(19) Deutsches Patent- und Markenamt

(10) **DE 10 2015 215 569 A1** 2017.02.16

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2015 215 569.2**
(22) Anmeldetag: **14.08.2015**
(43) Offenlegungstag: **16.02.2017**

(51) Int Cl.: ***H04L 9/08*** (2006.01)
H04L 9/06 (2006.01)

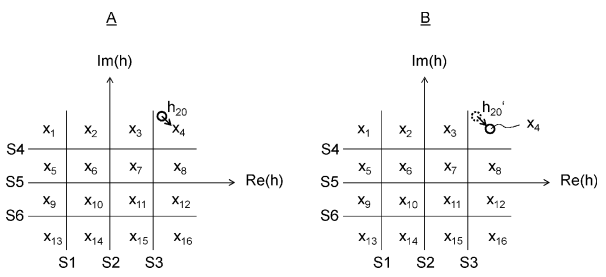
(71) Anmelder:
Robert Bosch GmbH, 70469 Stuttgart, DE

(72) Erfinder:
Ludwig, Stephan, 71272 Renningen, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren zur Generierung eines Geheimnisses zwischen Teilnehmern eines Netzwerkes sowie dazu eingerichtete Teilnehmer des Netzwerks**

(57) Zusammenfassung: Vorgestellt wird ein Verfahren zur Generierung eines gemeinsamen Geheimnisses zwischen einem ersten Teilnehmer und einem zweiten Teilnehmer eines Netzwerkes. Dabei empfängt der erste Teilnehmer von dem zweiten Teilnehmer eine erste Trainingssequenz über eine Kommunikationsverbindung zwischen dem ersten Teilnehmer und dem zweiten Teilnehmer. Der erste Teilnehmer ermittelt mindestens einen ersten Wert für mindestens eine physikalische Eigenschaft der Kommunikationsverbindung und bestimmt abhängig von dem ersten Wert einen Teil des gemeinsamen Geheimnisses. Für die Bestimmung des Teils des gemeinsamen Geheimnisses erfolgt ein Vergleich des ersten Werts mit mindestens einer Schwelle. Der erste Teilnehmer überträgt die erste Trainingssequenz an den zweiten Teilnehmer über die Kommunikationsverbindung und passt die Sendeparameter der ersten Trainingssequenz in Abhängigkeit der Lage des ersten Werts relativ zur Schwelle an.



Beschreibung

[0001] Die vorliegende Erfindung betrifft die Generierung eines gemeinsamen Geheimnisses zwischen Teilnehmern eines Netzwerkes, insbesondere zur Absicherung von Datenübertragungen zwischen den Teilnehmern.

[0002] Eine sichere Kommunikation zwischen verschiedenen Geräten wird in einer zunehmend vernetzten Welt immer wichtiger und stellt in vielen Anwendungsbereichen eine wesentliche Voraussetzung für die Akzeptanz und somit auch den wirtschaftlichen Erfolg der entsprechenden Anwendungen dar. Dies umfasst – je nach Anwendung – verschiedene Schutzziele, wie beispielsweise die Wahrung der Vertraulichkeit der zu übertragenden Daten, die gegenseitige Authentifizierung der beteiligten Knoten oder die Sicherstellung der Datenintegrität.

[0003] Zur Erreichung dieser Schutzziele kommen üblicherweise geeignete kryptographische Verfahren zum Einsatz, die man generell in zwei verschiedene Kategorien unterteilen kann: Symmetrische Verfahren, bei denen Sender und Empfänger über denselben kryptographischen Schlüssel verfügen, sowie asymmetrische Verfahren, bei denen der Sender die zu übertragenden Daten mit dem öffentlichen (d.h. auch einem potenziellen Angreifer möglicherweise bekannten) Schlüssel des Empfängers verschlüsselt, die Entschlüsselung aber nur mit dem zugehörigen privaten Schlüssel erfolgen kann, der idealerweise nur dem Empfänger bekannt ist.

[0004] Asymmetrische Verfahren haben unter anderem den Nachteil, dass Sie in der Regel eine sehr hohe Rechenkomplexität aufweisen. Damit sind sie nur bedingt für ressourcenbeschränkte Knoten, wie z.B. Sensoren, Aktuatoren, o.ä., geeignet, die üblicherweise nur über eine relativ geringe Rechenleistung sowie geringen Speicher verfügen und energieeffizient arbeiten sollen, beispielsweise aufgrund von Batteriebetrieb oder dem Einsatz von Energy Harvesting. Darüber hinaus steht oftmals nur eine begrenzte Bandbreite zur Datenübertragung zur Verfügung, was den Austausch von asymmetrischen Schlüsseln mit Längen von 2048 Bit oder noch mehr unattraktiv macht.

[0005] Bei symmetrischen Verfahren hingegen muss gewährleistet sein, dass sowohl Empfänger als auch Sender über den gleichen Schlüssel verfügen. Das zugehörige Schlüsselmanagement stellt dabei generell eine sehr anspruchsvolle Aufgabe dar. Im Bereich des Mobilfunks werden Schlüssel beispielsweise mit Hilfe von SIM-Karten in ein Mobiltelefon eingebracht und das zugehörige Netz kann dann der eindeutigen Kennung einer SIM-Karte den entsprechenden Schlüssel zuordnen. Im Fall von Wireless LANs hingegen erfolgt üblicherweise eine manuelle Eingabe der zu verwendenden Schlüssel (in der Regel durch die Eingabe eines Passwortes) bei der Einrichtung eines Netzwerkes. Ein solches Schlüsselmanagement wird allerdings schnell sehr aufwändig und impraktikabel wenn man eine sehr große Anzahl von Knoten hat, beispielsweise in einem Sensornetzwerk oder anderen Maschine-zu-Maschine-Kommunikationssystemen. Darüber hinaus ist eine Änderung der zu verwendenden Schlüssel oftmals überhaupt nicht bzw. nur mit sehr großem Aufwand möglich.

[0006] Seit einiger Zeit werden daher unter dem Schlagwort „Physical Layer Security“ neuartige Ansätze untersucht und entwickelt, mit Hilfe derer Schlüssel für symmetrische Verfahren automatisch auf der Grundlage der Übertragungskanäle zwischen den involvierten Knoten erzeugt werden können. Die Ermittlung von Zufallszahlen oder Pseudozufallszahlen aus Kanalparametern ist z.B. der WO 1996023376 A2 zu entnehmen, die Erzeugung geheimer Schlüssel aus Kanalparametern ist in der WO 2006081122 A2 und der DE 10 2012 215326 A1 offenbart. Dabei werden gewöhnlich (vorzugsweise beiden Seiten bekannte) Pilotsignalfolgen zunächst von ersten Knoten zum zweiten Knoten gesendet und dann Pilotsignalfolgen vom zweiten Knoten zum ersten Knoten gesendet. Aus den empfangenen Pilotsignalfolgen kann der jeweilige Empfänger Kanaleigenschaften abschätzen und daraus geeignete Parameter für eine Schlüsselgenerierung ableiten. Ein wichtiger Schritt ist dabei die sogenannte Quantisierung, also die Ableitung einer digitalen Bitsequenz aus den abgeschätzten Kanaleigenschaften.

[0007] Ebenfalls wurden bereits verschiedene Algorithmen zur Quantisierung und Protokolle für den Schlüssel- bzw. Geheimnisabgleich („Information Reconciliation“) zwischen den Teilnehmern vorgeschlagen. Bekannte Quantisierverfahren basieren meist auf einer oder mehreren Schwellen, welche auf Basis der Verteilung der gewonnenen Messwerte definiert werden können. Je nachdem, auf welcher Seite der Schwelle ein Messwert liegt, wird ihm ein quantisierter Wert zugeordnet. In der Regel erfolgt die Quantisierung auf beiden Seiten (in beiden Teilnehmern) unabhängig voneinander mit identischen Quantisierverfahren (und identischen Schwellen). Die dabei entstehende Sequenz ist für die Teilnehmer in der Regel in der Praxis aufgrund von Messungenauigkeiten und Schwankungen der Kanaleigenschaften nicht identisch, weswegen ein Abgleich der ermittelten geheimen Information vorteilhaft ist. Dieser Abgleich stützt sich im Wesentlichen auf den Austausch von Informationen, welche möglichst wenig Rückschlüsse auf den eigentlichen kryptografischen Schlüssel bzw. das eigentliche Geheimnis zwischen den Teilnehmern zulassen.

[0008] Eingesetzt werden für einen solchen Abgleich können z.B. das CASCADE-Protokoll, offenbart unter anderem in der Veröffentlichung Brassard, Salvail: „Secret-Key Reconciliation by Public Discussion", Advances in Cryptology, 1994, sowie fehlerkorrigierende Codes, offenbart unter anderem in der Veröffentlichung Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith: "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data", Advances in Cryptology – EUROCRYPT 2004, Lecture Notes in Computer Science Volume 3027, 2004, pp 523–540. Die bei einem solchen Abgleich ausgetauschten Paritätsbits geben Informationen preis, mit denen ein Angreifer auf Teile des geheimen Schlüssels rückschließen kann. Damit verliert dieser an Qualität bzw. Entropie. Der Angreifer muss im Falle einer „Brute-Force"-Attacke weniger Kombinationen testen, da er schon Teile des Schlüssels kennt. Um die Menge ausgetauschter Informationen möglichst gering zu halten, ist es wichtig, möglichst robuste Quantisierverfahren einzusetzen. Je robuster das Quantisierungsverfahren, desto weniger Teile eines Geheimnisses (in der Regel Bits einer jeweils erstellten Bitsequenz) sind zwischen den Teilnehmern unterschiedlich und desto weniger Informationen müssen bei einem Abgleich des Geheimnisses zwischen den Teilnehmern ausgetauscht werden.

[0009] Ein Quantisierverfahren ist offenbart in Wallace: "Secure Physical Layer Key Generation Schemes: Performance and Information Theoretic Limits", IEEE International Conference on Communications, 2009. Dabei werden zwei verschiedene Quantisierer (bzw. Quantisierungsverfahren) pro Partei verwendet. Eine Partei bestimmt für jeden Messwert des Kanals, welcher der beiden Quantisierer besser geeignet ist, d.h. einen größeren Abstand des Messwertes zur Intervallgrenze besitzt, und quantisiert mit diesem. Die Wahl wird der anderen Partei mitgeteilt.

[0010] Ein weiteres Quantisierverfahren ist offenbart in Shehadeh, Alfandi, Hogrefe: „On Improving the Robustness of Physical-layer Key Extraction Mechanisms against Delay and Mobility", Wireless Communications and Mobile Computing Conference, 2012. Dabei erfolgt die Quantisierung der komplexwertigen Messwerte jeweils auf einen aus einer Menge vorbestimmter Konstellationspunkte, von denen jeder einer Bitfolge zugeordnet ist. Die Zuordnung zu Konstellationspunkten wird abgebildet durch Gebiete in der komplexen Ebene, deren Grenzen den o.g. Schwellen entsprechen. Die Abweichung vom Konstellationspunkt (jedoch nicht der Konstellationspunkt selbst), wird von einer Partei zur anderen übertragen. Diese ändert dann ihren Messwert entsprechend. Die Übertragung der Abweichung lässt keinen Rückschluss auf den Konstellationspunkt selbst (und damit auf die ermittelte Bitfolge) zu.

Offenbarung der Erfindung

[0011] Die Erfindung betrifft Verfahren gemäß den unabhängigen Verfahrensansprüchen sowie Teilnehmer an einem Netzwerk bzw. Netzwerke, die dazu eingerichtet sind, eines der Verfahren durchzuführen. Des Weiteren betrifft die Erfindung ein Computerprogramm, das dazu eingerichtet ist, eines der Verfahren durchzuführen.

[0012] Es wird dabei vorgeschlagen, dass zwei Teilnehmer eines Netzwerkes ein gemeinsames Geheimnis (insbesondere eine gemeinsame, geheime Bitsequenz) aus Eigenschaften eines Übertragungskanals zwischen den Teilnehmern ermitteln. Der erste Teilnehmer ermittelt dabei einen Teil des Geheimnisses, indem er eine Trainingssequenz von dem zweiten Teilnehmer empfängt und dabei die Eigenschaften des Übertragungskanals ermittelt. Werte für die ermittelten Eigenschaften sind dabei abhängig von Sendeparametern (Parametern des Sendesignals) der Trainingssequenz. Über eine Quantisierung, insbesondere durch einen Vergleich der ermittelten Eigenschaften mit einem oder mehreren Schwellwerten, bestimmt der erste Teilnehmer den Teil des Geheimnisses, vorzugsweise als Bitsequenz. Im weiteren Verfahren ist vorgesehen, dass der erste Teilnehmer die Trainingssequenz ebenfalls an den zweiten Teilnehmer sendet, welcher dann eine entsprechende Quantisierung und Ableitung des Geheimnisses durchführt.

[0013] Um für möglichst viele übereinstimmende Teile des Geheimnisses (vorzugsweise übereinstimmende Bits in der gemeinsamen, geheimen Bitsequenz) zu sorgen, wird nun vorgeschlagen, dass der erste Teilnehmer die Übertragung der Trainingssequenz, speziell das Sendesignal, in Abhängigkeit davon anpasst, wie die Lage der ermittelten Werte für die physikalischen Eigenschaften des Übertragungskanals relativ zu mindestens einer Schwelle ist. Angepasst werden dabei Sendeparameter wie z.B. eine Amplitude oder Phase (äquivalente Tiefpassdarstellung) des Sendesignals. Dadurch kann der erste Teilnehmer das erwartete Ergebnis im zweiten Teilnehmer wie gewünscht manipulieren, wodurch ein flexibles Quantisierungsverfahren möglich ist. In dem ersten Teilnehmer sind hierzu vorzugsweise Informationen darüber abgelegt, wie sich eine Änderung von Sendeparametern auf Werte für die physikalische Eigenschaft des Übertragungskanals während der Übertragung der Trainingssequenz auswirkt. In der bevorzugten Ausgestaltung des Verfahrens erfolgt die Anpassung derart, dass die Schwellwertvergleiche möglichst eindeutig ausfallen, also die mit den Schwellen verglichenen Werte möglichst weit von der oder den nächsten Schwellen entfernt liegen.

[0014] Durch eine solche Anpassung der Trainingssequenz (oder auch Pilotsignalfolge) wird eine deut-

lich robustere und damit rauschtolerantere Quantisierung erreicht. Damit werden hohe Fehlerraten in den entstehenden Geheimnis-Sequenzen vermieden und bei einem gegebenenfalls folgenden Schlüssel- oder Geheimnisabgleich müssen weniger Information offenbart werden. Im Vergleich zu bekannten, robusten Quantisierverfahren ist dazu kein weiterer Informationsaustausch zwischen den Teilnehmern (z.B. über einen Abstand zwischen Wert und Schwelle oder über ein bevorzugtes Quantisierungsverfahren) nötig. Das Verfahren ist auch für reellwertige Messwerte geeignet und ebenso für mehrere Schwellen in der Amplitude und/oder Phase (z.B. höherstufige Quadratur-Amplituden-Konstellationspunkte).

[0015] Das Verfahren ist ebenfalls so flexibel, dass es unabhängig von dem verwendeten Quantisierungsverfahren und der Anzahl und den genauen Werten der Schwellen angewendet werden kann. Vorteilhafterweise arbeiten dabei aber die beteiligten Teilnehmer mit dem gleichen (ausgehandelten oder vorbestimmten) Quantisierungsverfahren und mit den gleichen Schwellen.

[0016] In bevorzugter Ausgestaltung erstellen die Teilnehmer einen gemeinsamen, symmetrischen Schlüssel auf Basis des gemeinsamen Geheimnisses (insbesondere der gemeinsamen Bitsequenz) und legen dieser eine verschlüsselten Kommunikation zugrunde.

[0017] Die Verfahren lassen sich dabei besonders gut in drahtlosen Netzwerken realisieren mit Empfangsstärke, insbesondere Received Signal Strength Indicator (RSSI), Phasenverschiebung, Dämpfung oder einer Kombination dieser Größen als physikalischer Eigenschaft und mit einer Anpassung der Sendeparamter der Trainingssequenz durch Veränderung einer Amplitude oder einer Phase des Sendesignals oder einer Kombination.

Zeichnungen

[0018] Nachfolgend ist die Erfindung unter Bezugnahme auf die beiliegenden Zeichnungen und anhand von Ausführungsbeispielen näher beschrieben. Dabei zeigen

[0019] Fig. 1 ein beispielhaftes Netzwerk mit Netzwerkteilnehmern sowie eine Einheit, die nicht Teilnehmer des Netzwerkes ist,

[0020] Fig. 2 schematisch Schritte eines beispielhaften Verfahrens zur Schlüsselerzeugung zwischen zwei Teilnehmern eines Netzwerks basierend auf Eigenschaften des Kommunikationskanals zwischen den Teilnehmern,

[0021] Fig. 3 schematisch eine Quantisierung von Messwerten aufgrund eines Vergleichs mit einem Schwellwert,

[0022] Fig. 4 schematisch eine Quantisierung von Messwerten aufgrund eines Vergleichs mit einem Schwellwert, wobei einzelne Messwerte durch eine Anpassung der zugrundeliegenden Sendesignale im Vergleich zu **Fig.** 3 verändert sind,

[0023] Fig. 5 schematisch ein Beispiel für eine zweidimensionale Quantisierung mit sechs Schwellwerten,

[0024] Fig. 6 ein Verfahren zur Generierung eines gemeinsamen Geheimnisses gemäß Stand der Technik und

[0025] Fig. 7 ein Verfahren zur Generierung eines gemeinsamen Geheimnisses durch Anpassung des Sendesignals einer Trainingssequenz-Übertragung für eine robustere Quantisierung.

Beschreibung der Ausführungsbeispiele

[0026] Die hierin beschriebenen Verfahren eignen sich zur Absicherung eines Netzwerks aus mindestens zwei Geräten, die untereinander vorzugsweise über drahtlose Kommunikationsverbindungen bzw. -kanäle kommunizieren. Die Geräte können dabei über Punkt-zu-Punkt-Verbindungen oder in einem Kommunikationsnetzwerk anderer Ausprägung miteinander verknüpft sein.

[0027] Ein möglicher Aufbau für ein Kommunikationsnetzwerk ist in **Fig.** 1 gezeigt. Dabei sind mehrere Geräte (hier: Teilnehmer A, B, C, D) in einem Kommunikationsnetzwerk **1** miteinander verknüpft, Teilnehmer A mit Teilnehmer B beispielsweise über eine Kommunikationsverbindung kAB. Zudem ist ein weiteres Gerät M gezeigt, das nicht Teilnehmer des Netzwerkes ist und demgegenüber das Netzwerk und insbesondere die Kommunikation seiner Teilnehmer abgesichert werden soll. Die Geräte bzw. Teilnehmer A, B, C, D sind insbesondere kleine, ressourcenlimitierte Sensor- oder Aktorknoten.

[0028] Bei Verfahren der sogenannten physical layer security können von zwei Geräten gemeinsame Geheimnisse (z.B. gemeinsame Bitsequenzen als Grundlage für symmetrische Schlüssel) aus physikalischen Eigenschaften des gemeinsamen Kommunikationskanals abgeleitet und gegebenenfalls ausgehandelt werden. Aus physikalischen Eigenschaften ihres gemeinsamen Übertragungskanals ermitteln die Geräte dabei jeweils Werte, insbesondere eine Bitfolge, die sie dem jeweils ermittelten Geheimnis zugrunde legen. Dabei werden die Reziprozität und die inhärente Zufälligkeit des Übertragungskanals zwischen den beteiligten Geräten ausgenutzt.

Dies kann im Detail beispielsweise ablaufen wie im Folgenden beschrieben und in **Fig.** 2 gezeigt.

[0029] Die zwei Geräte A und B schätzen in Schritten **11** bzw. **21** eine bestimmte Anzahl von Kanalparametern, evtl. auch über die Zeit. Als Kanalparameter kommen z.B. durch den Übertragungskanal bedingte Phasenverschiebungen, Dämpfungen sowie daraus abgeleitete Größen in Frage. Der Received Signal Strength Indicator (RSSI) stellt z.B. einen gängigen Indikator für die Empfangsfeldstärke kabelloser Kommunikationsanwendungen dar und kann für diese Zwecke herangezogen werden. Zur Ermittlung der Kanalparameter werden in einem Schritt **10** beiden Teilnehmern bekannte Trainingssequenzen zwischen den Teilnehmern übertragen.

[0030] Diese Kanalparameter werden von beiden Geräten in den Schritten **12** bzw. **22** geeignet quantisiert. Vorzugsweise folgen dann in den Schritten **13** bzw. **23** Maßnahmen zur Rausch- bzw. Fehlerreduktion, z.B. durch Verwendung von fehlerkorrigierenden Codes.

[0031] Mit Hilfe geeigneter Mechanismen erfolgt daraufhin in den Schritten **14** bzw. **24** ein Abgleich der quantisierten Kanalparameter zwischen den Geräten, vorzugsweise unter Verwendung eines öffentlichen Protokolls. Dies ist oft notwendig, da aufgrund von Messungenauigkeiten, Rauschen, Interferenzen, etc. beide Geräte im Allgemeinen zunächst keine identischen Parametersätze ermittelt haben. Der Abgleich erfolgt durch einen Austausch von Informationen in Schritt **20** und sollte dabei derart gestaltet sein, dass ein potenzieller Angreifer, der die ausgetauschten Daten mithören kann, davon nicht ohne Weiteres auf die quantisierten Kanalparameter schließen kann. Hierzu können beispielsweise Paritätsbits zwischen den Geräten ausgetauscht werden oder ebenfalls fehlerkorrigierende Codes eingesetzt werden.

[0032] Optional können noch in den Schritten **15** bzw. **25** eine Validierung des geteilten Geheimnisses (z.B. eine Entropieabschätzung) und in den Schritten **16** bzw. **26** eine Verbesserung des so bestimmten, geteilten Parametersatzes bzw. der geteilten Bitfolge (z.B. durch Verdichtung über Hashwert-Bildung) durchgeführt werden. Schließlich bestimmten beide Geräte auf Grundlage der derart quantisierten, verarbeiteten und abgeglichenen Kanalparameter in den Schritten **17** bzw. **27** ein geteiltes Geheimnis, das sie gegebenenfalls einer verschlüsselten Kommunikation in Schritt **30** als Schlüssel zugrunde legen können.

[0033] Dabei wird angenommen, dass ein potenzieller Angreifer einen genügend großen Abstand zu den beiden Geräten hat, in denen das geteilte Geheimnis erzeugt werden soll. Der Abstand sollte dabei mindestens in der Größenordnung der so genannten Kohärenzlänge liegen, die bei den gängigen drahtlosen Kommunikationssystemen im Bereich von wenigen Zentimetern liegt. Damit sieht der Angreifer jeweils andere (unabhängige) Übertragungskanäle zu diesen beiden Geräten und kann nicht ohne weiteres dasselbe geteilte Geheimnis rekonstruieren.

[0034] Bei den beschriebenen Verfahren wird davon ausgegangen, dass die Übertragungskanäle zwischen den Geräten ausreichende Schwankungen ihrer Kanaleigenschaften aufweisen, um daraus geeignete Kanalparameter ableiten zu können, die sich als Grundlage für eine Generierung eines geteilten Geheimnisses in den Teilnehmern eignen (insbesondere ausreichende Zufallseigenschaften aufweisen). Diese Schwankungen können dabei insbesondere sowohl im Zeit- als auch im Frequenzbereich auftreten sowie bei Mehrantennensystemen auch im räumlichen Bereich. Es wird aber auch angenommen, dass die Kanaleigenschaften über kurze Zeitspannen eine ausreichend hohe Korrelation aufweisen, dass Datenübertragungen in beide Richtungen erfolgen können, aus denen die jeweiligen Geräte trotz zeitlichen Versatzes ausreichend gleiche Kanaleigenschaften abschätzen können, um ausreichend ähnliche Kanalparameter zu erhalten, aus denen gleiche geteilte Geheimnisse erhalten werden können.

[0035] Bei bekannten Quantisierungsverfahren kann ein Wert aus der Ermittlung der physikalischen Eigenschaft des Übertragungskanals auf die Grenze zwischen zwei Quantisierintervalle fallen oder sehr nahe an einer solchen Grenze liegen, was mit großer Wahrscheinlichkeit zu ungleichen Geheimnisteilen bzw. ungleichen Bitsequenzen bei den beiden Teilnehmern führt. Dies führt wiederum dazu, dass mehr Informationen im Rahmen des Geheimnisabgleichs ausgetauscht werden müssen. Wie zuvor beschrieben, sollte aber die Menge der auszutauschenden Informationen möglichst gering gehalten werden.

[0036] In **Fig.** 3 ist eine beispielhafte Quantisierung gezeigt. Dabei werden von Teilnehmer A im Zeitverlauf (t) Werte h1 bis h13 für eine physikalische Größe y aus den Kanaleigenschaften des Übertragungskanals zu Teilnehmer B bestimmt. Zugrunde liegen Übertragungen von Trainingssequenzen (bzw. Pilotsignalfolgen) von Teilnehmer B an Teilnehmer A. Für jede Trainingssequenz ermittelt Teilnehmer A einen Wert h für die Eigenschaft y und vergleicht den Wert h mit der Schwelle S. Liegt der Wert h oberhalb der Schwelle S, quantisiert Teilnehmer A den Wert als 1, liegt er unterhalb quantisiert ihn Teilnehmer A als 0. Der Teilnehmer enthält so eine Bitsequenz aus gemessenen Kanaleigenschaften.

[0037] Gemäß dem oben beschriebenen Verfahren kann Teilnehmer A nach dem Empfang einer Trainingssequenz von Teilnehmer B seinerseits die Trainingssequenz an Teilnehmer B senden und Teilnehmer B eine entsprechende Quantisierung durchfüh-

ren. Allerdings fällt auf, dass die Werte h 8, h 10 und h 12 sehr nahe an der Schwelle S liegen. Schon durch kleine Schwankungen und Messungenauigkeiten könnte daher Teilnehmer B für diese Messwerte zu anderen Quantisierungsergebnissen kommen als Teilnehmer A (0 statt 1 bzw. 1 statt 0). Um das zu vermeiden, wird nun vorgeschlagen, dass Teilnehmer A die diesen Messwerten zugrunde liegenden Sendesignale der Übertragungen der Trainingssequenzen derart anpasst, dass die erwarteten Messwerte von Teilnehmer B weiter entfernt von der Schwelle in Richtung der von Teilnehmer A ermittelten Quantisierung liegen. Für das Beispiel, dass die physikalische Eigenschaft y eine Übertragungsstärke der Kommunikationsverbindung ist (mit steigenden Übertragungsstärken im Diagramm nach oben aufgetragen), könnte Teilnehmer A z.B. für die Trainingssequenz-Übertragung, welche Wert h8 zugrunde liegt, als Sendeparameter die Sendesignalstärke reduzieren, und für die Trainingssequenz-Übertragung, welche den Werten h10 und h12 zugrunde liegt, als Sendeparameter die Sendesignalstärke erhöhen.

[0038] In **Fig.** 4 ist gezeigt, wie eine solche Anpassung sich auf die Quantisierung durch Teilnehmer B auswirkt. Die entsprechenden, von Teilnehmer B bestimmten Werte h1‘ bis h13‘ führen nach dem Schwellwertvergleich zur gleichen Bitsequenz wie im Teilnehmer A. Die als kritisch eingeschätzten Werte h8‘, h10‘ und h12‘ liegen durch die Anpassungen der Sendeparameter entsprechenden Trainingssequenzübertragungen durch Teilnehmer A ausreichend weit von Schwellwert S entfernt, so dass auch bei kleineren Wertschwankungen oder Messungenauigkeiten nicht mit einer von Teilnehmer A abweichenden Quantisierung und damit unterschiedlichen Bitsequenzen gerechnet werden muss.

[0039] **Fig.** 5 zeigt ein Quantisierungsverfahren mit zwei Dimensionen und insgesamt sechs Schwellen (drei pro Dimension). In diesem Beispiel wird von einem komplexen Messwert h ausgegangen, der einen Imaginärteil Im(h) und einen Realteil Re(h) aufweist. Für den Realteil Re(h) sind die Schwellen S1, S2, S3 und für den Imaginärteil Im(h) die Schwellen S4, S5, S6 festgesetzt. Durch die Schwellen S1 bis S6 sind in der komplexen Ebene insgesamt 16 Gebiete definiert, denen jeweils eine Bitsequenz zugeordnet werden kann (z.B. 0000 bis 1111). Fällt ein Messwert h = Re(h) + Im(h) in ein bestimmtes Gebiet, so wird ihm im Rahmen der Quantisierung die entsprechende Bitsequenz als zugewiesen. Dabei können die Mittelpunkte solcher Gebieten als Konstellationspunkte bezeichnet werden.

[0040] Liegt ein Messwert h20 wie in **Fig.** 6 gezeigt nicht mittig in einem der Gebiete, so wird ihm trotzdem die dem Gebiet entsprechende Bitsequenz zugeordnet. Liegt der Wert allerdings nahe einer Schwelle, also nahe einer Grenze zu einem benachbarten Gebiet, so besteht wiederum die Gefahr einer unterschiedlichen Quantisierung zwischen Teilnehmer A und Teilnehmer B.

[0041] Im oben beschriebenen, aus dem Stand der Technik bekannten Quantisierungsverfahren für komplexwertige Messwerte wird daher von Teilnehmer A an Teilnehmer B zusätzlich zu einer Trainingssequenz auch noch die Information gesendet, wie weit von der Mitte des Gebietes der Messwert entfernt liegt (also hier h20 von der Mitte des Gebiets x4), und zwar über eine übermittelte Phasendifferenz d, damit Teilnehmer B seinen entsprechenden Messwert geeignet anpassen kann. Dies führt allerdings zu zusätzlichen Datenübertragungen von Teilnehmer A zu Teilnehmer B, die es zu verhindern gilt.

[0042] In **Fig.** 7 ist daher das hier vorgeschlagene Verfahren für den Fall mehrdimensionaler Quantisierung gezeigt.

[0043] Teilnehmer B sendet eine bekannte Standardtrainingsfolge (Trainingssequenz oder Pilotsignalfolge) über den gemeinsamen Übertragungskanal an Teilnehmer A, welcher diese verwendet, um mit dem Empfangssignal den Übertragungskanal zu schätzen. Der dabei ermittelte Kanalschätzwert h20 ist aufgrund des Empfängerrauschens verrauscht. In diesem Beispiel ist der Kanalschätzwert (der Messwert) komplexwertig und skalar. Im Allgemeinen kann dieser sowohl reellwertig als auch ein Vektor sein. Im Falle von reellen Werten degradieren die Quantisierungsgebiete zu Quantisierungsintervallen wie oben gezeigt. Im Falle von Vektoren ist jedes Element einzeln zu betrachten.

[0044] Teilnehmer A quantisiert nun den Messwert h20 auf den nächstgelegenen Konstellationspunkt, hier die Mitte von Gebiet x4. Die zu diesem Gebiet bzw. dessem Konstellationspunkt gehörige Bitfolge bildet nun eine Sequenz, die einem geteilten Geheimnis mit Teilnehmer B zugrunde liegen soll bzw. einem Teil des Geheimnisses.

[0045] Teilnehmer A bestimmt dann eine Anpassung der Sendesignalparameter der Übertragung der entsprechenden Standardtrainingsfolge an Teilnehmer B in Abhängigkeit der relativen Lage des Messwertes (h20) zu einer Schwelle, z.B. über die Werte des Konstellationspunktes x4 und des Messwertes h20. Die Lage zur Schwelle kann also durch einen Abstand zur Schwelle selbst oder auch durch den Wert eines über Schwellen definierten Punktes (z.B. eines Konstellationspunktes) in die Anpassung eingehen. Beispielsweise kann Teilnehmer A den Faktor x4/h20 bestimmen, die Standardtrainingsfolge B mit diesem Faktor multiplizieren und das Ergebnis B‘ = x4/h20·B an Partei 2 senden. Diese schätzt mithilfe dieser abgewandelten Trainingsfolge den Kanal (Messwert h20‘). Da der Kanal zwischen beiden Parteien reziprok ist, ent-

spricht der Messwert von Teilnehmer B (h‘ = x4/h20·h + n), wobei (n) für das Empfängerrauschen steht. Damit liegt der Erwartungswert von h‘ genau auf dem Konstellationspunkt, was die größtmögliche Robustheit/Toleranz gegen Rauschen bei Teilnehmer B bedeutet.

[0046] Wenn die Messung der Kanaleigenschaften im Rahmen einer physical layer security durch zwei Geräte also zeitlich nacheinander erfolgt (sog. time division duplex), dann kann das erste Gerät zuerst seinen Messwert quantisieren und anschließend das Messsignal für das zweite Gerät durch Veränderung eines Sendesignals so manipulieren, dass deren Messwert in die Mitte des gleichen Quantisierintervalls oder -gebiets fällt, in welchem die erste Partei seinen entsprechenden Messwert detektiert hat. Durch diese Veränderung wird keine Information über das resultierende Geheimnis an einen mithörenden Angreifer verraten.

[0047] In einer alternativen Ausgestaltung muss Teilnehmer A nicht unbedingt auf den nächsten Konstellationspunkt quantisieren, sondern kann auch auf einen beliebigen anderen quantisieren und das Sendesignal der Trainingssequenz entsprechend anpassen, so dass für den entsprechenden Messwert bei Teilnehmer B der gleiche Konstellationspunkt resultiert. Allerdings ist es sinnvoll auf dann nächsten Punkt zu quantisieren, da dann die Veränderung des Sendesignals am geringsten ist.

[0048] Um die Robustheit weiter zu erhöhen, können die Quantisierungsbereiche durch einen Schutzbereich voneinander getrennt werden. Das vorgeschlagene Vorgehen ist kombinierbar mit Multiplex-Verfahren in Raum- und/oder Frequenz-Richtung.

[0049] Das vorgeschlagene Protokoll kann besonders vorteilhaft in allen vernetzten Produkten mit Funkschnittstelle, insbesondere Geräten des sogenannten Internets der Dinge eingesetzt werden.

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

- WO 1996023376 A2 [0006]
- WO 2006081122 A2 [0006]
- DE 102012215326 A1 [0006]

Zitierte Nicht-Patentliteratur

- Brassard, Salvail: „Secret-Key Reconciliation by Public Discussion", Advances in Cryptology, 1994 [0008]
- Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith: "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data", Advances in Cryptology – EUROCRYPT 2004 [0008]
- Lecture Notes in Computer Science Volume 3027, 2004, pp 523–540 [0008]
- "Secure Physical Layer Key Generation Schemes: Performance and Information Theoretic Limits", IEEE International Conference on Communications, 2009 [0009]
- Shehadeh, Alfandi, Hogrefe: „On Improving the Robustness of Physical-layer Key Extraction Mechanisms against Delay and Mobility", Wireless Communications and Mobile Computing Conference, 2012 [0010]

Patentansprüche

1. Verfahren zur Generierung eines gemeinsamen Geheimnisses zwischen einem ersten Teilnehmer (A) und einem zweiten Teilnehmer (B) eines Netzwerkes (**1**), wobei der erste Teilnehmer (A) von dem zweiten Teilnehmer (B) eine erste Trainingssequenz über eine Kommunikationsverbindung (kAB) zwischen dem ersten Teilnehmer (A) und dem zweiten Teilnehmer (B) empfängt, wobei der erste Teilnehmer mindestens einen ersten Wert (h) für mindestens eine physikalische Eigenschaft der Kommunikationsverbindung (kAB) ermittelt, wobei der erste Teilnehmer (A) abhängig von dem ersten Wert (h) einen Teil des gemeinsamen Geheimnisses bestimmt, wobei für die Bestimmung des Teils des gemeinsamen Geheimnisses ein Vergleich des ersten Werts (h) mit mindestens einer Schwelle (S) erfolgt und wobei der erste Teilnehmer (A) die erste Trainingssequenz an den zweiten Teilnehmer (B) über die Kommunikationsverbindung (kAB) sendet, **dadurch gekennzeichnet,** dass der erste Teilnehmer (A) Sendeparameter der ersten Trainingssequenz in Abhängigkeit der Lage des ersten Werts (h) relativ zur Schwelle (S) anpasst.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,** dass der erste Teilnehmer (A) die Sendeparameter der ersten Trainingssequenz in Abhängigkeit eines Abstands des ersten Werts (h) relativ zur Schwelle (S) anpasst.

3. Verfahren nach einem der vorangegangenen Ansprüche, **dadurch gekennzeichnet,** dass die angepassten Sendeparameter derart angepasst werden, dass sich ein ermittelter Wert (h) für die physikalische Eigenschaft der Kommunikationsverbindung (kAB) bei der Übertragung von der Schwelle entfernt.

4. Verfahren nach einem der vorangegangenen Ansprüche, **dadurch gekennzeichnet,** dass der erste Teilnehmer (A) und der zweite Teilnehmer (B) aus dem gemeinsamen Geheimnis einen gemeinsamen, symmetrischer Schlüssel ableitet.

5. Verfahren nach Anspruch 4, **dadurch gekennzeichnet,** dass der erste Teilnehmer (A) und der zweite Teilnehmer (B) den gemeinsamen, symmetrischen Schlüssel einer verschlüsselten Kommunikation zugrunde legen.

6. Verfahren nach einem der vorangegangenen Ansprüche, **dadurch gekennzeichnet,** dass das Netzwerk (**1**) drahtlos ist.

7. Verfahren nach einem der vorangegangenen Ansprüche, **dadurch gekennzeichnet,** dass die physikalische Eigenschaft eine Empfangsstärke, insbesondere ein Received Signal Strength Indicator (RSSI), oder eine Phasenverschiebung oder eine Dämpfung oder eine aus einer oder mehrere dieser Größen abgeleitete Größe darstellt.

8. Verfahren nach einem der vorangegangenen Ansprüche, **dadurch gekennzeichnet,** dass die Anpassung der Sendeparamter durch eine Veränderung einer Amplitude oder einer Phase des Sendesignals erfolgt oder durch eine Veränderung der Amplitude und einer Phase des Sendesignals erfolgt.

9. Teilnehmer (A) an einem Netzwerk (**1**), welcher dazu eingerichtet ist, ein Verfahren nach einem der Ansprüche 1 bis 8 durchzuführen.

10. Netzwerk (**1**) mit mindestens zwei Teilnehmern (A, B) nach Anspruch 9.

11. Computerprogramm, welches dazu eingerichtet ist, die Schritte eines Verfahrens nach einem der Ansprüche 1 bis 8 durchzuführen.

12. Maschinenlesbares Speichermedium mit einem Computerprogramm nach Anspruch 11.

Es folgen 7 Seiten Zeichnungen

Anhängende Zeichnungen

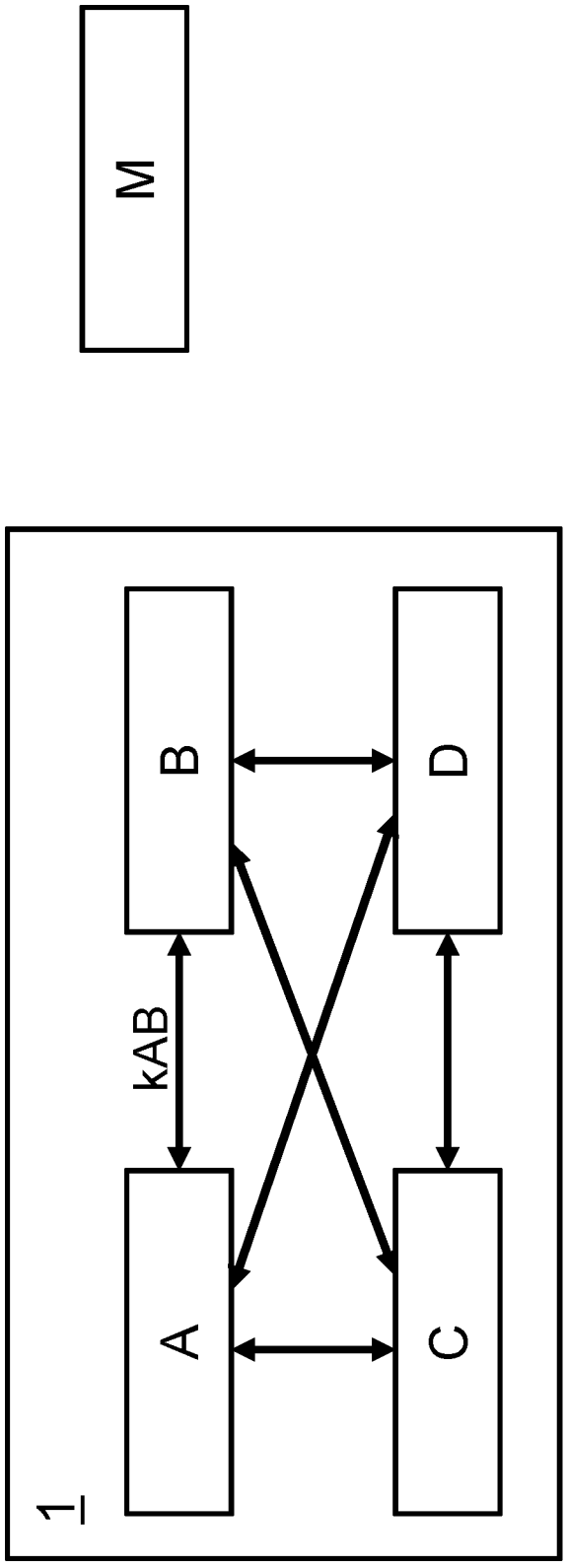


Fig. 1

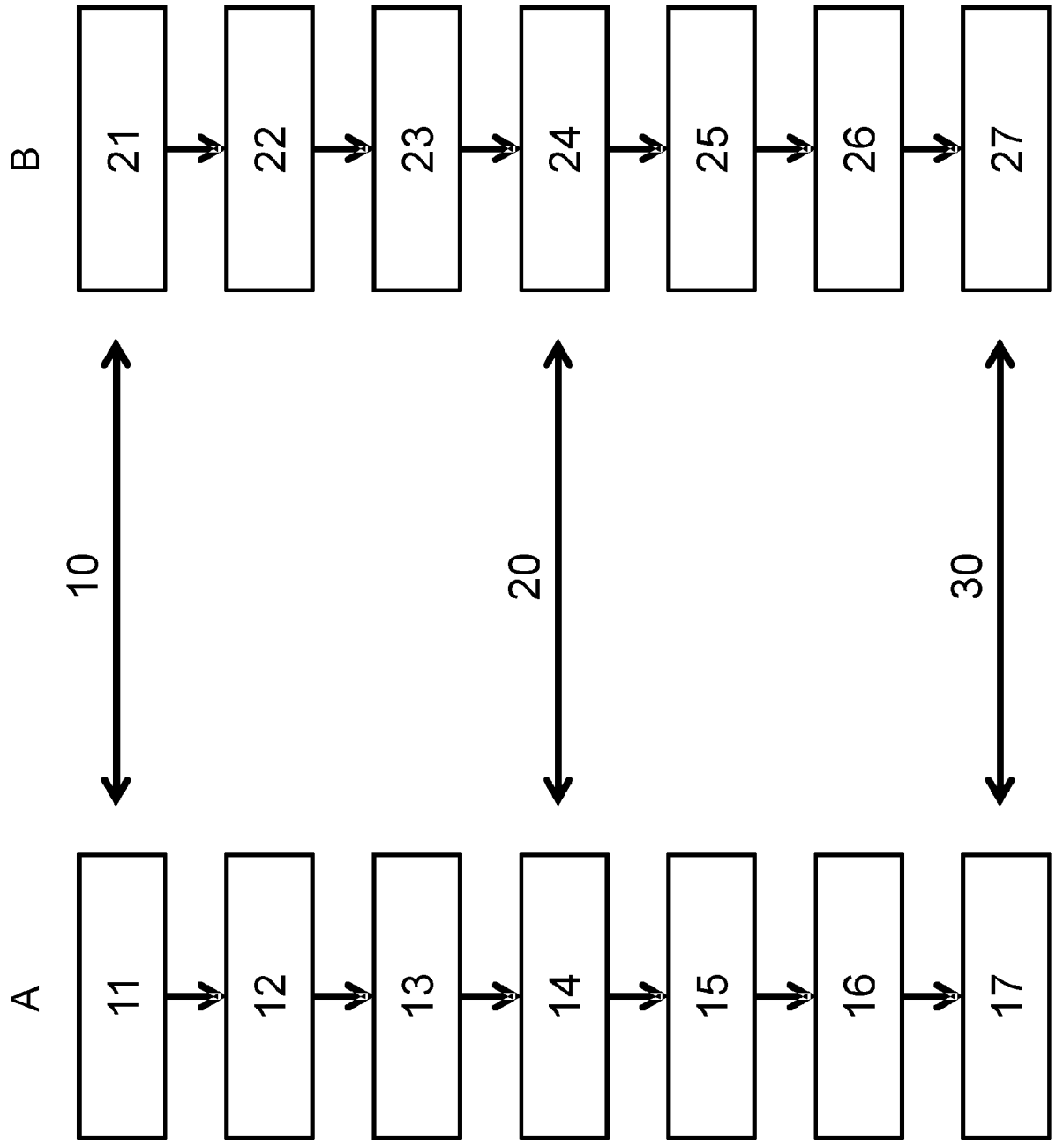


Fig. 2

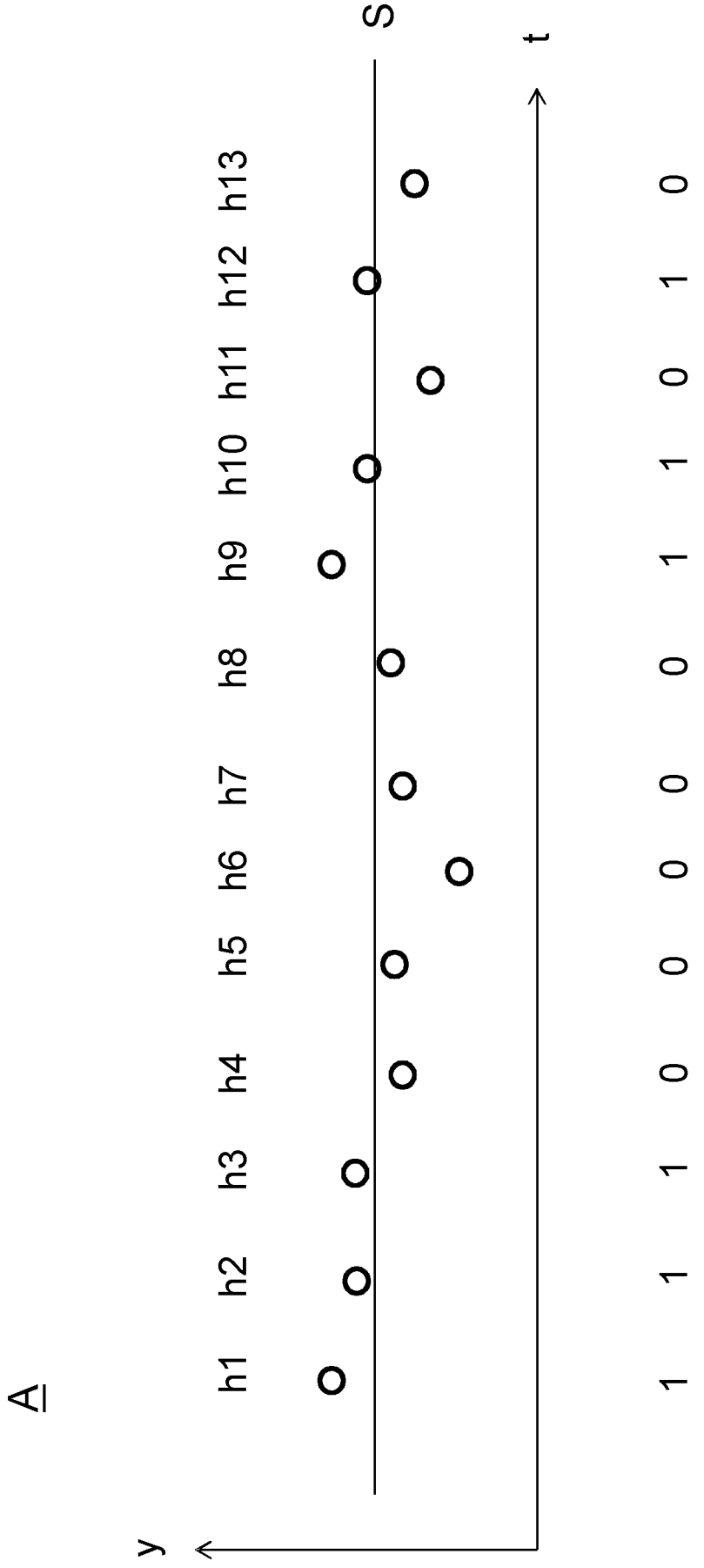


Fig. 3

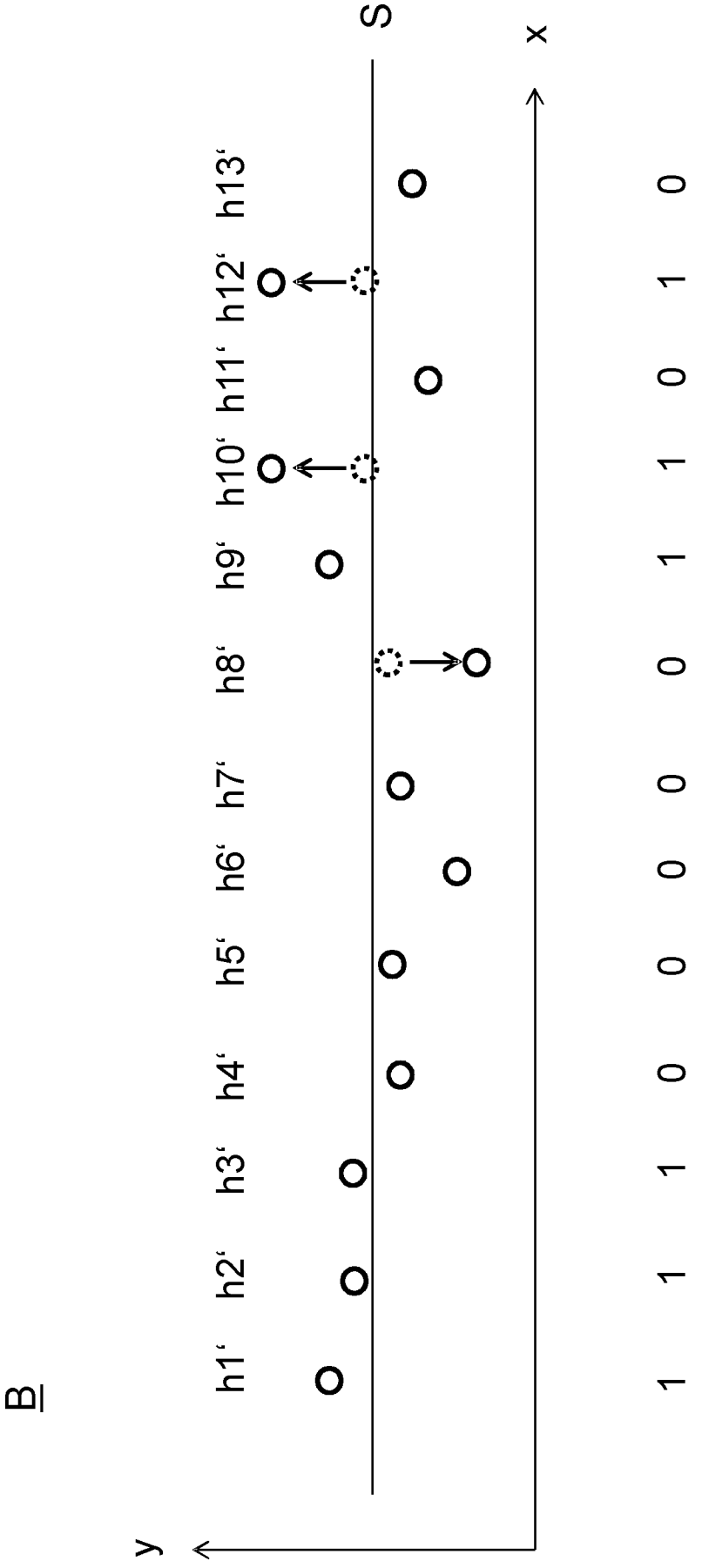


Fig. 4

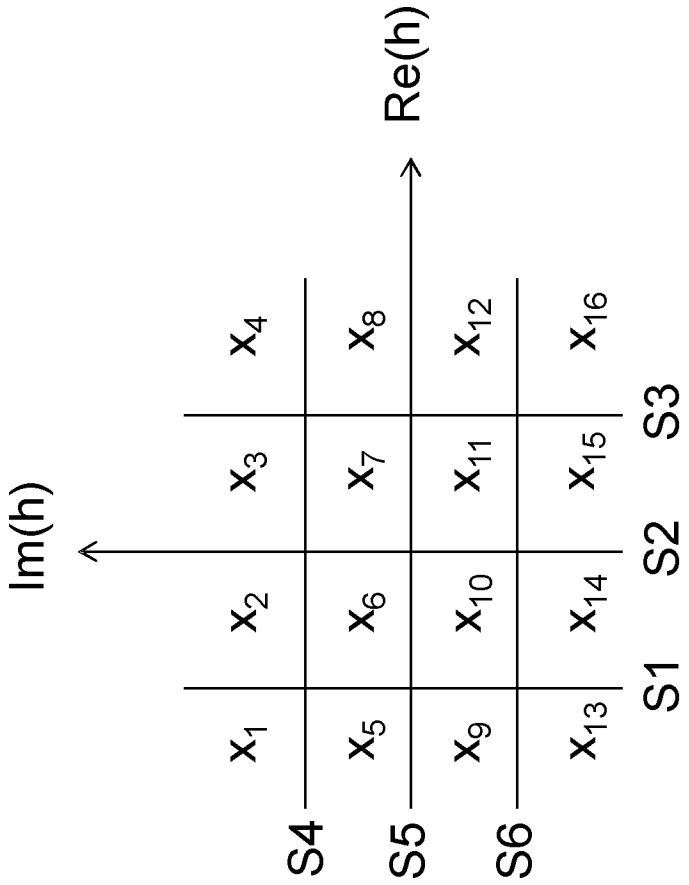

Im(h)
Re(h)
S1
S2
S3
S4
S5
S6
x1
x2
x3
x4
x5
x6
x7
x8
x9
x10
x11
x12
x13
x14
x15
x16

Fig. 5

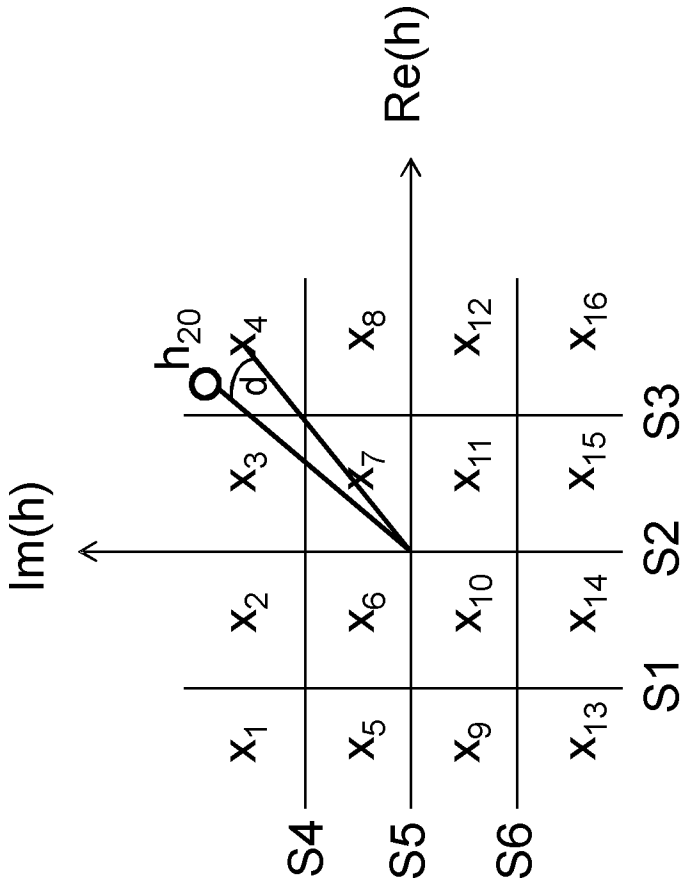

Im(h)
Re(h)
h20
d
x1
x2
x3
x4
x5
x6
x7
x8
x9
x10
x11
x12
x13
x14
x15
x16
S1
S2
S3
S4
S5
S6

Fig. 6

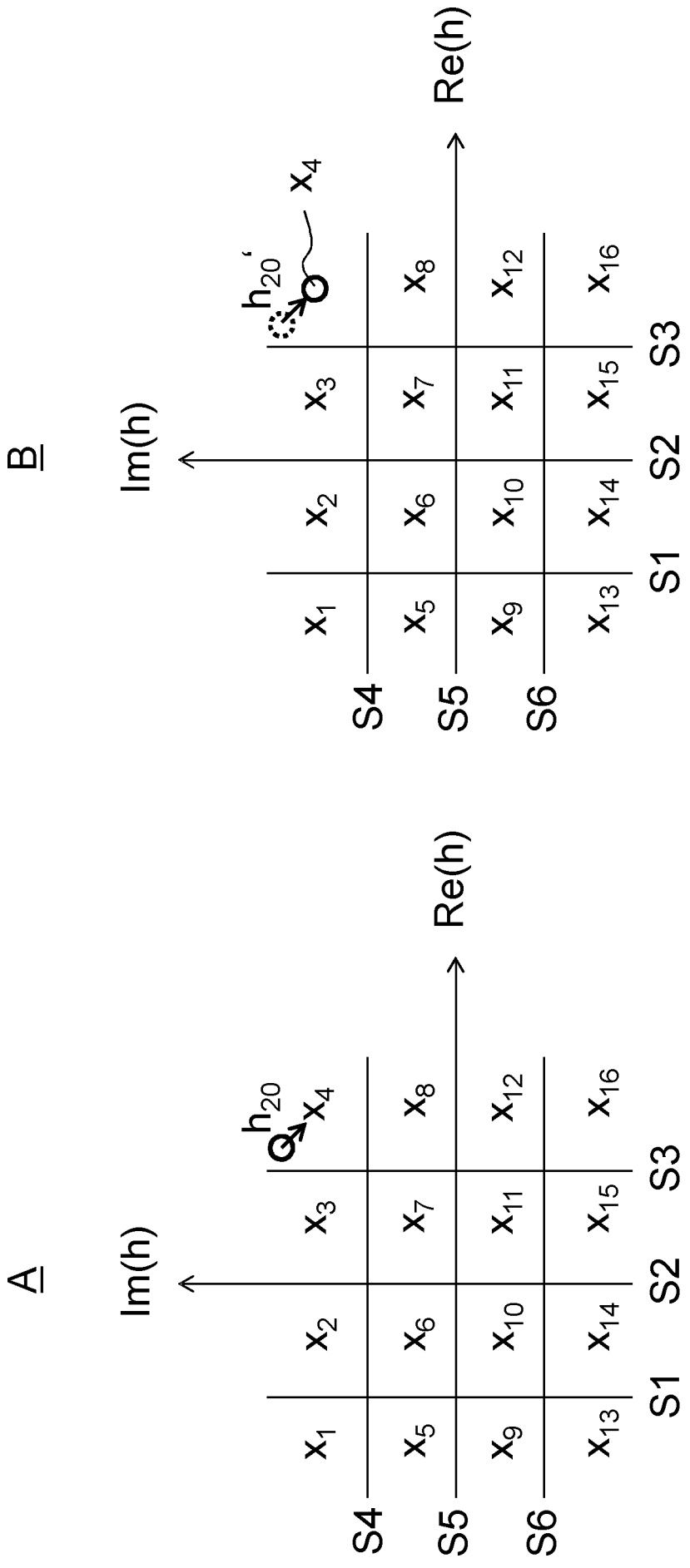

A
B
Im(h)
Re(h)
S1
S2
S3
S4
S5
S6
x1
x2
x3
x4
x5
x6
x7
x8
x9
x10
x11
x12
x13
x14
x15
x16
h20
h20'

Fig. 7