(19) österreichisches patentamt

(10) **AT 519476 B1 2018-07-15**

(12) # Patentschrift

(21) Anmeldenummer: A 50280/2017
(22) Anmeldetag: 05.04.2017
(45) Veröffentlicht am: 15.07.2018

(51) Int. Cl.: ***G06F 11/08*** (2006.01)
G06F 11/10 (2006.01)
G06F 21/40 (2013.01)
G06F 21/42 (2013.01)
H04L 1/00 (2006.01)
H04L 9/08 (2006.01)

(56) Entgegenhaltungen:
DE 3919734 C1
DE 10059230 A1
Todd K. MOON: "Error Correction Coding. Mathematical Methods and Algorithms." Wiley-Interscience, Hoboken NJ, USA, 2005. ISBN 0-471-64800-0.
EP 2515499 A1
US 2013145170 A1

(73) Patentinhaber:
AIT Austrian Institute of Technology GmbH
1220 Wien (AT)

(72) Erfinder:
Lorünser Thomas
1100 Wien (AT)
Krenn Stephan
2340 Mödling (AT)
Schrenk Bernhard
2122 Ulrichskirchen (AT)
Pacher Christoph
1200 Wien (AT)

(74) Vertreter:
Wildhack & Jellinek Patentanwälte OG
1030 Wien (AT)

(54) **Verfahren zur Erstellung und Verteilung von kryptographischen Schlüsseln**

(57) Die Erfindung betrifft ein Verfahren zur Erstellung und Verteilung von kryptographischen Schlüsseln, insbesondere zum Schutz der Kommunikation auf zwei Endgeräten (A, B),

a) wobei über einen fehlerbehafteten ersten Kommunikationskanal (Q), insbesondere über einen Quantenkommunikationskanal, Signale zur Erstellung korrelierter Werte in den beiden Endgeräten (A, B) verteilt werden, und diese korrelierten Werte derart als Schlüssel (k_A, k_B) in den beiden Endgeräten vorliegen,

b) basierend auf dem im ersten Endgerät (A) vorliegenden ersten Schlüssel (k_A) eine Prüfsumme (s_A) gebildet wird und diese Prüfsumme (s_A) über einen vom ersten Kommunikationskanal (Q) verschiedenen zweiten Kommunikationskanal (L) an das zweite Endgerät (B) übertragen wird,

c) basierend auf dem im zweiten Endgerät (B) vorliegenden zweiten Schlüssel (k_B) eine zweite Prüfsumme (s_B) gebildet wird und die beiden Prüfsummen (s_A, s_B) oder die Differenz (s_{err}) der beiden Prüfsummen (s_A, s_B) oder daraus abgeleitete Informationen über den zweiten Kommunikationskanal (L) an einen von den beiden Endgeräten (A, B) verschiedenen und von diesem räumlich getrennten Server (C) übertragen wird,

d) dass der Server (C) basierend auf den beiden Prüfsummen (s_A, s_B) oder der Differenz (s_{err}) der beiden Prüfsummen (s_A, s_B) oder den daraus abgeleiteten Informationen einen Korrekturwert (k_{err}) ermittelt, der bei Anwendung auf einen oder beide Schlüssel (k_A, k_B) die Schlüssel (k_A, k_B) zur Übereinstimmung bringt, und

e) dass der Korrekturwert (k_{err}) an eines oder beide Endgeräte (A, B) über den zweiten Kommunikationskanal (L) übertragen wird und auf einen oder beide Schlüssel (k_A, k_B) angewendet wird.

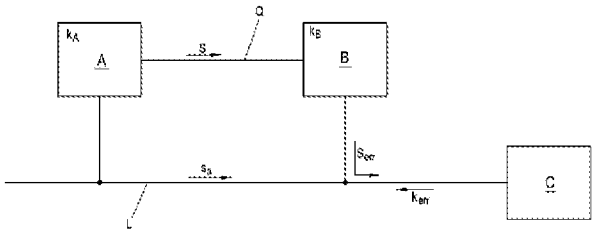

Fig. 1

AT 519476 B1 2018-07-15

Beschreibung

VERFAHREN ZUR ERSTELLUNG UND VERTEILUNG VON KRYPTOGRAPHISCHEN SCHLÜSSELN

[0001] Die Erfindung betrifft ein Fehlerkorrektur-Verfahren zur Erstellung und Verteilung eines Schlüssels für zwei Endgeräte zur Verwendung als Kryptografieschlüssel im Rahmen eines symmetrischen Kryptographieverfahrens.

[0002] Aus dem Stand der Technik ist es bekannt, zwischen zwei Endgeräten einen kryptographischen Schlüssel mittels Quantenkommunikation zu erzeugen. Die Übertragung des Schlüssels über einen Quantenkommunikationskanal oder einen anderen stark fehlerbehafteten Kanal bewirkt, dass in den beiden Endgeräten in den betreffenden Endgeräten voneinander verschiedene Schlüssel enthalten sind. Aus dem Stand der Technik ist es auch bekannt, einen der beiden oder beide Schlüssel derart zu korrigieren, dass die beiden Schlüssel gleich sind und diese beiden Schlüssel im Rahmen eines symmetrischen Kryptographieverfahrens bei der Kommunikation zwischen den beiden Endgeräten verwendet werden können. Um diese Korrektur vorzunehmen, wird typischerweise in einem der beiden Endgeräte, basierend auf einem Schlüssel und einer öffentlich bekannten Prüfmatrix, eine Prüfsumme gebildet und diese an das andere Endgerät übermittelt. Dabei sind Verfahren bekannt, mit denen der Schlüssel des zweiten Endgeräts derart abgeändert wird, dass die Prüfsumme derjenigen Prüfsumme entspricht, die sich als Produkt der Prüfmatrix und des ersten Schlüssels ergibt. Solche Verfahren sind beispielsweise aus Todd K. Moon: Error Correction Coding. Mathematical Methods and Algorithms. Wiley-Interscience, Hoboken NJ, 2005, ISBN 0-471-64800-0 bekannt.

[0003] Wesentlicher Nachteil dieser Vorgehensweise ist, dass die Korrektur des Schlüssels äußerst rechenaufwändig ist und nach erstmaliger Übertragung des Schlüssels zu einer hohen Ressourcenbelastung des den Schlüssel korrigierenden Endgeräts führt.

[0004] Aus dem Stand der Technik ebenfalls bekannte Maßnahmen zur externen Berechnung von Daten, beispielsweise die Durchführung des zur Korrektur des Schlüssels erforderlichen Algorithmus in einem Rechenzentrum, hat jedoch das wesentliche Problem, dass der notwendigerweise geheime Schlüssel das Endgerät verlässt und an ein nicht notwendigerweise zuverlässiges Rechenzentrum übertragen werden muss.

[0005] Aufgabe der Erfindung ist es, ein Schlüsselkorrekturverfahren zu schaffen, das auf einem Rechner ausführbar ist, der über größere Rechenkapazität verfügt und der geringeren Anforderungen hinsichtlich der Vertraulichkeit zu genügen braucht.

[0006] Die Erfindung löst diese Aufgabe mit den Merkmalen des Patentanspruchs 1.

[0007] Erfindungsgemäß ist vorgesehen, dass

[0008] a) über einen fehlerbehafteten ersten Kommunikationskanal, insbesondere über einen Quantenkommunikationskanal, Signale zur Erstellung korrelierter Werte in den beiden Endgeräten verteilt werden, und diese korrelierten Werte derart als Schlüssel in den beiden Endgeräten vorliegen,

[0009] b) basierend auf dem im ersten Endgerät vorliegenden ersten Schlüssel eine Prüfsumme gebildet wird und diese Prüfsumme über einen vom ersten Kommunikationskanal verschiedenen zweiten Kommunikationskanal an das zweite Endgerät übertragen wird,

[0010] c) basierend auf dem im zweiten Endgerät vorliegenden zweiten Schlüssel eine zweite Prüfsumme gebildet wird und die beiden Prüfsummen oder die Differenz der beiden Prüfsummen oder daraus abgeleitete Informationen über den zweiten Kommunikationskanal an einen von den beiden Endgeräten verschiedenen und von diesem räumlich getrennten Server übertragen wird,

[0011] d) dass der Server basierend auf den beiden Prüfsummen oder der Differenz der beiden Prüfsummen oder den daraus abgeleiteten Informationen einen Korrekturwert ermittelt, der bei

Anwendung auf einen oder beide Schlüssel die Schlüssel zur Übereinstimmung bringt, und

[0012] e) dass der Korrekturwert an eines oder beide Endgeräte über den zweiten Kommunikationskanal übertragen wird und auf einen oder beide Schlüssel angewendet wird.

[0013] Ein wesentlicher Vorteil des erfindungsgemäßen Vorgehens liegt darin, dass der für die Bildung des Korrekturwerts verwendete Server beliebigen anderen Personen offen stehen kann und keine konkrete Sicherheitsfreigabe für den Server erforderlich ist.

[0014] Darüber braucht der für die Kommunikation zwischen dem Server und den Erdgeräten verwendete Kommunikationskanal nicht abhörsicher zu sein.

[0015] Eine besonders einfache, initiale Verteilung der Schlüssel auf die beiden Endgeräte sieht vor, dass die Signale zur Erstellung korrelierter Werte in den beiden Endgeräten verteilt werden, indem

[0016] - vom ersten Endgerät ein zufälliges Signal erstellt wird und, insbesondere mittels Quantenkommunikation, an das zweite Endgerät übertragen wird, oder

[0017] - vom zweiten Endgerät ein zufälliges Signal erstellt wird und, insbesondere mittels Quantenkommunikation, an das erste Endgerät übertragen wird, oder

[0018] - von einer externen Signalquelle ein verschränkter Quantenzustand erzeugt und mittels Quantenkommunikation an beide Endgeräte übertragen werden.

[0019] Eine weitere Verbesserung der Sicherheit kann erreicht werden, indem zu Bildung der korrelierten Werte Teile des übertragenen Signals ausgewählt werden und die übrigen Teile des übertragenen Signals verworfen werden.

[0020] Ein besonders effizientes Vorgehen, das eine einfache Korrektur der Schlüssel aufgrund einer linearen Vorgehensweise ermöglicht, sieht vor,

[0021] - dass ein Schlüssel als Binärvektor einer vorgegebenen Länge angegeben wird,

[0022] - dass eine öffentlich bekannte Prüfmatrix umfassend Binärzahlen als Einträge vorgegeben wird, deren Zeilenzahl der Länge der Schlüssel und deren Spaltenzahl der Länge der Prüfsummen entspricht und

[0023] - dass die Prüfsummen durch Bildung einer Matrix-Vektor-Multiplikation gebildet wird, wobei als Addition von Bits die XOR-Operation und als Multiplikation von Bits die AND-Operation verwendet wird.

[0024] Ebenso kann zu diesem Zweck vorgesehen sein,

[0025] - dass ein Schlüssel als Vektor einer vorgegebenen Länge angegeben wird, dessen Elemente aus einem Galois-Körper stammen,

[0026] - dass eine öffentlich bekannte Prüfmatrix umfassend Elemente aus einem Galois-Körper als Einträge vorgegeben wird, deren Zeilenzahl der Länge der Schlüssel und deren Spaltenzahl der Länge der Prüfsummen entspricht und

[0027] - dass die Prüfsummen durch Bildung einer Matrix-Vektor-Multiplikation gebildet wird, wobei als Addition und Multiplikation die betreffenden Operationen des Elemente aus einem Galois-Körper verwendet werden.

[0028] Um die Übertragungssicherheit zu erhöhen, insbesondere um auszuschließen, dass Angreifer genug Information über den Schlüssel durch jegliches Mithören im Rahmen des Schlüsselaustauschs oder des Schlüsselabgleichs erlangen, kann vorgesehen sein, dass die Länge der Schlüssel auf vorab vorgegebene Weise um eine Anzahl von Bits reduziert wird, die zumindest der Anzahl der Bits der Prüfsumme entspricht.

[0029] Nach Austausch der Schlüssel ist eine abhörsichere Datenübertragung möglich, wobei zwischen den beiden Endgeräten Nachrichten ausgetauscht werden, die mittels eines symmetrischen Kryptographieverfahrens jeweils unter Verwendung des in den Endgeräten abgespei-

cherten Schlüssels geschützt wurden.

[0030] Nach Austausch der Schlüssel ist es möglich die Authentizität übermittelter Nachrichten zu prüfen, indem zwischen den Endgeräten Nachrichten ausgetauscht werden, wobei jeder der Nachrichten jeweils ein Hash-Wert angehängt wird, die sich auf vorgegebene Weise aus dem Schlüssel und aus der in der Nachricht zu übertragenden Information ergibt,

[0031] wobei das jeweils empfangende Endgerät beim Erhalt überprüft, ob sich der übermittelte Hash-Wert auf vorgegebene Weise aus dem Schlüssel und aus der in der Nachricht zu übertragenden Information ergibt und in diesem Fall die Authentizität der Nachricht festgestellt wird.

[0032] Eine bevorzugte Ausführungsform der Erfindung wird anhand der Zeichnungsfigur näher dargestellt.

[0033] In Fig. 1 sind die Endgeräte A, B zweier Kommunikationsteilnehmer dargestellt, die über einen potentiell unsicheren zweiten Kommunikationskanal L sowie über einen ersten Kommunikationskanal Q, insbesondere über einen Quantenkommunikationskanal, miteinander verbunden sind. Im vorliegenden Ausführungsbeispiel der Erfindung verfügt das Endgerät A über eine Sendeeinrichtung, mit der über den ersten Kommunikationskanal Q Signale an das Endgerät B übertragen werden können. Das Endgerät B verfügt über eine Empfangseinrichtung, mit der Signale über den ersten Kommunikationskanal Q vom Endgerät A ausgehende Signale empfangen werden können.

[0034] Als über den ersten Kommunikationskanal Q zu übertragende Signale werden typischerweise Quantensignale verwendet, die lediglich durch eine sehr geringe Anzahl von Photonen repräsentiert sind. Im Rahmen der Quantenkommunikation ist es auf diese Weise möglich, Angreifer zu detektieren, da im Falle des Auslesens einzelner Signale über den ersten Kommunikationskanal Q Störungen auf dem Kanal bewirkt werden, sodass das Signal beim empfangenden Endgerät B überhaupt nicht oder nur mit Störungen ankommt. Es können jedoch auch alternativ andere Signale über einen Kommunikationskanal Q übertragen werden, bei denen der Angreifer auch nicht in der Lage ist das vollständige Signal zu kopieren.

[0035] Als Signal wird vorteilhafterweise vom ersten Endgerät A ein zufälliges Datensignal über den ersten Kommunikationskanal Q übermittelt. Dieses Datensignal wird darüber hinaus als Schlüssel k_A abgespeichert. Das zweite Endgerät B speichert das über den ersten Kommunikationskanal Q empfangene Datensignal als Schlüssel k_B ab.

[0036] Darüber hinaus kann bei der Verteilung des Schlüssels vorgesehen sein, dass das Signal erzeugende Endgerät A die einzelnen, das Signal erzeugenden Photonen mit einer ständig wechselnden Polarisation aussendet. Dabei kann das Endgerät B seinen Empfänger ebenfalls auf unterschiedliche Polarisation einstellen, wobei die Polarisation der ausgesendeten Photonen mit der Polarisation des Empfangsgeräts im zweiten Endgerät B nicht abgestimmt sind. Erst nah der Übertragung des Signals stimmen die beiden Endgeräte A, B in einem Abgleichschritt diejenigen Signalanteile untereinander ab, bei der die Polarisation der vom ersten Endgerät A ausgesandten Photonen der Polarisation des Empfangsgeräts des zweiten Endgeräts B entspricht. Die übrigen Signalanteile, bei denen die Polarisation des vom Endgerät A ausgesandten Signalanteils mit der Polarisation des Empfangsgeräts des zweiten Endgeräts B nicht übereinstimmt, werden verworfen. Werden in beiden Endgeräten A, B zwei Polarisationsrichtungen vorgegeben, reduziert sich der Informationsgehalt des für die Bildung des Schlüssels zur Verfügung stehenden Signals um die Hälfte.

[0037] Um einen Abgleich durchzuführen, tauschen die beiden Endgeräte nach der Übertragung des Schlüssels die jeweils verwendete Polarisationsrichtung untereinander aus und können damit für den jeweils bei ihnen vorliegenden Signalanteil bzw. Schlüssel feststellen, welche der Bits mit aufeinander abgestimmten Sende- und Empfangseinrichtungen gesendet wurden. Die übrigen Bits des jeweiligen Schlüssels werden verworfen. Die jeweils verwendeten Polarisationen werden erst ausgetauscht, nachdem das Signal vom ersten Endgerät A an das zweite Endgerät B über den ersten Kommunikationskanal Q übertragen wurde. Von besonderem Vorteil ist es dabei, dass der Austausch der jeweils für das Senden und Empfangen verwende-

ten Polarisationsrichtungen einem Angreifer keinerlei Information über den ausgetauschten Schlüssel gibt.

[0038] Nach diesem initialen Schritt des Schlüsselabgleichs liegt nunmehr jeweils ein Schlüssel k_A, k_B in jedem der beiden Endgeräte A, B vor. Aufgrund von nicht perfekten Übertragungseigenschaften des Kanals und dem möglichen Einfluss von Angreifern sind die Schlüssel k_A, k_B nicht identisch.

[0039] In einem ersten Schritt erstellt nun eines der beiden Endgeräte, im vorliegenden Fall das erste Endgerät A, basierend auf dem bei ihm vorliegenden Schlüssel k_A eine Prüfsumme s_A. Die Bildung dieser Prüfsumme kann auf unterschiedliche Weise erfolgen, wobei im vorliegenden Ausführungsbeispiel eine Variante gewählt wird, die zu einer numerisch besonders einfachen Behandlung führt. Dabei wird der Schlüssel k_A als Bit-Vektor, umfassend eine Vielzahl von einzelnen Bits, angesehen. Darüber hinaus wird eine öffentlich bekannte Prüfmatrix P einer vorgegebenen Größe zwischen den beiden Endgeräten A, B vereinbart, die auch beliebigen Angreifern bekannt sein kann.

[0040] Die im Rahmen der Prüfsummenbildung verwendete Prüfmatrix P weist eine Anzahl von Zeilen auf, die mit der Anzahl der Elemente im Zeilen-Vektor des Schlüssels k_A übereinstimmt. Die Prüfmatrix P weist eine Anzahl von Spalten auf, die mit der Anzahl der gewünschten Einträge im Spalten-Vektor der Prüfsumme s_A übereinstimmt. Die konkrete Bildung von Prüfmatrizen ist vorteilhaft in Information Theory, Inference, and Learning Algorithms, by David J.C. MacKay, discusses LDPC codes in Chapter 47 näher dargestellt.

[0041] Für die Bildung eines Prüfsummen-Vektors s_A wird eine Matrix-Vektor-Multiplikation zwischen der Prüfmatrix P und dem, hier als Zeilen-Vektor dargestellten, Schlüssel-Vektor k_A durchgeführt, woraufhin man einen Zeilen-Prüfsummenvektor s_A erhält. Im vorliegenden Ausführungsbeispiel wird zur einfachen Darstellung ein binärer Vektor für den Schlüssel k_A, eine mit Binärzahlen gefüllte Prüfmatrix P und ein mit Binärzahlen gefüllter Spalten-Vektor als Prüfsumme s_A verwendet. Wird im Rahmen der Vektor-Matrix-Multiplikation eine Multiplikation zwischen einzelnen Binärzahlen benötigt, so verwendet man hierfür die AND-Operation. Wird im Rahmen der Matrix-Vektor-Multiplikation eine Addition benötigt, werden die einzelnen, zu addierenden Werte der XOR-Operation unterzogen. Ein derart mit den Operationen AND und XOR als Multiplikation und Addition versehene Struktur mit den Werten 0 und 1 bildet einen Körper und wird in der Mathematik auch als Galois-Körper GF2 bezeichnet.

[0042] Anstelle des hier verwendeten Galois-Körpers GF2 können auch andere lineare Strukturen, insbesondere andere Galois-Körpers als Elemente der Schlüssel, der Prüfsummen oder der Prüfmatrix verwendet werden. Diese Strukturen weisen, wie auch GF2, die Eigenschaften eines Körpers auf, bieten insbesondere auch die Möglichkeit der Addition und Multiplikation.

[0043] Als Ergebnis dieser Matrix-Vektor-Multiplikation erhält man eine Prüfsumme s_A, die im Folgenden ihrerseits als Zeilenvektor behandelt wird.

[0044] Das erste Endgerät A übermittelt die so übermittelte erste Prüfsumme s_A über den weiteren Kommunikationskanal L an das zweite Endgerät B. Das zweite Endgerät B bildet nun seinerseits, basierend auf dem bei ihm vorliegenden Schlüssel k_B, auf dieselbe Weise wie das erste Endgerät A eine Prüfsumme s_B. Anschließend bildet das zweite Endgerät B die Differenz s_{err} als Differenz zwischen den beiden Prüfsummen s_A und s_B.

[0045] $s_{err} = s_A - s_B = (k_A - k_B) \cdot P = k_{err} \cdot P$

[0046] Anstelle der Bildung der unmittelbaren Differenz zwischen den beiden Prüfsummen kann auch eine andere Funktion verwendet werden, die linear von den Prüfsummen sowie von den beiden Schlüsseln abhängt und einen vorgegebenen Wert, insbesondere einen Nullvektor, liefert, wenn die beiden Schlüssel übereinstimmen.

[0047] Aus der vorstehend dargestellten Formel ergibt sich, dass die Differenz s_{err} der beiden Prüfsummen s_A, s_B, insbesondere aufgrund der Linearität des verwendeten Galois- Körpers hinsichtlich seiner beiden Operationen auch als Produkt der Prüfmatrix P mit einem vektoriellen

Korrekturwert k_{err} dargestellt werden kann. Übermittelt nun das zweite Endgerät B die Differenz s_{err} der beiden Prüfsummen s_A, s_B an einen von den beiden Endgeräten A, B verschiedenen, von diesen räumlich getrennten Server C über den potentiell unsicheren Kommunikationskanal L, so kann dieser lediglich unter Kenntnis der Differenz s_{err} der beiden Prüfsummen s_A, s_B einen Korrektur-Vektor k_{err} berechnen, der, wenn er zu einem der beiden Schlüssel k_A, k_B addiert wird, den jeweils anderen Schlüssel ergibt.

[0048] Alternativ besteht auch die Möglichkeit, dass die beiden Prüfsummen s_A, s_B voneinander unabhängig an den Server C über den zweiten Kommunikationskanal L übertragen werden und dieser Server C die Differenz der Prüfsummen s_A, s_B bildet. Die Bildung der Differenz der beiden Prüfsummen s_A, s_B ist numerisch mit sehr geringem Ressourcenaufwand zu erledigen, sodass es keine Rolle spielt, ob diese Operation von einem der Endgeräte A, B oder vom Server C vorgenommen wird. Die wesentliche Aufgabe des Servers C besteht darin, ausgehend von dem Differenzwert s_{err} der beiden Prüfsummen s_A, s_B einen Korrektur-Vektor k_{err} zu bilden, für den gilt:

[0049] $s_{err} = k_{err} \cdot P$

[0050] Vereinfacht gesprochen wird nach einem Korrektur-Vektor k_{err} gesucht, der, angewendet auf die gemeinsam vereinbarte Prüfmatrix P, eine Prüfsumme ergibt, die der Differenz s_{err} zwischen den beiden Prüf-Vektoren s_A, s_B entspricht. Ein solches, korrektes Verfahren ist beispielsweise in Robert G. Gallager (1963). Low Density Parity Check Codes (PDF). Monograph, M.I.T. Press. Retrieved August 7, 2013 gezeigt. Ein derartiges Verfahren ist gerade, wenn möglichst kurze Prüfsummen verwendet werden, nur mit großem Rechenaufwand zu lösen.

[0051] Nach Durchführung wird der Korrekturwert k_{err} entsprechend der Vereinbarung an eines oder beide der Endgeräte A, B übertragen. Im vorliegenden Fall wird der Schlüssel k_B des zweiten Endgeräts B durch Aufsummieren des Korrekturvektors k_{err} derart angepasst, dass er dem Schlüssel k_A des ersten Endgeräts A entspricht. Alternativ wäre es selbstverständlich auch möglich, den Korrekturwert k_{err} lediglich zum Schlüssel k_A des ersten Endgeräts A zu addieren, um im ersten Endgerät A einen Schlüssel k_A' zu erhalten, dessen Wert den Schlüssel des zweiten Endgeräts B entspricht. Da bei der Erstellung des Signals in der Regel ohnehin zufällige Signale gewählt werden, ist es nicht erforderlich, exakt denjenigen Wert zu rekonstruieren, der über den ersten Kommunikationskanal Q übermittelt wurde.

[0052] Nachdem die Schlüssel k_A, k_B in den Endgeräten A, B zur Übereinstimmung gebracht wurden, wird im Folgenden, optionalen Schritt darauf Rücksicht genommen, dass etwaige Angreifer aufgrund der übermittelten Prüfsumme und der Informationen, die der Angreifer beim Abhören erfahren hat, einzelne Eigenschaften des verwendeten Schlüssels k_A, k_B erfahren konnten. Wird nun die Anzahl der Bits der einzelnen Schlüssel k_A, k_B auf möglicherweise bekannte, jedenfalls zwischen den Endgeräten A, B vorab vereinbarte Weise eine Anzahl von Bits reduziert, die zumindest der Anzahl der Bits der Prüfsumme s_A, s_B entspricht, so gewinnt ein potentieller Angreifer möglichst wenige Informationen über den Schlüssel k_A, k_B aus den übertragenen Prüfsummen s_A, s_B.

[0053] Hinsichtlich der Art der Erstellung des den Schlüssel enthaltenden Signals bestehen mehrere, unterschiedliche Ausführungsvarianten. Dieses Signal kann vorteilhaft ein Quantensignal sein, jedoch auch ein anderes Signal, das über einen fehlerbehafteten und speziell für einen Angreifer nicht ideal kopierbaren ersten Kommunikationskanal Q übertragen wird.

[0054] Es ist möglich, dass bei im Übrigen gleicher Vorgehensweise das zweite Endgerät B über den Kommunikationskanal Q an das erste Endgerät A ein Signal überträgt, das von diesem empfangen wird. Wiederum erhält man in beiden Endgeräten A, B voneinander abweichende Schlüssel k_A, k_B.

[0055] Daneben ist es auch möglich, dass das Signal als Quantensignal über einen den ersten Kommunikationskanal Q, der in diesem Fall als Quantenkommunikationskanal ausgebildet ist, von dritter Stelle an die beiden Endgeräte A, B übermittelt wird. Dabei werden typischerweise miteinander verschränkte Photonen über den ersten Kommunikationskanal Q übermittelt, so-

dass sich in den beiden Endgeräten A, B jeweils miteinander korrespondierende Signale feststellen lassen.

[0056] Ebenso ist es im Rahmen der Erfindung auch möglich, dass beide Endgeräte A, B jeweils separat eine Prüfsumme bilden und diese über den zweiten potentiell unsicheren Kommunikationskanal L an den Server C übertragen. Bei dieser Alternative bestimmt der Server jeweils die Differenz der Prüfsummen selbst.

[0057] In weiterer Folge können zwischen den beiden Endgeräten A, B Nachrichten ausgetauscht werden, die mittels eines symmetrischen Kryptographieverfahrens jeweils unter Verwendung des in den Endgeräten A, B abgespeicherten und zur Übereinstimmung gebrachten Schlüssels k_A, k_B geschützt werden.

[0058] Insbesondere besteht auch die Möglichkeit, die Authentizität der Nachrichten durch die Bildung von schüsselabhängigen Hash-Werten zu verbessern. Dabei werden das zwischen den Endgeräten A, B Nachrichten ausgetauscht werden. Jeder der Nachrichten wird jeweils ein Hash-Wert angehängt, der sich auf vorgegebene Weise aus dem Schlüssel und aus der in der Nachricht zu übertragenden Information ergibt. Anschließend wird die Nachricht über den zweiten Kommunikationskanal L übertragen. Das jeweils empfangende Endgerät A, B überprüft beim Erhalt der Nachricht, ob sich der übermittelte Hash-Wert auf dieselbe vorgegebene Weise aus dem Schlüssel und aus der in der Nachricht zu übertragenden Information ergibt. In diesem Fall wird die Authentizität der Nachricht festgestellt und die Nachricht für echt gehalten.

Patentansprüche

1. Verfahren zur Erstellung und Verteilung von kryptographischen Schlüsseln, insbesondere zum Schutz der Kommunikation auf zwei Endgeräten (A, B),
   a) wobei über einen fehlerbehafteten ersten Kommunikationskanal (Q), insbesondere über einen Quantenkommunikationskanal, Signale zur Erstellung korrelierter Werte in den beiden Endgeräten (A, B) verteilt werden, und diese korrelierten Werte derart als Schlüssel (k_A, k_B) in den beiden Endgeräten vorliegen,
   b) basierend auf dem im ersten Endgerät (A) vorliegenden ersten Schlüssel (k_A) eine Prüfsumme (s_A) gebildet wird und diese Prüfsumme (s_A) über einen vom ersten Kommunikationskanal (Q) verschiedenen zweiten Kommunikationskanal (L) an das zweite Endgerät (B) übertragen wird,
   c) basierend auf dem im zweiten Endgerät (B) vorliegenden zweiten Schlüssel (k_B) eine zweite Prüfsumme (s_B) gebildet wird und die beiden Prüfsummen (s_A, s_B) oder die Differenz (s_{err}) der beiden Prüfsummen (s_A, s_B) oder daraus abgeleitete Informationen über den zweiten Kommunikationskanal (L) an einen von den beiden Endgeräten (A, B) verschiedenen und von diesem räumlich getrennten Server (C) übertragen wird,
   d) dass der Server (C) basierend auf den beiden Prüfsummen (s_A, s_B) oder der Differenz (s_{err}) der beiden Prüfsummen (s_A, s_B) oder den daraus abgeleiteten Informationen einen Korrekturwert (k_{err}) ermittelt, der bei Anwendung auf einen oder beide Schlüssel (k_A, k_B) die Schlüssel (k_A, k_B) zur Übereinstimmung bringt, und
   e) dass der Korrekturwert (k_{err}) an eines oder beide Endgeräte (A, B) über den zweiten Kommunikationskanal (L) übertragen wird und auf einen oder beide Schlüssel (k_A, k_B) angewendet wird.

2. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet**, dass die Signale zur Erstellung korrelierter Werte in den beiden Endgeräten (A, B) verteilt werden, indem
   - vom ersten Endgerät (A) ein zufälliges Signal erstellt wird und, insbesondere mittels Quantenkommunikation, an das zweite Endgerät (B) übertragen wird, oder
   - vom zweiten Endgerät (B) ein zufälliges Signal erstellt wird und, insbesondere mittels Quantenkommunikation, an das erste Endgerät (B) übertragen wird, oder
   - von einer externen Signalquelle ein verschränkter Quantenzustand erzeugt und mittels Quantenkommunikation an beide Endgeräte (A, B) übertragen werden.

3. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet**, dass zu Bildung der korrelierten Werte (k_A, k_B) Teile des übertragenen Signals (S) ausgewählt werden und die übrigen Teile des übertragenen Signals (S) verworfen werden.

4. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet**,
   - dass ein Schlüssel (k_A, k_B) als Binärvektor einer vorgegebenen Länge angegeben wird,
   - dass eine öffentlich bekannte Prüfmatrix (P) umfassend Binärzahlen als Einträge vorgegeben wird, deren Zeilenzahl der Länge der Schlüssel (k_A, k_B) und deren Spaltenzahl der Länge der Prüfsummen (s_A, s_B) entspricht und
   - dass die Prüfsummen (s_A, s_B) durch Bildung einer Matrix-Vektor-Multiplikation gebildet wird, wobei als Addition von Bits die XOR-Operation und als Multiplikation von Bits die AND-Operation verwendet wird.

5. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet**,
   - dass ein Schlüssel (k_A, k_B) als Vektor einer vorgegebenen Länge angegeben wird, dessen Elemente aus einem Galois-Körper stammen,
   - dass eine öffentlich bekannte Prüfmatrix (P) umfassend Elemente aus einem Galois-Körper als Einträge vorgegeben wird, deren Zeilenzahl der Länge der Schlüssel (k_A, k_B) und deren Spaltenzahl der Länge der Prüfsummen (s_A, s_B) entspricht und - dass die Prüfsummen (s_A, s_B) durch Bildung einer Matrix-Vektor-Multiplikation gebildet wird, wobei als Addition und Multiplikation die betreffenden Operationen des Elemente aus einem Galois-Körper verwendet werden.

6. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet**, dass die Länge der Schlüssel (k_A, k_B) auf vorab vorgegebene Weise um eine Anzahl von Bits reduziert wird, die zumindest der Anzahl der Bits der Prüfsumme (s_A, s_B) entspricht.

7. Verfahren nach einem der vorangehenden Ansprüche, wobei zwischen den beiden Endgeräten (A, B) Nachrichten ausgetauscht werden, die mittels eines symmetrischen Kryptographieverfahrens jeweils unter Verwendung des in den Endgeräten (A, B) abgespeicherten Schlüssels (k_A, k_B) geschützt wurden.

8. Verfahren nach einem der vorangehenden Ansprüche, wobei das zwischen den Endgeräten (A, B) Nachrichten ausgetauscht werden, wobei jeder der Nachrichten jeweils ein Hash-Wert angehängt wird, die sich auf vorgegebene Weise aus dem Schlüssel und aus der in der Nachricht zu übertragenden Information ergibt,
wobei das jeweils empfangende Endgerät (A, B) beim Erhalt überprüft, ob sich der übermittelte Hash-Wert auf vorgegebene Weise aus dem Schlüssel und aus der in der Nachricht zu übertragenden Information ergibt und in diesem Fall die Authentizität der Nachricht festgestellt wird.

Hierzu 1 Blatt Zeichnungen

1/1

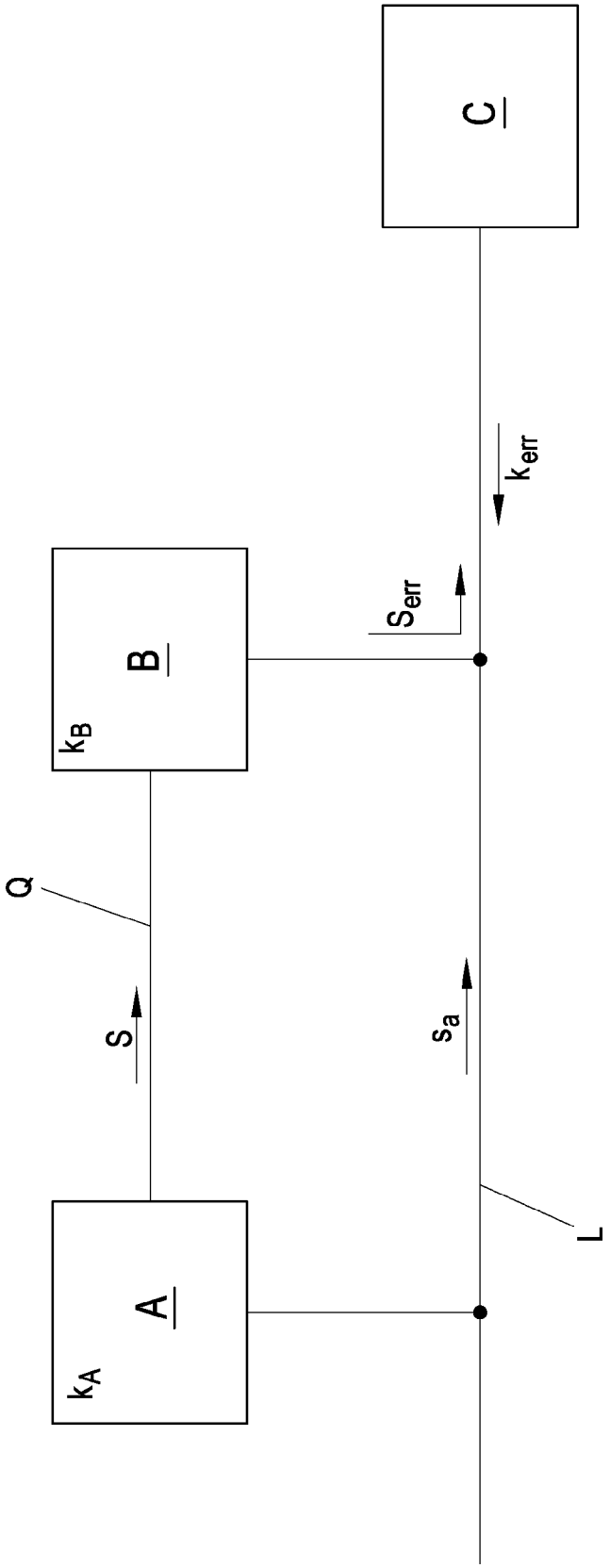

Fig. 1