(19) österreichisches patentamt

(10) **AT 523056 B1 2021-05-15**

(12) **Patentschrift**

(21) Anmeldenummer: A 21/2020
(22) Anmeldetag: 23.01.2020
(45) Veröffentlicht am: 15.05.2021

(51) Int. Cl.: ***H04K 1/00*** (2006.01)
H04W 12/00 (2021.01)
H04L 29/06 (2006.01)
H04L 1/00 (2006.01)

(56) Entgegenhaltungen:
US 2005169469 A1
EP 1612986 A1
KITAURA Akito et al.: "A Scheme of Secret Key Agreement Based on Received Signal Strength Variation by Antenna Switching in Land Mobile Radio." In: The 9th International Conference on Advanced Communication Technology, 12.-14. Februar 2007 (12.02.2007). Konferenzbeitrag. ICACT2007. IEEE, Okamoto, Kobe, Japan. Seiten 1763-1767. doi:10.1109/ICACT.2007.358712
YAN Shihaho, et al.: "Antenna switching for security enhancement in full-duplex wiretap channels." In: IEEE Globecom Workshops (GC Wkshps) 2014, 8.-12. Dezember 2014 (08.12.2014). IEEE, Austin, TX, USA. Seiten 1308-1313. doi:10.1109/GLOCOMW.2014.7063614

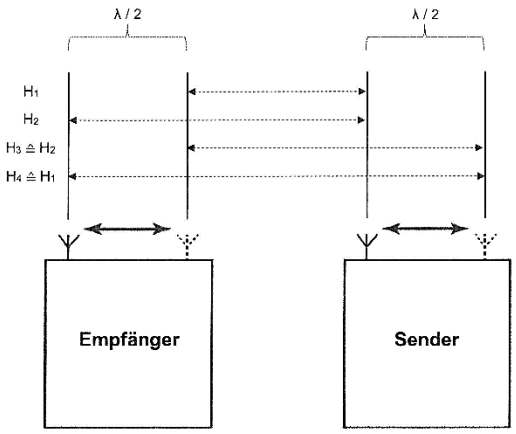
(73) Patentinhaber:
Artner Gerald Dr.
1070 Wien (AT)

(72) Erfinder:
Artner Gerald Dr.
1070 Wien (AT)

(74) Vertreter:
Häupl & Ellmeyer KG, Patentanwaltskanzlei
1070 Wien (AT)

(54) **Verschlüsselung durch Funkkanalmodulation**

(57) Die Erfindung betrifft ein Verfahren zur Verschlüsselung von Daten, die von einem Sender zu einem Empfänger über jeweils zumindest eine Antenne und über zumindest zwei Funkkanäle (H_1, H_2, H_3, H_n), zwischen denen während der Übertragung zumindest einmal gewechselt wird, übertragen werden, wobei das erfindungsgemäße Verfahren dadurch gekennzeichnet ist, dass
zumindest der Empfänger der zu verschlüsselnden Daten während der Signalübertragung den jeweils aktiven Funkkanal zumindest einmal gemäß einem kryptografischen Schlüssel, in dem der Modus des Funkkanalwechsels festgelegt ist, wechselt, wobei jeder Kanalwechsel jeweils abrupt oder allmählich erfolgen kann.



Figur 7

AT 523056 B1 2021-05-15

Beschreibung

[0001] Die vorliegende Erfindung betrifft die Verschlüsselung von mittels Funk übertragenen Daten durch Funkkanalmodulation.

STAND DER TECHNIK

[0002] In den letzten Jahren sind zahlreiche unterschiedliche Verfahren zur drahtlosen Datenübertragung mittels elektromagnetischer Wellen - hierin kollektiv als Funkübertragung bezeichnet - theoretisch beschrieben worden, bei denen Daten dadurch übertragen werden, dass der oder die Funkkanäle einer Funkverbindung modifiziert werden und/ oder zwischen Funkkanälen gewechselt wird. Im Folgenden werden solche Verfahren als Kanalmodulation bezeichnet. Kanalmodulation kann beispielsweise dadurch realisiert werden, dass die Position(en) einer oder mehrerer Antennen von Sendern und/ oder Empfängern von Funksignalen verändert werden. Auf diese Weise kann die Qualität von Datenübertragungen deutlich verbessert werden. Siehe z. B. J. Jeganathan, A. Ghrayeb, L. Szczecinski, A. Ceron, "Space shift keying modulation for MIMO Channels", IEEE Trans. Wireless Commun. 8(7), 3692-3703 (2009); M. Di Renzo, H. Haas, P. M. Grant, "Spatial modulation for multiple-antenna wireless systems: a survey", IEEE Commun. Mag. 49(12), 182-191 (2011); R. Mesleh, H. Haas, S. Sinanovic, C. W. Ahn, S. Yun, "Spatial Modulation", IEEE Trans. Veh. Technol. 64(6), 2738-2742 (2015); R. Mesleh, S. S. Ikki, H. M. Aggoune, "Quadrature Spatial Modulation", IEEE Trans. Veh. Technol. 64(6), 2738-2742 (2015); I. Yildirim, E. Basar, I. Altunbas, "Quadrature Channel Modulation", IEEE Wireless Commun. Lett. 6(6), 790-793 (2017); A. Mokh, M. Crussiére, M. Hélard, M. Di Renzo, "Theoretical Performance of Coherent and Incoherent Detection for Zero-Forcing Receive Antenna Shift Keying", IEEE Access 6, 39907-39916 (2018). Nachteilig ist dabei jedoch die oftmals mangelnde Möglichkeit einer zuverlässigen Verschlüsselung der so übertragenen Daten. Insbesondere wäre es wünschenswert eine Verschlüsselung auf physikalischer Basis zu erreichen, die nützlicherweise auf den besonderen Eigenschaften von Kanalmodulationsverfahren basiert.

[0003] Ziel der Erfindung war daher die Entwicklung eines verbesserten Verfahrens zur Verschlüsselung von mittels Kanalmodulation übertragenen Daten.

OFFENBARUNG DER ERFINDUNG

[0004] Dieses Ziel erreicht die vorliegende Erfindung durch Bereitstellung eines Verfahrens zur Verschlüsselung von Daten, die von einem Sender zu einem Empfänger über jeweils zumindest eine Antenne und über zumindest zwei Funkkanäle (H_1, H_2, H_3, H_n), zwischen denen während der Übertragung zumindest einmal gewechselt wird, übertragen werden,
wobei das erfindungsgemäße Verfahren dadurch gekennzeichnet ist, dass zumindest der Empfänger der zu verschlüsselnden Daten während der Signalübertragung den jeweils aktiven Funkkanal zumindest einmal gemäß einem kryptografischen Schlüssel, in dem der Modus des Funkkanalwechsels festgelegt ist, wechselt, wobei jeder Kanalwechsel jeweils abrupt oder allmählich erfolgen kann.

[0005] Durch einen oder vorzugsweise mehrere derartige Kanalwechsel, die entweder nur durch den Empfänger der Daten oder auch durch den Empfänger und den Sender der Daten gemäß einem zuvor festgelegten kryptografischen Schlüssel erfolgen können, wird es für Dritte praktisch unmöglich, die so übertragenen Daten zur Gänze aufzuzeichnen.

[0006] Wobei hierin unter "Daten" jegliche mittels Funk übertragbare, nicht für Dritte bestimmte und daher zu verschlüsselnden Signale zu verstehen sind, d. h. sowohl analoge Signale, wie z.B. Gespräche, als auch digitale Dateien wie etwa Text-, Bild-, Video- oder Sounddateien usw.

[0007] Unter dem "Sender" ist hierin jene Funkstation zu verstehen, die die zu verschlüsselnden Daten an den "Empfänger" zu übermitteln hat, womit jene Funkstation bezeichnet wird, die diese Daten mittels der Funkübertragung empfängt. Beide Bezeichnungen sind unabhängig von sonstigen Kommunikation während der Funkübertragung, also von der speziellen Art und Weise der Übertragung, von der Reihenfolge der Signalübermittlung, d. h. davon, welche Station zuerst

überträgt, von der Menge an ausgesandten oder empfangenen Signalen, d. h. davon, welche Station welche oder wie viele Signale übermittelt, von der Anzahl an während der Übertragung vorgenommenen Kanalwechseln usw. Entscheidend ist lediglich, welche Station die zu verschlüsselnden Daten überträgt.

[0008] Weiters ist zu beachten, dass sich die hierin offenbarte Erfindung auf jegliche Art von Signalen bezieht, also beispielsweise sowohl auf unmodulierte Trägersignale als auch auf solche mit darauf aufmodulierten Nutzsignalen, die in beliebigen Frequenzbereichen, gepulst oder ungepulst, polarisiert oder nichtpolarisiert übertragen werden können.

[0009] Unter einem "Funkkanal" ist hierin eine definierte Auswahl sämtlicher von außen beeinflussbarer Parameter der Übertragung von Funksignalen ohne signifikante Schwankungen der Signalqualität während der Übertragung zu verstehen. Umgekehrt wird jede von Sender oder vom Empfänger bewusst herbeigeführte Änderung zumindest eines dieser Parameter, die zu einer signifikanten Änderung in der Signalübertragung führt, als "Funkkanalwechsel" bezeichnet.

[0010] Unter einem "kryptografischen Schlüssel" wird hierin jene Information bezeichnet, anhand derer Kanalwechsel durch eine der beiden an der Funkübertragung beteiligten Stationen identifizierbar ist, wobei vor Beginn der Übertragung beiden Funkstationen zumindest ein zu benutzender kryptografischer Schlüssel bekannt sein muss, um den oder die während der Übertragung erfolgenden Kanalwechsel vorhersehbar zu machen.

[0011] In bevorzugten Ausführungsformen der Erfindung sendet zu Beginn der Signalübertragung entweder der Sender Start- oder Pilotsignale an den Empfänger oder der Empfänger Startsignale an den Sender aus, um so die für die Signalübertragung aktiven Funkkanäle zu indentifizieren ("Kanalschätzung"), wobei im weiteren Verlauf der Signalübertragung zumindest der Empfänger gemäß dem kryptografischen Schlüssel den jeweils aktiven Funkkanal zumindest einmal wechselt, was die Sicherheit der späteren Datenübertragung noch weiter erhöht.

[0012] In erfindungsgemäß besonders bevorzugten Ausführungsformen gibt während der Signalübertragung der Empfänger mittels Signal an den Sender einen neuen, für die weitere Signalübertragung gültigen kryptografischen Schlüssel bekannt, durch den die darauf folgende Art und Weise des oder der späteren Funkkanalwechsel festgelegt wird, was erneut die Sicherheit der Datenübertragung steigert.

[0013] Eine ganz besonders bevorzugte Ausführungsform der vorliegenden Erfindung besteht darin, dass während der Signalübertragung für eine definierte Zeitspanne ausschließlich der Empfänger der zu verschlüsselnden Daten Signale aussendet, wobei der Empfänger zwischen zumindest zwei Funkkanäle auswählt und den jeweils aktiven Funkkanal in einer definierten Abfolge wechselt, wobei die zu verschlüsselnden Daten in der Abfolge der vom Sender zum Empfangen der Signale ausgewählten Funkkanäle bestehen, die dem Empfänger nach der Beendigung - oder während und nach der Beendigung - der Abfolge auf zumindest einem gesonderten Kanal bekanntgegeben wird.

[0014] Auf diese Weise kommt es gewissermaßen zu einer Umkehr von Sender und Empfänger, da der Sender der eigentlichen Daten während der Funkübertragung gar keine potenziell von Dritten mitverfolgbaren Signale aussendet, sondern lediglich die zum Empfangen der ausschließlich vom Empfänger ausgesandten Signale gewählten Funkkanäle wechselt und durch den Modus seiner Funkkanalwechsel die eigentlichen Daten erzeugt. Die gewählten Kanäle werden dem Empfänger entweder bereits während oder aber erst nach Beendigung seiner Signalübertragung an den Sender auf zumindest einem gesonderten Kanal bekannt. Der Empfänger der so verschlüsselten Daten übermittelt während der Funkübertragung somit nur Scheinsignale oder Scheindaten an den Sender, die für Dritte völlig wertlos sind, da die eigentliche Übertragung der Daten durch die Auswahl des Funkkanals durch den Sender erfolgt.

[0015] Die Bekanntgabe der eigentlichen Daten, d. h. der Abfolge, in der der Sender die Funkkanäle zum Empfangen der Signale vom Empfänger gewechselt hat, erfolgt dabei über zumindest einen gesonderten Kanal. Dabei kann es sich entweder ebenfalls um einen oder vorzugsweise mehrere Funkkanäle, d. h. eine Übertragung mittels Radiowellen, handeln, noch bevorzugter sol-

che Funkkanäle, die der Sender nicht zum Empfangen der Signale des Empfängers nutzt, oder aber, es wird gemäß besonders bevorzugten Ausführungsformen eine andere Art der Signalübertragung als gesonderter Kanal gewählt, wie z.B. optische oder akustische Signale, sofern sich beide Beteiligte in Reichweite solcher Signale befinden, also z. B. Sichtkontakt zueinander haben oder sich in "Hörreichweite" befinden, womit hierin auch die Reichweite von Schallwellen im Ultra- oder Infraschallbereich gemeint ist.

[0016] Speziell um auch größere Datenmengen auf diese Weise übermitteln zu können, erfolgt die Bekanntgabe der vom Sender gewählten Funkkanalabfolge an den Empfänger besonders bevorzugt mittels einer Vorrichtung, die in der Lage ist, den jeweils vom Sender zum Empfangen der Signale gewählten Funkkanal zu bestimmen und die Abfolge des Kanalwechsels zu speichern und dem Empfänger auf dem gesonderten Kanal bekanntzugegeben, wobei der Empfänger auf die Vorrichtung direkten oder indirekten Zugriff hat oder diesen Zugriff vom Sender vor, während oder nach Beendigung der Abfolge erhält - wie auch immer dieser Zugriff konkret geartet ist.

[0017] Für den Fall, dass die Abfolge in Form von optischen Signalen über den gesonderten Kanal übertragen wird, kann beispielsweise der Sender über eine Vorrichtung verfügen, die für jeden der von ihm zum Empfangen der "Scheinsignale" gewählten Funkkanäle ein bestimmtes Lichtsignal aussendet, z. B. je nach dem gewählten Kanal ein Signal in unterschiedlicher Farbe, d. h. mit unterschiedlicher Frequenz, oder ein gepulstes Signal mit jeweils unterschiedlicher Pulsdauer. Zu diesem Zweck können anstelle von sichtbarem Licht auch elektromagnetische Wellen aus anderen Frequenzbändern, vorzugsweise jedoch keine mittels Funk zu übertragenden Radiowellen, eingesetzt werden, wobei die Übermittlung in analoger Weise erfolgen kann.

[0018] Der Empfänger der so verschlüsselten Daten verfügt in diesen Fällen gemäß vorliegender Erfindung vorzugsweise über eine entsprechende Vorrichtung, die in der Lage ist, die von der Vorrichtung des Senders ausgewählten Kanäle zu erkennen und zu speichern, wodurch er in den Besitz der so verschlüsselten Daten gelangt - und das parallel zu bzw. nach der Übertragung der Scheindaten während des Funkkontakts zwischen Empfänger und Sender.

[0019] Die Übertragung der Daten von einer Vorrichtung des Senders zu einer Vorrichtung des Empfängers kann dabei auch über eine oder mehrere Zwischenstationen erfolgen, z. B. über eine oder mehrere weitere Vorrichtungen, die zusammen eine entsprechende - wie auch immer geartete - Verbindung zwischen den beiden Vorrichtungen und somit schließlich zwischen den beiden Funkgeräten von Sender und Empfänger herstellen. Ausschlaggebend für diese Ausführungsformen der vorliegenden Erfindung ist dabei weiterhin der Umstand, dass die von Dritten möglicherweise verfolgbare Funkübertragung zwischen Empfänger und Sender zum einen in umgekehrter Richtung wie die Übermittlung der eigentlichen Daten und zum anderen nur zum Schein erfolgt. Ein vereinfachtes repräsentatives Beispiel für solche Ausführungsformen der vorliegenden Erfindung wird später näher beschrieben.

[0020] Die Art des oder der Wechsel des jeweils genutzten Funkkanals ist gemäß vorliegender Erfindung nicht speziell eingeschränkt, solange es sich, wie erwähnt, um eine bewusst herbeigeführte Änderung zumindest eines der Parameter der Funkübertragung handelt, die zu einer signifikanten Änderung in der Signalübertragung führt. Vorzugsweise kann ein Funkkanalwechsel etwa auf folgende Weise erfolgen:

a) durch Änderung der Länge des Funkkanals mittels
   a1) eines Wechsels von einer ersten zu zumindest einer zweiten Antenne durch den Sender und/oder den Empfänger und/oder
   a2) Änderung der Position zumindest einer Antenne des Senders und/ oder des Empfängers von einer ersten zu zumindest einer zweiten Position,

   wobei die Länge des Funkkanals in ausreichendem Maße geändert wird, um eine signifikante Änderung des Signals zu bewirken und

   wobei die Positionen der Antenne(n) des Empfängers optisch verschleiert sind;
b) durch Änderung der Frequenz(en) oder des Frequenzbandes der gesendeten und/oder empfangbaren Signale;
c) durch Änderung der Pulsdauer von gepulst gesendeten und/oder empfangbaren Signalen;

d) durch Änderung der Phase der gesendeten und/oder empfangbaren Signale;
e) durch Änderung der Polarisation von gesendeten und/oder empfangbaren polarisierten Wellen;
f) durch Änderung der Richtcharakteristik der Sende- und/oder Empfangsantenne(n);
g) durch Änderung des Codes von codiert gesendeten und/oder empfangbaren Signalen;
h) durch Änderung der Signalübertragungseigenschaften des Funkkanals durch den Sender und/oder den Empfänger; oder
i) durch eine beliebige Kombination zweier oder mehrerer der obigen Schritte a) bis h).

[0021] Noch bevorzugter sind dabei Ausführungsformen, bei denen
- in Schritt a) durch die Änderung der Länge des Funkkanals eine Änderung des Signals um eine halbe Wellenlänge λ/2 bewirkt wird; und/oder
- in Schritt d) die Phase um eine halbe Periode π geändert wird; und/oder
- in Schritt e) die Polarisationsebene polarisiert gesendeter und/oder empfangbarer Signalwellen um 90° gedreht wird; und/oder
- in Schritt h) die Signalübertragungseigenschaften des Funkkanals durch Zwischenschaltung eines Dämpfers, Verstärkers, Streuers oder Reflektors verändert werden.

[0022] Zur weiteren Erhöhung der Sicherheit der Datenübertragung besonders bevorzugt sind gemäß vorliegender Erfindung Kombinationen mehrerer verschiedener der obigen Schritte a) bis h), auf die später noch näher eingegangen wird.

[0023] Weiters wird gemäß vorliegender Erfindung bevorzugt, dass zusätzlich zur Übertragung von die zu verschlüsselnden Daten umfassenden Signale über den jeweils aktiven Funkkanal vom Sender und/oder vom Empfänger auch auf zumindest einem weiteren Funkkanal Signale übertragen werden, die nicht zur Übermittlung der zu verschlüsselnden Daten dienen. Auch solche Scheinsignale oder Scheindaten erschweren den Zugriff für Dritte auf die eigentlichen Daten erheblich.

[0024] Und schließlich wird gemäß vorliegender Erfindung bevorzugt, dass die Antenne(n) zur Verschleierung ihrer Eigenschaften unter einer dielektrischen Hülle, wie z. B. einer Antennenkuppel, untergebracht ist/sind, was die Identifizierung der aktiven Funkkanäle für Dritte weiter erschwert.

KURZBESCHREIBUNG DER ZEICHNUNGEN

[0025] Die Erfindung wird nachstehend anhand von konkreten Beispielen unter Bezugnahme auf die beiliegenden Zeichnungen näher beschrieben, die Folgendes zeigen.

[0026] Fig. 1 ist eine schematische Darstellung des Vorliegens mehrerer auswählbarer Funkkanäle für sowohl den Sender als auch den Empfänger der zu verschlüsselnden Daten, wobei gemäß Fig. 1a jeweils 2 Kanäle, H_1 und H_2, und gemäß Fig. 1b jeweils n Kanäle, H_1 bis H_n, auswählbar sind. Der Empfänger kann durch seine Wahl des Kanals die Bedeutungen der Auswahl des Senders ändern, so wird in Fig. 1a die Bedeutung des linken Sendekanals als H_1 oder H_2 erst durch die Wahl des Empfängers (links oder rechts) gemäß einem kryptografischen Schlüssel festgelegt.

[0027] Fig. 2 zeigt schematisch, wie in der Ausführungsform aus Fig. 1a unter der Annahme, dass es sich jeweils um zwei getrennte Antennenpositionen handelt, zwischen den jeweils zwei Kanälen ausgewählt werden kann, nämlich in Fig. 2a durch Umschalten zwischen den je zwei Antennen und in Fig. 2b durch Verschieben der Position je einer Antenne von einer Position zu einer anderen.

[0028] Die Fig. 3 bis 5 sind schematische Darstellungen verschiedener Arten des Funkkanalwechsels durch Änderung jeweils eines bestimmten Parameters der Funkübertragung.

[0029] Fig. 6 zeigt schematisch die Aussendung eines Pilotsignals zu Beginn der Funkübertragung durch den Empfänger der zu verschlüsselnden Daten.

[0030] Fig. 7 zeigt schematisch die Versuchsanordnung eines exemplarischen praktischen Beispiels für eine besonders bevorzugte Ausführungsform der vorliegenden Erfindung, und Fig. 8 ist eine Fotografie derselben.

BEISPIELE

[0031] Unter Bezugnahme auf die Zeichnungen werden nun konkrete beispielhafte und nicht als Einschränkung zu verstehende Ausführungsformen der vorliegenden Erfindung näher beschrieben.

[0032] Wie erwähnt stellt Fig. 1 schematisch das Vorliegen mehrerer für die Funkübertragung auswählbarer Kanäle für sowohl den Sender als auch den Empfänger der zu verschlüsselnden Daten dar. Dabei kann es sich jeweils um physisch getrennte Antennen oder Antennenpositionen oder auch um mittels ein und derselben Antenne gespeiste Funkkanäle handeln. In Fig. 1a sind für Sender und Empfänger jeweils zwei Funkkanäle H_1 und H_2 auswählbar, was in der Praxis der vorliegenden Erfindung am einfachsten mittels jeweils zweier räumlich getrennter Antennen realisiert werden kann, sofern diese ausreichend weit voneinander beabstandet sind, um die Länge des Funkkanals - gemäß obigen Schritt a) der Optionen des Funkkanalwechsels - in ausreichendem Maße zu ändern, um eine signifikante Änderung des Signals zu bewirken. Dies ist vor allem bei stationären Funkstationen, sowohl als Sender als auch als Empfänger, gegeben, ist aber beispielsweise auch für Fahrzeugantennen realisierbar, die durchaus mehrere Meter Abstand zueinander aufweisen können.

[0033] Gemäß bereits bekannten Kanalmodulationsverfahren überträgt der Sender Daten, indem er zwischen den Kanälen H_1 und H_2 wählt. Erfindungsgemäß kann der Empfänger jedoch die gewählten Kanäle beeinflussen, beispielsweise durch räumliche Änderung seiner Antenne wie in Fig. 2a oder 2b. Der Empfänger beeinflusst die Kanäle gemäß einem kryptografischen Schlüssel, der dem Sender bekannt ist. Ein Dritter könnte zwar mit Aufwand die gewählten Antennenposition des Senders detektieren, nicht jedoch, ob diese in H_1 oder H_2 resultiert, da die Position der Empfangsantenne verschleiert ist.

[0034] In der Ausführungsform gemäß Fig. 1b können beide Beteiligte jeweils zwischen n Funkkanälen H_1 bis H_n wählen, was speziell bei höheren Werten für n, z. B. für n = 4 oder mehr, in Form von physischen Antennen praktisch wohl nur für stationäre Funkstationen realisierbar ist.

[0035] Fig. 2 stellt schematisch die einfachste Ausführungsform mit je zwei Antennen und je zwei Funkkanälen H_1 und H_2 dar, die jeweils unterschiedliche Länge aufweisen und zwischen denen auf folgende Weise gewählt werden kann: Im Falle von je zwei fix montierten Antennen, wie in Fig. 2a gezeigt, kann zwischen diesen beiden hin und her geschaltet werden kann, um die jeweils aktive Antenne zu definieren, wie dies zuvor als Schritt a1) beschrieben wurde. Im Falle von nur jeweils einer, aber nicht ortsfesten Antenne, wie in Fig. 2b dargestellt, kann der Funkkanal dadurch gewechselt werden, dass die Antenne gemäß obigen Schritt a2) um eine ausreichende Distanz in eine neue Position verschoben wird. Mit "ausreichend" ist wiederum eine Entfernung gemeint, durch die sich die Länge des Funkkanals in ausreichendem Maße ändert, dass eine signifikante Änderung, z. B. eine Verstärkung oder Abschwächung, des Signals bewirkt wird, damit der Funkkanalwechsel vom zweiten Beteiligten an der Funkübertragung auch als solcher wahrgenommen werden kann. Vorzugsweise wird in Schritt a) eine solche Änderung der Länge des Funkkanals herbeigeführt, dass dadurch eine Änderung des Signals um eine halbe Wellenlänge $\lambda/2$ bewirkt wird, um so einen deutlich wahrnehmbaren, abrupten Funkkanalwechsel vorzunehmen.

[0036] Wie erwähnt sind beide Arten des Funkkanalwechsels sowohl für stationäre als auch für mobile Sender und Empfänger in Fahrzeugen realisierbar. In allen Fällen sind die Positionen der Antenne(n) für stationäre Empfänger vorzugsweise verschleiert, um die Identifizierung des jeweils aktiven Funkkanals für Dritte zu erschweren.

[0037] In Fig. 3 sind zwei weitere Arten des Funkkanalwechsels schematisch dargestellt, nämlich in Fig. 3a durch Änderung der Frequenz(en) oder des Frequenzbandes der Signalübertragung, wie zuvor als Schritt b) beschrieben, und in Fig. 3b durch Änderung der Pulsdauer von gepulst übertragenen Signalen gemäß Schritt c) oben.

[0038] Die Fig. 4 und 5 zeigen schematisch fünf weitere der oben beschrieben Optionen, nämlich:
in Fig. 4a durch Phasenänderung der Signale gemäß Schritt d), vorzugsweise durch Änderung der Phase um eine halbe Wellenlänge λ/2, erneut um so einen deutlich erkennbaren, abrupten Funkkanalwechsel zu bewirken;
in Fig. 4b durch Änderung der Polarisation von polarisiert übermittelten Wellen gemäß Schritt e), für einen abrupten Funkkanalwechsel vorzugsweise durch eine Drehung der Polarisationsebene um 90°;
in Fig. 4c durch Änderung der Richtcharakteristik der Sende- und Empfangsantennen gemäß Schritt f); z. B. durch Veränderung der Ausrichtung von Richtantennen;
in Fig. 5a durch Änderung des Codes von codiert übermittelten Signalen gemäß Schritt g); und
in Fig. 5b durch Änderung der Signalübertragungseigenschaften des Funkkanals gemäß Schritt h), z. B. durch eine, gegebenenfalls intermittierende, Zuschaltung eines Dämpfers, Verstärkers, Streuers oder Reflektors, um das Signal signifikant zu verändern.

[0039] In allen diesen Darstellungen ist die Möglichkeit eines Funkkanalwechsels jeweils für den Sender und den Empfänger eingezeichnet. Gemäß vorliegender Erfindung ist es jedoch essenziell, dass zumindest der Empfänger dazu in der Lage ist, d. h. zumindest der Empfänger muss gemäß vorliegender Erfindung im Verlauf der Signalübertragung die Möglichkeit haben, den aktiven Kanal einmal oder mehrmals zu wechseln.

[0040] Vorzugsweise ist es jedoch sowohl dem Sender als auch dem Empfänger möglich, den Funkkanal zumindest einmal, noch bevorzugter jeweils mehrmals, zu wechseln, um die Qualität der dadurch erzielten Verschlüsselung weiter zu verbessern.

[0041] Und insbesondere ist es gemäß vorliegender Erfindung beiden möglich, den aktiven Funkkanal mehrere Male jeweils auf unterschiedliche Art, beispielsweise auf zwei oder mehrere in den Schritten a) bis h) oben definierte Arten, zu wechseln, was eine besonders zuverlässige Art der Verschlüsselung darstellt.

[0042] In Fig. 6 ist schließlich eine Variante einer weiteren bevorzugten Ausführungsform der Erfindung schematisch dargestellt, bei welcher der Empfänger der zu verschlüsselnden Daten bereits das Pilotsignal aussendet, mittels dessen physikalisch festgelegt wird, welche Funkkanäle während der Signalübertragung aktiv sind.

[0043] Diese Variante der Aussendung des Pilotsignals durch den Empfänger kommt insbesondere bei einer besonders bevorzugten Ausführungsform der Erfindung zur Anwendung, bei der während der Funksignalübertragung ausschließlich der Empfänger der zu verschlüsselnden Daten elektromagnetische Wellen bzw. Signale, nämlich Scheinsignale, an den Sender der Daten übermittelt und Letzterer die Daten erst dadurch erzeugt, dass er zwischen mehreren aktiven Empfangskanälen hin und her wechselt und die Abfolge dieses Wechselns die eigentlichen Daten bilden.

[0044] Auf diese Weise sendet während der gesamten Funkübertragung ausschließlich der schlussendliche Empfänger der Daten Funksignale, die freilich keinerlei Wert für Dritte besitzen und nur davon ablenken sollen, dass die eigentlichen Daten durch die Kanalwahl erzeugt werden. Je mehr Kanäle der Empfänger zum Senden der Scheinsignale verwendet, umso schwieriger wird es für einen Dritten, den tatsächlich zum Übertragen der verschlüsselten Daten gewählten Funkkanal - wenn es sich denn überhaupt um einen Funkkanal handelt - zu identifizieren.

[0045] Da in bevorzugten Ausführungsformen mit passivem Sender der Empfänger das Pilotsignal aussendet, muss die Wahl des Funkkanals durch den Sender dem Empfänger bekannt werden. Besonders bevorzugt wird, wie zuvor erwähnt, kein Funkkanal als gesonderter Kanal benutzt, sondern die Daten - die in der Abfolge der Funkkanäle, die vom Sender zum Empfangen der von Empfänger ausgesandten Scheinsignale ausgewählt werden, bestehen - werden auf an-

dere Weise an den Empfänger übertragen.

[0046] Wie bereits erwähnt, können beispielsweise optische oder akustische Signale eingesetzt werden, solange Sender und Empfänger relativ nahe beieinander positioniert sind. So könnten etwa im Falle eines Sichtkontakts zwischen den beiden Beteiligten vom Sender mittels einer entsprechenden Vorrichtung, die zur Detektion des jeweils aktiven Funkkanals und vorzugsweise zur Speicherung dieser Abfolge in der Lage ist, Lichtsignale mit unterschiedlicher Wellenlänge je nach dem vom Sender gewählten Empfangskanal ausgesandt werden. Diese empfängt der Empfänger vorzugsweise ebenfalls mittels einer entsprechenden Vorrichtung detektiert und speichert sie ab.

[0047] Je größer die Anzahl der vom Sender gewählten Funkkanäle, desto besser natürlich die Qualität Verschlüsselung. Im Falle der Verwendung von nur zwei Funkkanälen H_1 und H_2 und der Übermittlung eines Binärcodes an den Empfänger könnte die Auswahl des Kanals H_1 zum Empfangen eines Blocks an vom Empfänger an den Sender übertragenen Scheinsignalen für "0" stehen und die Auswahl des Kanals und H_2 für "1". Werden hingegen beispielsweise vier Funkkanäle H_1 bis H_4 genutzt, so könnte eine einfache Kodierung etwa darin bestehen, dass die Kanäle H_1 für "00", H_2 für "01", H_3 für "10" und H_4 für "11" steht oder dergleichen.

[0048] Unabhängig davon, ob die Übermittlung der Abfolge der vom Sender ausgewählten Funkkanäle, also der eigentlichen verschlüsselten Daten, über einen oder mehrere weitere Funkkanäle oder über andere Kanäle, z. B. optische oder akustische, erfolgt, werden in bevorzugten Ausführungsformen der Erfindung eine oder mehrere Vorrichtungen dazu eingesetzt, diese Abfolge der aktiven Funkkanäle zu detektieren, zu speichern und an den Empfänger zu übermitteln. Dies kann entweder direkt, indem der Empfänger auf die Vorrichtung des Senders Zugriff hat oder erhält, oder vorzugsweise an eine entsprechende Vorrichtung des Empfängers erfolgen, die zum Empfang und zur Speicherung der Daten in der Lage ist. Die Übermittlung von einer Vorrichtung zur anderen kann auch über eine oder mehrere Zwischenstufen, d. h. weitere Vorrichtungen, erfolgen, beispielsweise mehrere Vorrichtungen, die miteinander optisch oder akustisch oder auf sonstige Weise zu kommunizieren in der Lage sind.

AUSFÜHRUNGSBEISPIEL

[0049] Ein stark vereinfachtes Beispiel für eine solche Übertragung der Daten über einen gesonderten Kanal wurde vom Erfinder auf die nachstehend beschriebene und in Fig. 7 schematisch dargestellte Weise in einem reflexionsfreien Raum durchgeführt.

[0050] Darin ist ein Mehrwegempfang zwischen zwei Funkantennen praktisch vollständig unterdrückt, so dass eine Kanalmodulation über den Einfallswinkel der Radiosignale oder über verzögerte Echos unmöglich ist. Die Amplitude der an zwei unterschiedlichen Antennenpositionen empfangenen Signale variiert hier nur geringfügig, da solche Variationen üblicherweise durch Freiraumdämpfung, nicht aber durch kleinräumigen Schwund zustandekommen. Der Phasenunterschied der an den beiden Antennenpositionen empfangenen Signale stellt jedoch eine experimentell nutzbare Messgröße dar, um zwischen mehreren für die Signalübertragung genutzten Funkkanälen unterscheiden und reproduzierbare Versuche durchführen zu können.

[0051] Im konkreten Versuch wurden zwei positionsveränderliche Antennen, die jeweils in horizontaler Ebene mittels eines Schlittens linear zwischen zwei Positionen verschiebbar waren, als Sender bzw. als Empfänger eingesetzt. Diese wurden nebeneinander in einer Geraden angeordnet, wie in Fig. 7 und Fig. 8 dargestellt, und waren somit miteinander sowie zueinander bzw. auseinander verschiebbar, woraus vier verschiedene Positionen und damit vier potentielle Funkkanäle H_1 bis H_4 resultieren. Kanal H_3 ist jedoch das Resultat einer parallelen Miteinanderbewegung der beiden Antennen aus der vorherigen Position, weswegen der Abstand gleich bleibt und die Signalübertragung mit jener von Kanal H_2 identisch ist. Kanal H_4 ist hingegen das Resultat der Auseinanderbewegung der Antennen und ist somit gegenüber H_1 um die doppelte Bewegungslänge verschoben. Bei einer geschickten räumlichen Wahl der Antennenpositionen um jeweils den halben Betrag der Sendewellenlänge, $\lambda/2$, verschoben ergibt das die folgenden Phasenverschiebungen der Signale im Vergleich zur Übertragung über Kanal H_1: Über die Kanäle H_2

und H_3 sind die Signale um eine halbe Schwingungsperiode, π, verschoben und über Kanal H_4 um eine ganze Periode, 2π, womit die Übertragung jener über Kanal H_1 entspricht. Folglich sind zwei verschiedene, sich in der Länge um $\lambda/2$ unterscheidende Funkkanäle, H_1 und H_2, anhand der Phasenverschiebung der Signale um π identifizierbar.

[0052] Die resultierenden Kanäle sind dann derart gestaltet, dass sowohl die linke als auch die rechte Position der Antenne am Sender jeweils H_1 und H_2 entsprechen können. Die linke und rechte Antennenposition am Empfänger sind dann derart gestaltet, dass der Empfänger durch die Wahl der Position seiner Antenne die Zuordnung der Sendeantennenposition zu H_1 und H_2 ändern kann. Werden die Abfolgen der Empfangsantennenposition zuvor geplant, werden sie zu einem kryptografischen Schlüssel, da nur durch sie eine eindeutige Zuordnung der Sendeantennenpositionen zu H_1 und H_2 möglich ist. Dieser kryptografische Schlüssel, also hier die geplanten Empfangsantennenpositionen, wird/werden dem Sender vor oder während der Übertragung bekannt gemacht, damit dieser die Sendeantennenpositionen entsprechend wählen kann, um einen Funkkanal H_1 oder H_2 zu erzeugen. Die Kanäle und die benötigten Vorrichtungen von Sender und Empfänger (z.B. zur Bewegung der Antennen) sind hinsichtlich dieser Übertragungsweise symmetrisch bzw. gleich, sodass Sender und Empfänger ihre Rolle tauschen können und eine bidirektionale Kommunikation möglich ist.

[0053] Als Antennen wurden zwei herkömmliche Groundplane-Antennen (oder auch Viertelwellenstrahler) für das 2,45-GHz-Frequenzband verwendet, wie sie beispielsweise in der Industrie, Wissenschaft oder Medizin zum Einsatz kommen. Beide wurden jeweils auf einer kreisförmigen Aluminium-Massefläche mit 18 cm Durchmesser platziert, die ihrerseits mittels Ständern jeweils 51 cm oberhalb der Schlitten angeordnet wurden, deren Bewegung mittels eines MATLAB-Skripts auf einem Laptop gesteuert wurde. Beide Antennen wurden zudem über Koaxialkabel an einen Netzwerkanalysator angeschlossen, der ebenfalls mittels MATLAB-Skript gesteuert wurde und der die Streuungsparameter messen und daraus anhand der gemessenen Phasenverschiebung den jeweils aktiven Funkkanal, H_1 oder H_2, identifizieren sollte.

[0054] Fig. 7 ist eine schematische Darstellung dieser Versuchsanordnung in Seitenansicht, während die Fig. 8a bis 8d Fotografien derselben sind, die im Wesentlichen entlang der Längsachse des Schlittens aufgenommen wurden. In den vier Fotografien von Fig. 8 sind sowohl für die vordere als auch die hintere Antenne die beiden jeweils möglichen Positionen der Mittelpunkte der kreisrunden Antennen-Masseflächen mittels kleiner Kreise dargestellt, von denen jeweils zwei auf einer Geraden eingezeichnet sind. Diese Geraden stellen für beide Antennen jeweils deren hintere, d. h. in den Fotografien: obere, und vordere, d. h. in den Fotografien: untere, Position dar, die jeweils um den halben Betrag der Sendewellenlänge, A/2, verschoben sind. (Der geringere Abstand zwischen den beiden Geraden für die hintere Antenne resultiert aus der Perspektive der Fotografien.)

[0055] Bei der Aufnahme der vier Fotografien aus Fig. 8 waren die Positionen der hinteren bzw. der vorderen Antenne daher die nachstehenden, was den in Fig. 7 von oben nach unten dargestellten vier Zuständen entspricht, wobei die linke Antenne aus Fig. 7 der hinteren aus Fig. 8 entspricht und die rechte Antenne aus Fig. 7 der vorderen aus Fig. 8.

	hintere / linke Antenne	vordere / rechte Antenne	Kanal
Fig. 8a / Fig. 7	vorne / rechts	hinten / links	H_1
Fig. 8b / Fig. 7	hinten / links	hinten / links	H_2
Fig. 8c / Fig. 7	vorne / rechts	vorne / rechts	H_2
Fig. 8d / Fig. 7	hinten / links	vorne / rechts	H_1

[0056] Wie zuvor erwähnt, werden durch diesen Modus der Antennenverschiebungen vier mögliche Zustände erzeugt, wovon in jeweils zwei Zuständen die beiden Antennen denselben Ab-

stand zueinander aufweisen, was die Funkkanäle H_1 und H_2 definiert, die sich in ihrer Länge um λ/2 unterscheiden.

[0057] Der jeweils aktive Kanal war sowohl für den Sender als auch den Empfänger zugänglich, da die Abfolge der Kanäle für beide abrufbar als Bitstream gespeichert wurde. Auf diese Weise war es möglich, dass der "Sender" die erst durch seine Auswahl des jeweils aktiven Kanals erzeugten Daten übermitteln konnte, ohne überhaupt irgendwelche Signale gesendet zu haben: Die Signalübertragung erfolgte ausschließlich durch den (späteren) Empfänger der Daten, und zwar in Form von Scheindaten, wie zuvor erläutert wurde, die für Dritte keinerlei verwertbare Information enthielten.

[0058] Die Übermittlung des gewählten Funkkanals mittels des Netzwerkanalysators an Sender und Empfänger, die entweder schon während oder auch erst nach Beendigung der Aussendung der Scheindaten erfolgen kann, stellt hier nur ein illustratives praktisches Beispiel für eine Übermittlung "auf einem gesonderten Kanal" dar, der, wie ebenfalls bereits erwähnt, kein Funkkanal zu sein braucht. Als Alternative kann zwar optional auch ein dritter Funkkanal gewählt werden, allerdings können beispielsweise auch optische oder akustische Signale denselben Zweck erfüllen, solange sich Sender und Empfänger in deren Reichweite befinden.

[0059] Die vorliegende Erfindung stellt somit ein völlig neuartiges Verfahren der Datenverschlüsselung bereit, das es für Dritte praktisch unmöglich macht, die so übertragenen Daten zur Gänze aufzuzeichnen.

Patentansprüche

1. Verfahren zur Verschlüsselung von Daten, die von einem Sender zu einem Empfänger über jeweils zumindest eine Antenne und über zumindest zwei Funkkanäle (H_1, H_2, H_3, H_n), zwischen denen während der Übertragung zumindest einmal gewechselt wird, übertragen werden, **dadurch gekennzeichnet**, dass
zumindest der Empfänger der zu verschlüsselnden Daten während der Signalübertragung den jeweils aktiven Funkkanal zumindest einmal gemäß einem kryptografischen Schlüssel, in dem der Modus des Funkkanalwechsels festgelegt ist, wechselt.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass zu Beginn der Signalübertragung entweder der Sender Startsignale an den Empfänger oder der Empfänger Startsignale an den Sender aussendet, um so die für die Signalübertragung aktiven Funkkanäle (H_1, H_2, H_3, H_n) zu identifizieren, und im weiteren Verlauf der Signalübertragung zumindest der Empfänger gemäß dem kryptografischen Schlüssel den jeweils aktiven Funkkanal (H_1, H_2, H_3, H_n) zumindest einmal wechselt.

3. Verfahren nach Anspruch 2, **dadurch gekennzeichnet**, dass während der Signalübertragung der Empfänger mittels Signal an den Sender einen neuen, für die weitere Signalübertragung gültigen kryptografischen Schlüssel bekanntgibt.

4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet**, dass während der Signalübertragung für eine definierte Zeitspanne ausschließlich der Empfänger der zu verschlüsselnden Daten Signale aussendet, wobei der Sender die Signale auf zumindest zwei Funkkanälen (H_1, H_2, H_3, H_n) empfängt, wobei die zu verschlüsselnden Daten in der Abfolge der vom Sender zum Empfangen der Signale ausgewählten Funkkanäle (H_1, H_2, H_3, H_n) bestehen, die dem Empfänger nach der Beendigung - oder während und nach der Beendigung - der Abfolge auf zumindest einem gesonderten Kanal bekanntgegeben wird.

5. Verfahren nach Anspruch 4, **dadurch gekennzeichnet**, dass die Bekanntgabe der Abfolge mittels einer Vorrichtung erfolgt, die in der Lage ist, den jeweils vom Sender zum Empfangen der Signale gewählten Funkkanal (H_1, H_2, H_3, H_n) zu bestimmen und die Abfolge des Kanalwechsels zu speichern und dem Empfänger auf dem gesonderten Kanal bekanntzugegeben, wobei der Empfänger auf die Vorrichtung direkten oder indirekten Zugriff hat oder diesen vom Sender vor, während oder nach Beendigung der Abfolge erhält.

6. Verfahren nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet**, dass der Wechsel des Funkkanals (H_1, H_2, H_3, H_n) auf folgende Weise erfolgt:
   a) durch Änderung der Länge des Funkkanals mittels
      a1) eines Wechsels von einer ersten zu zumindest einer zweiten Antenne durch den Sender und/oder den Empfänger und/oder
      a2) Änderung der Position zumindest einer Antenne des Senders und/ oder des Empfängers von einer ersten zu zumindest einer zweiten Position,

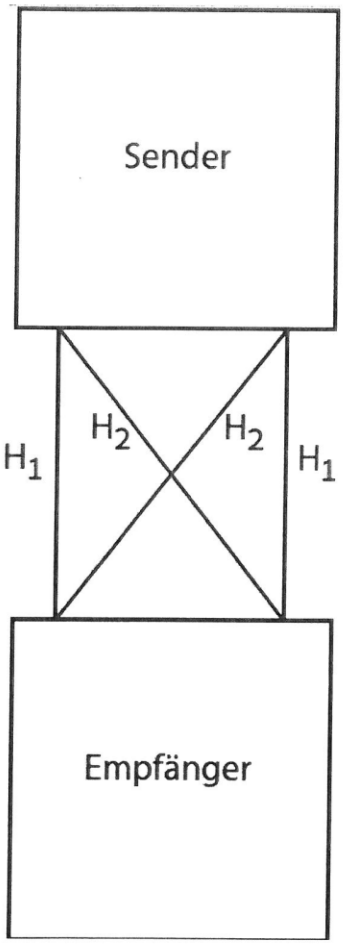
   wobei die Länge des Funkkanals in ausreichendem Maße geändert wird, um eine signifikante Änderung des Signals zu bewirken und
   wobei die Positionen der Antenne(n) des Empfängers optisch verschleiert sind;
   b) durch Änderung der Frequenz(en) oder des Frequenzbandes der übermittelten Signale;
   c) durch Änderung der Pulsdauer von gepulst übermittelten Signalen;
   d) durch Änderung der Phase der übermittelten Signale;
   e) durch Änderung der Polarisation von übermittelten polarisierten Wellen;
   f) durch Änderung der Richtcharakteristik der Sende- und/oder Empfangsantenne(n);
   g) durch Änderung des Codes von codiert übermittelten Signalen;
   h) durch Änderung der Signalübertragungseigenschaften des Funkkanals durch den Sender und/oder den Empfänger; oder
   i) durch eine beliebige Kombination zweier oder mehrerer der obigen Schritte a) bis h).

7. Verfahren nach Anspruch 6, **dadurch gekennzeichnet**, dass
   - in Schritt a) durch die Änderung der Länge des Funkkanals eine Änderung des Signals um eine halbe Wellenlänge λ/2 bewirkt wird; und/oder
   - in Schritt d) die Phase um eine halbe Periode π geändert wird; und/oder
   - in Schritt e) die Polarisationsebene polarisiert gesendeter und/oder empfangbarer Signalwellen um 90° gedreht wird; und/oder
   - in Schritt h) die Signalübertragungseigenschaften des Funkkanals durch Zwischenschaltung eines Dämpfers, Verstärkers, Streuers oder Reflektors verändert werden.

8. Verfahren nach einem der Ansprüche 1 bis 7, **dadurch gekennzeichnet**, dass zusätzlich zur Signalübertragung über den jeweils aktiven Funkkanal (H_1, H_2, H_3, H_n) vom Sender und/oder vom Empfänger auch auf zumindest einem weiteren Funkkanal (H_1, H_2, H_3, H_n) Signale übertragen werden, die nicht zur Übermittlung der zu verschlüsselnden Daten dienen.

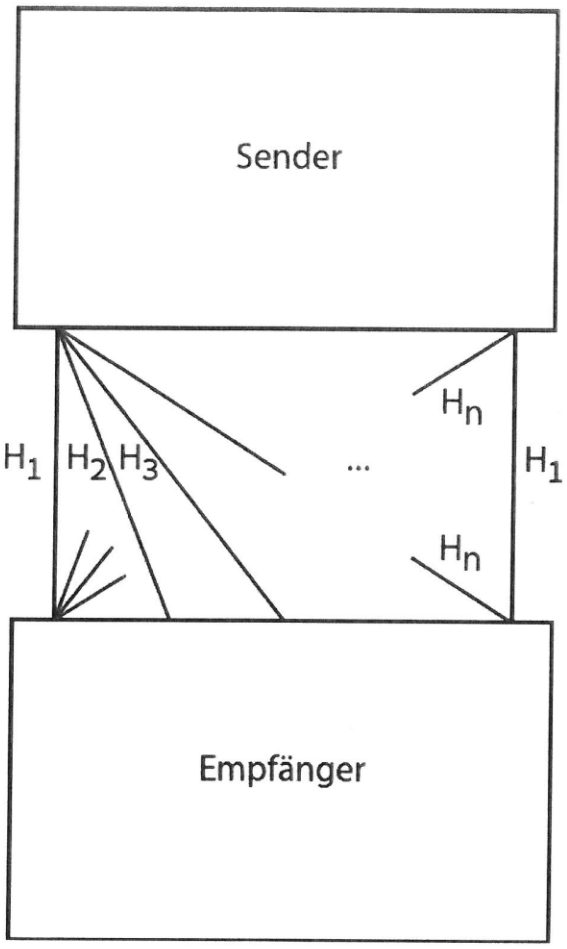
9. Verfahren nach einem der Ansprüche 1 bis 8, **dadurch gekennzeichnet**, dass die Antenne(n) zur Verschleierung ihrer Eigenschaften unter einer dielektrischen Hülle untergebracht ist/sind.

Hierzu 8 Blatt Zeichnungen



zwei Kanäle

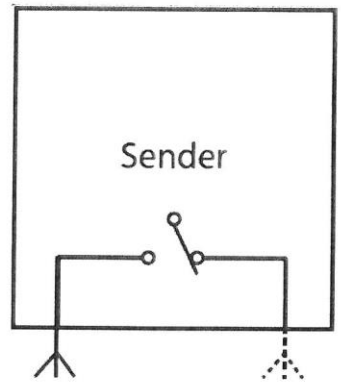
Fig. 1a

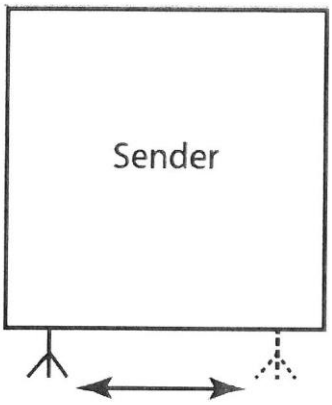


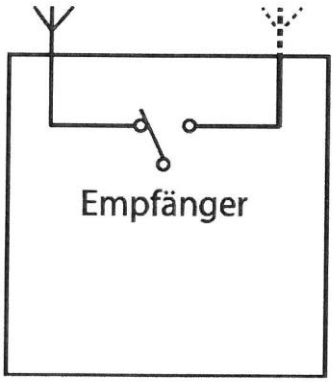
n Kanäle

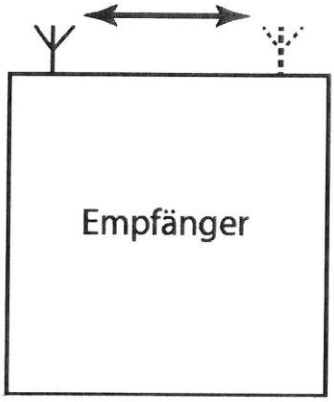
Fig. 1b

Figur 1









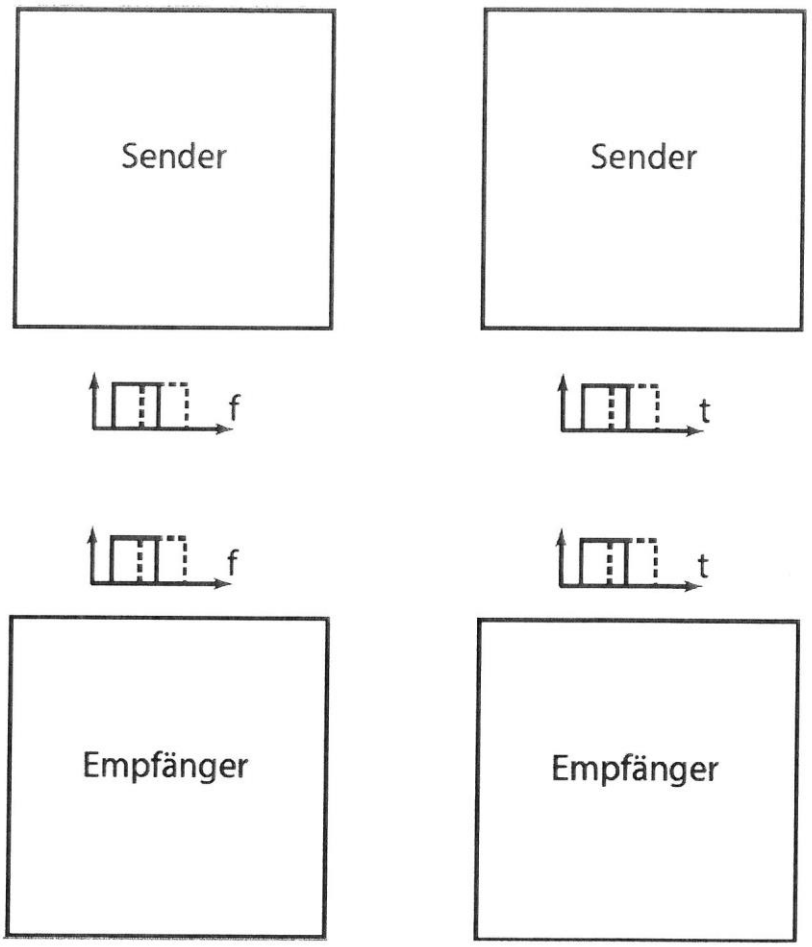
Antennenauswahl

Fig. 2a

Antennenbewegung

Fig. 2b

Figur 2



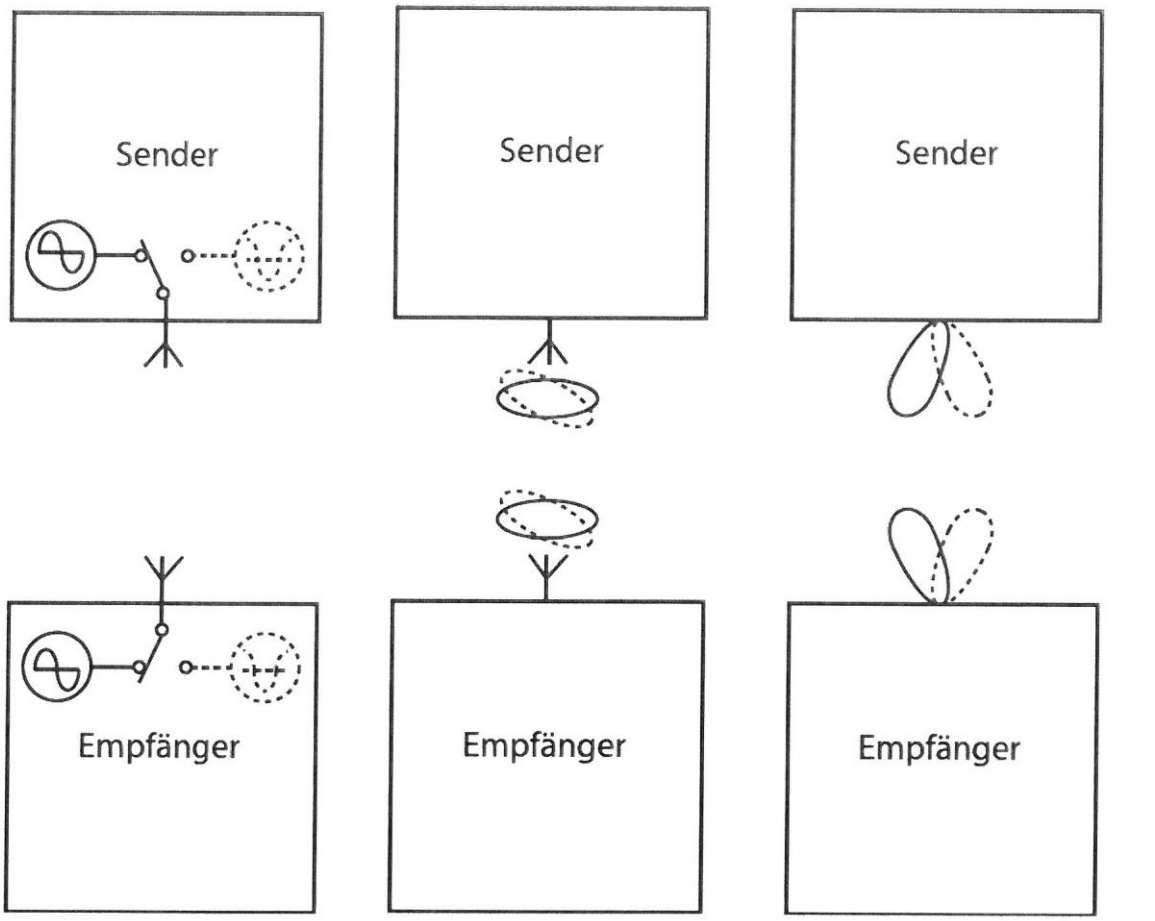
Frequenzänderung

Fig. 3a

Zeitänderung

Fig. 3b

Figur 3



Phasenänderung

Fig. 4a

Polarisationsänderung

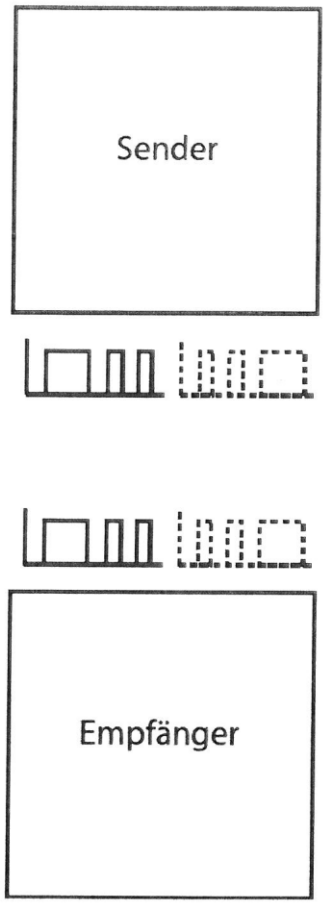
Fig. 4b

Richtcharakteristikänderung

Fig. 4c

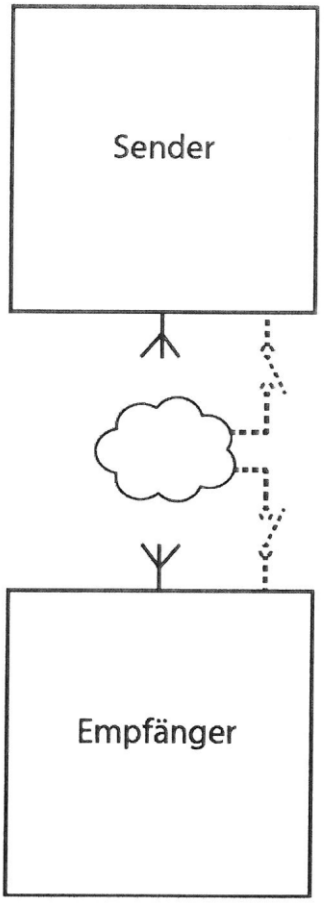
Figur 4

5/8



Codeänderung

Fig. 5a

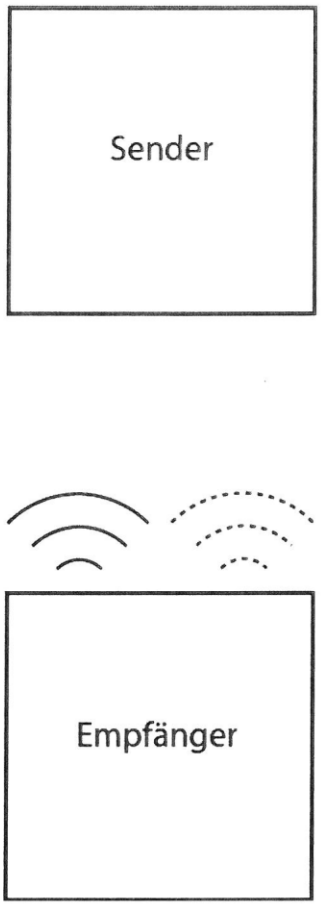


Kanalbeeinflussung

Fig. 5b

Figur 5

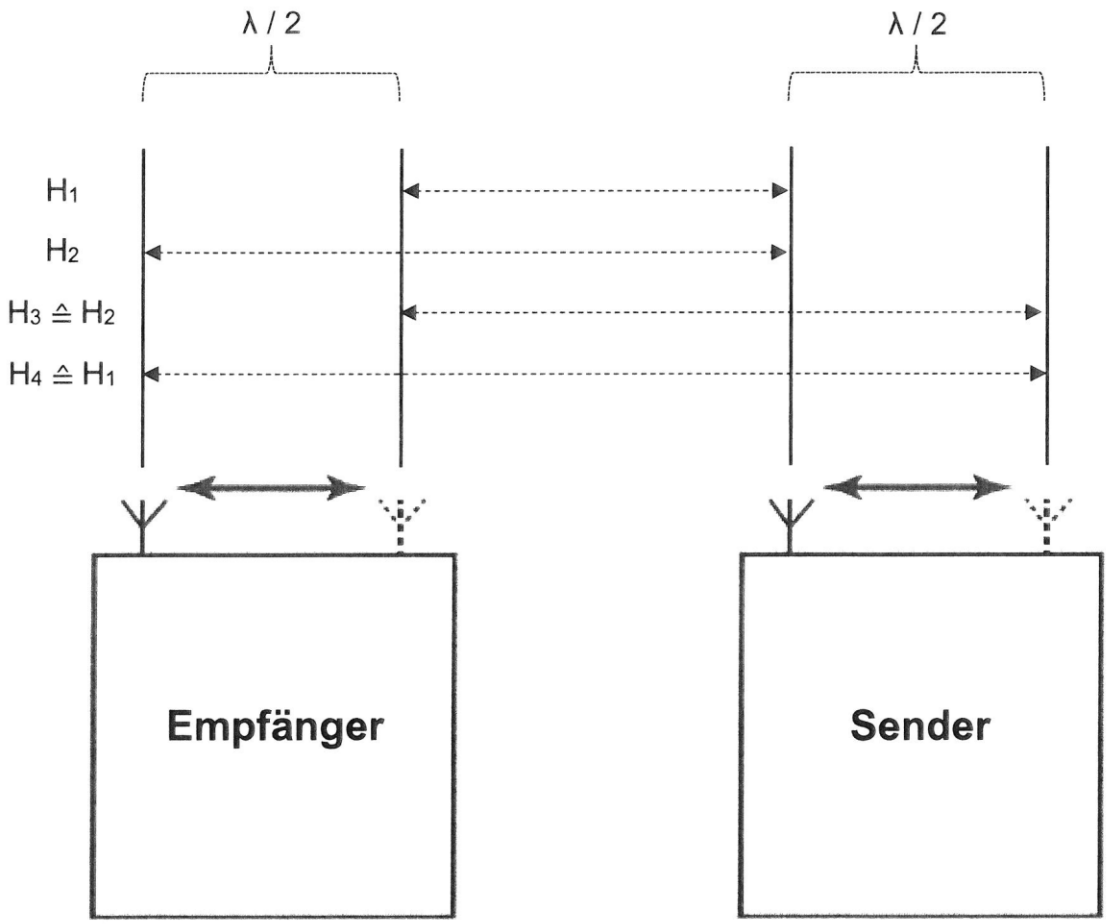
6/8



Empfänger sendet Pilotsignal

Figur 6

7/8



Figur 7

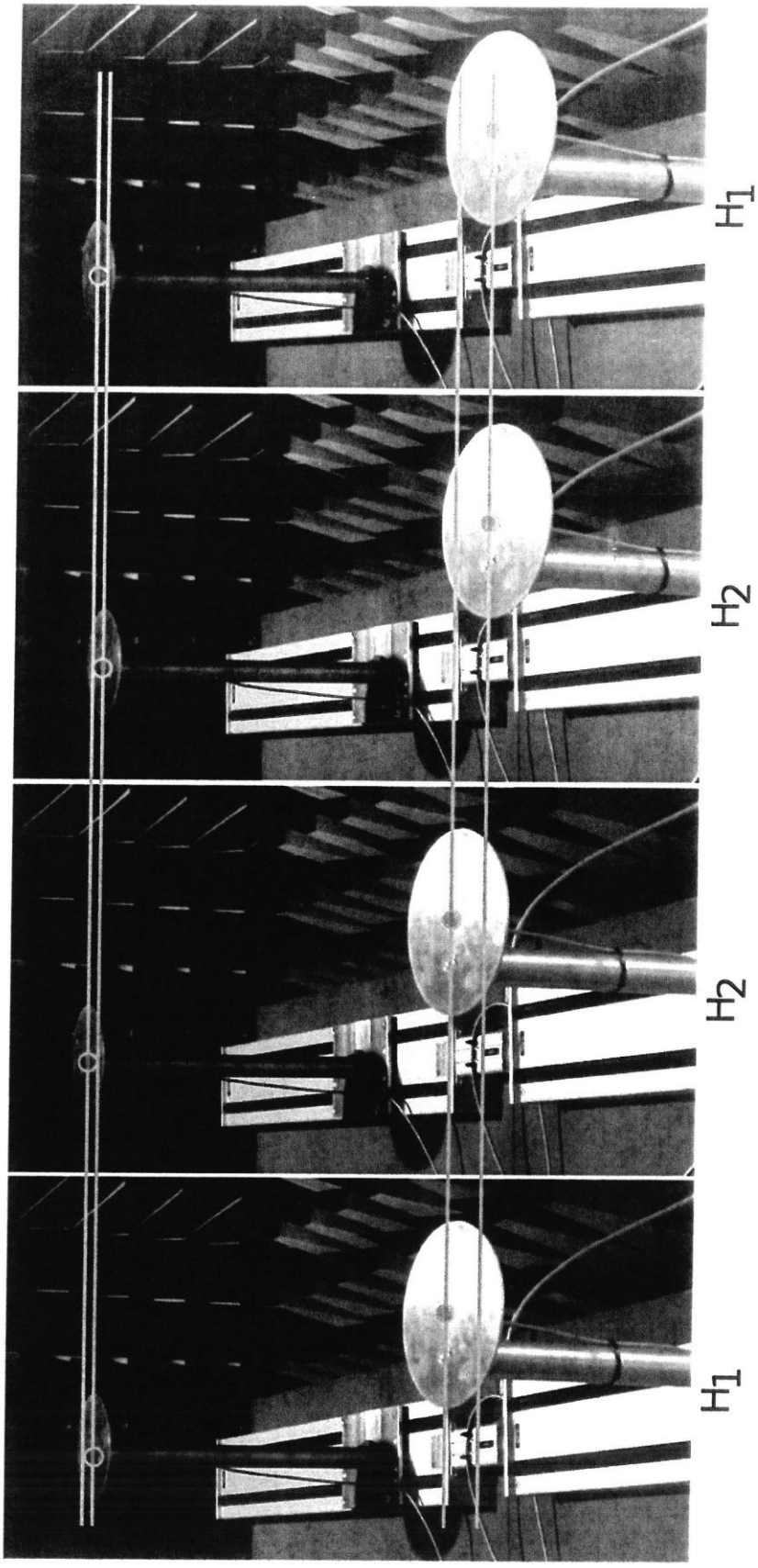


Fig. 8a

Fig. 8b

Fig. 8c

Fig. 8d

Figur 8

8/8