfangene Challenge zu der empfangenen Prüfsumme passt.

[0043] Dann überprüft der Empfänger, ob die erhaltene Response zur Challenge passt **310**. Schließlich überprüft der Empfänger zusätzlich, ob die Response in dem gültigen Zeitfenster empfangen wurde. Der übrige Verfahrenablauf entspricht dann wieder dem aus Fig. 1 bekannten Verfahrensablauf.

[0044] Es liegt selbstverständlich im Ermessen eines Fachmanns, die dargestellten Verfahrensschritte

in einer anderen Reihenfolge oder zumindest teilweise parallel durchzuführen.

[0045] Anwendungsfälle für die beschriebene Erfindung sind beispielsweise Bluetooth-Fußschalter für Medizingeräte, Garagentoröffner, Funkschlüssel für einen Gebäude- oder Fahrzeugzugang, Steuerung im Heimnetz (bspw. Jalousie- oder Lichtschalter).

Patentansprüche

1. Verfahren zur Übertragung eines Signals mit einer unidirektionalen Kommunikationsverbindung geschützt durch ein asymmetrisches Kryptographieverfahren, wobei durch einen Sender die folgenden Schritten ausgeführt werden:
– ein Zählerwert bei einem Sendevorgang inkrementiert wird,
– eine Challenge auf Basis des Zählerwertes und eines Steuerkommandos ermittelt wird,
– eine Response auf Basis der ermittelten Challenge ermittelt wird,
– die Challenge und die Response an einen Empfänger übertragen werden.

2. Verfahren nach Anspruch 1, wobei zur Erkennung von Übertragungsfehlern die Challenge wiederholt übertragen wird.

3. Verfahren nach Anspruch 2, wobei der Zählerwert mit jeder wiederholten Übertragung erhöht wird.

4. Verfahren nach Anspruch 2, wobei der Zählerwert mit jeder wiederholten Übertragung unverändert bleibt.

5. Verfahren nach Anspruch 1, wobei zur Initialisierung ein Empfänger eine Identifizierungsinformation eines Senders speichert, und die Identifizierungsinformation zumindest eine Seriennummer des Senders umfasst.

6. Verfahren nach Anspruch 5, wobei die Identifizierungsinformation ein digitales Zertifikat oder einen öffentlichen Schlüssel des Senders umfasst.

7. Verfahren nach Anspruch 1, wobei auf Basis der ermittelten Response ein Integritätsschlüssel abgeleitet wird, zum Schutz der Integrität der Challenge eine kryptographische Prüfsumme mit dem Integritätsschlüssel über die Challenge ermittelt wird.

8. Verfahren zur Überprüfung eines gemäß einem Verfahren nach den Ansprüchen 1 bis 7 übertragenen Signals, wobei durch einen Empfänger die folgenden Schritte ausgeführt werden:
– eine durch einen Sender übertragene Challenge und eine zugehörige Response empfangen werden,
– die empfangene Challenge daraufhin überprüft wird, ob der in der Challenge verwendete Zählerwert größer als ein bisher von dem übertragenden Sender gespeicherter Zählerwert ist,
– die empfangene Response auf Basis der überprüften Challenge überprüft wird,
– nach erfolgreicher Überprüfung von Challenge und Response das in der Challenge verwendete Steuerkommando ausgeführt wird.

9. Sender umfassend Mittel geeignet zum Durchführen eines Verfahrens nach den Ansprüchen 1–7.

10. Sender nach Anspruch 9, wobei im Sender ein Sicherheitsmodul zur effizienten und sicheren Ausführung kryptographischer Operationen vorgesehen ist, welches Mittel zum Schutz sowohl gegen softwaretechnische als auch gegen physikalische Angriffe oder Seitenkanalangriffe aufweist.

11. Empfänger umfassend Mittel geeignet zum Durchführen eines Verfahrens nach Anspruch 8.

Es folgen 3 Blatt Zeichnungen

Anhängende Zeichnungen

FIG 1

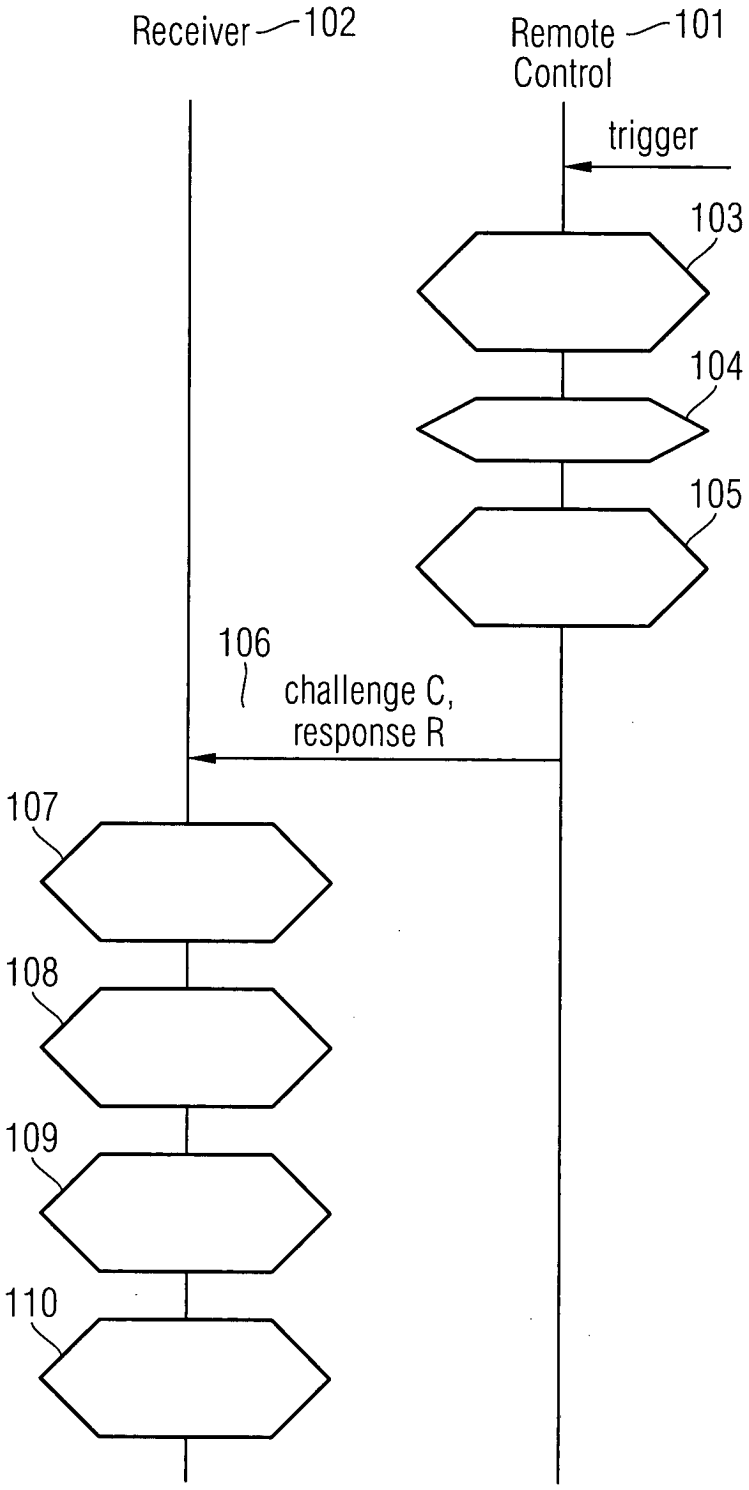


FIG 2

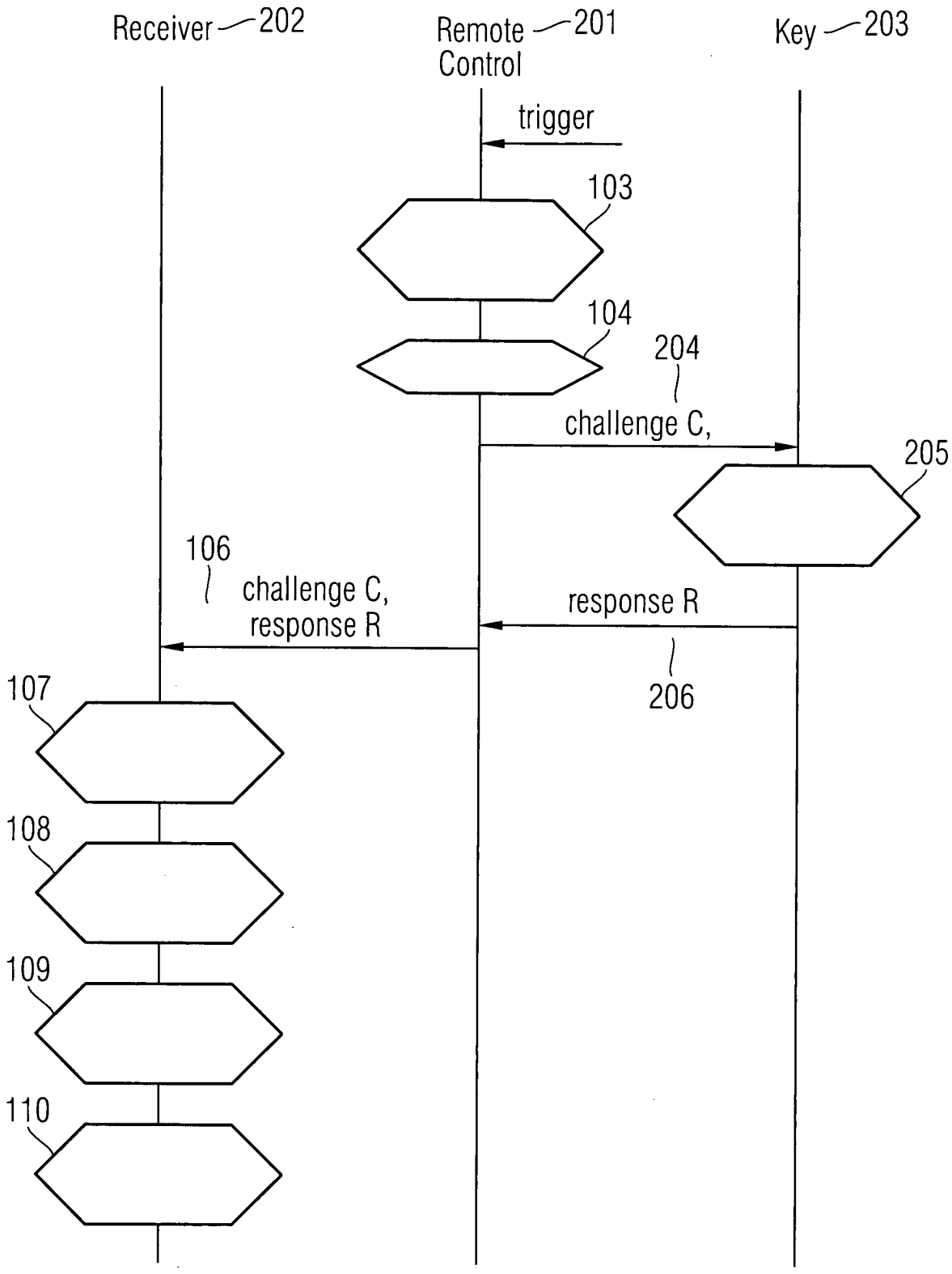
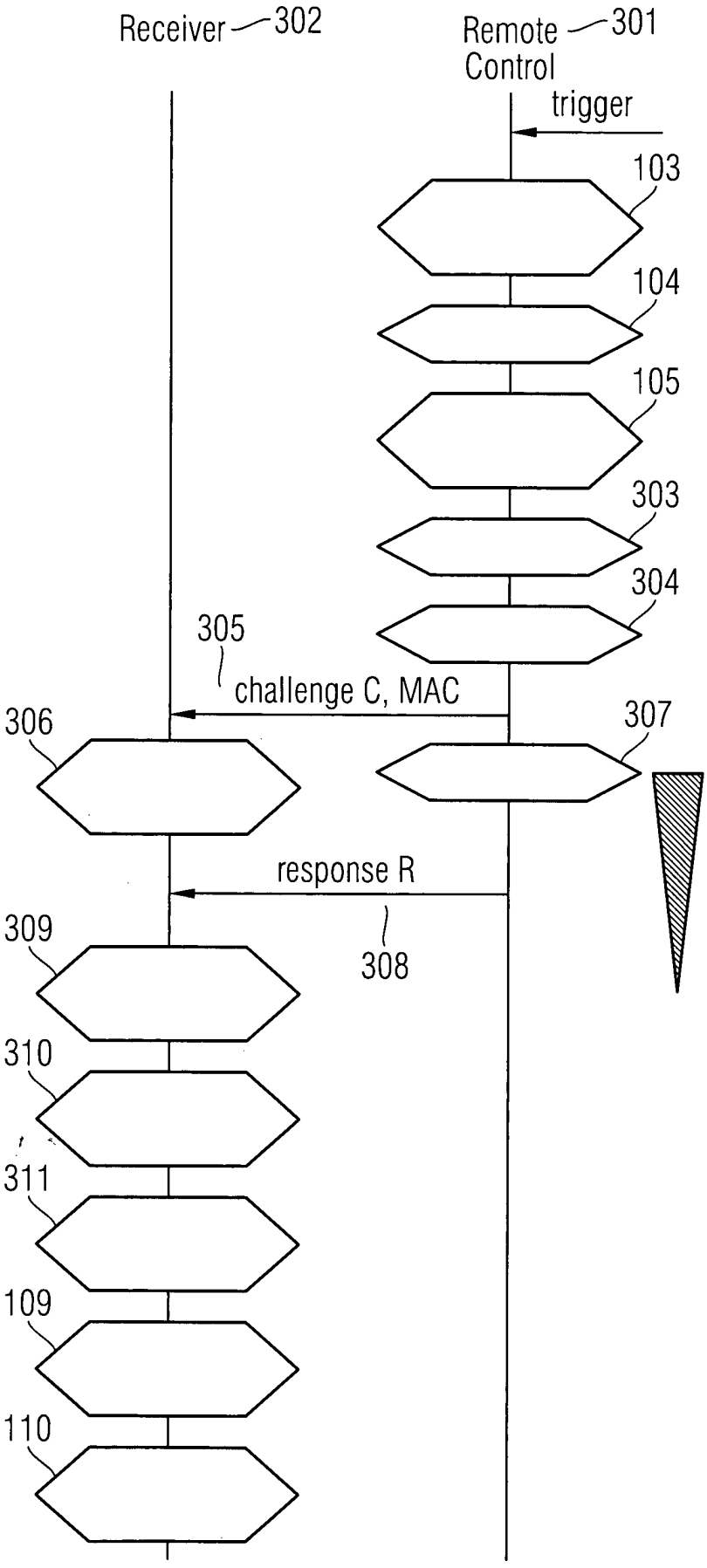

Receiver
202
Remote Control
201
Key
203
trigger
103
104
204
challenge C,
205
106
challenge C, response R
response R
206
107
108
109
110

FIG 3


Receiver
302
Remote Control
301
trigger
103
104
105
303
304
305
challenge C, MAC
306
307
response R
308
309
310
311
109
110