(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

PCT

(43) Internationales Veröffentlichungsdatum
23. Februar 2006 (23.02.2006)

(10) Internationale Veröffentlichungsnummer
WO 2006/017949 A1

(51) Internationale Patentklassifikation[7]: H04L 9/18

(21) Internationales Aktenzeichen: PCT/CH2005/000427

(22) Internationales Anmeldedatum:
20. Juli 2005 (20.07.2005)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2004 040 654.5 20. August 2004 (20.08.2004) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **GLOBAL SCALING TECHNOLOGIES AG** [CH/CH]; Bahnhofstrasse 105, CH-9240 Uzwil (CH).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **OTTE, Ralf** [DE/DE]; Weimarer Strasse 27, 69469 Weinheim (DE). **MÜLLER, Hartmut** [DE/DE]; Theresienhöhe 6B, 80339 München (DE).

(74) Anwalt: **BÜHLER AG**; Patentabteilung, CH-9240 Uzwil (CH).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Erklärungen gemäß Regel 4.17:

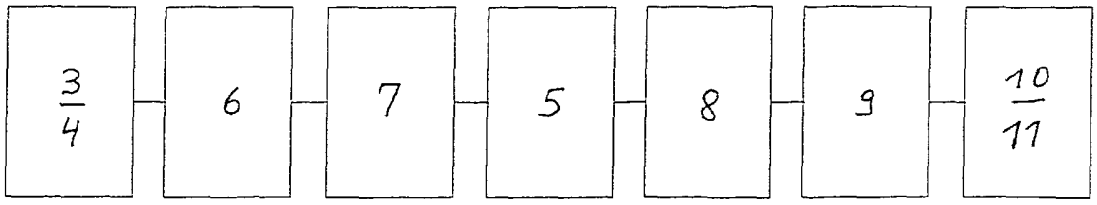
— *hinsichtlich der Identität des Erfinders (Regel 4.17 Ziffer i) für die folgenden Bestimmungsstaaten AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO Patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die folgenden Bestimmungsstaaten AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK,*

[Fortsetzung auf der nächsten Seite]

(54) Title: ENCRYPTION DEVICE AND METHOD USING GLOBAL SCALING FOR KEY DISTRIBUTION

(54) Bezeichnung: EINRICHTUNG UND VERFAHREN ZUR VERSCHLÜSSELUNG UNTER VERWENDUNG VON GLOBAL SCALING ZUR SCHLÜSSELVERTEILUNG



(57) Abstract: The invention relates to a method for encrypting data, which is characterized in that all required information is transmitted via random processes on the basis of a global scaling modulation and demodulation, whereby a modulation, injection, extraction and demodulation of resonant frequencies of coupled noise processes is carried out.

(57) Zusammenfassung: Die Erfindung bezieht sich auf ein Verfahren zur Verschlüsselung von Daten, bei dem alle notwendigen Informationen auf Grundlage einer Global Scaling Modulation und Demodulation über Zufallsprozesse übertragen werden, indem eine Modulation, Einkopplung, Auskopplung und Demodulation von Resonanzfrequenzen gekoppelter Rauschprozesse realisiert wird.

WO 2006/017949 A1

MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO Patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

— *hinsichtlich der Berechtigung des Anmelders, die Priorität einer früheren Anmeldung zu beanspruchen (Regel 4.17 Ziffer iii) für alle Bestimmungsstaaten*

— *Erfindererklärung (Regel 4.17 Ziffer iv) nur für US*

Veröffentlicht:

— *mit internationalem Recherchenbericht*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

EINRICHTUNG UND VERFAHREN ZUR VERSCHLÜSSELUNG UNTER VERWENDUNG VON GLOBAL SCALING ZUR SCHLÜSSELVERTEILUNG

Die Erfindung bezieht sich auf eine Einrichtung und ein Verfahren zur Verschlüsslung von Nachrichten. Die Einrichtung und das Verfahren ist geeignet zur Verschlüsslung digitaler Daten. Die Erfindung ist in sehr vielen Bereichen der Informationsübertragung anwendbar, z. B. in der Telekommunikation, Messtechnik, Sensorik, Medizintechnik, Nachrichtentechnik, Bank- und Versicherungswesen uvm.

Es ist üblich, für die Geheimhaltung von Nachrichten bzw. für die geheime Übertragung von Nachrichten Verschlüsslungsverfahren anzuwenden. Das Ziel der Verschlüsslung ist dabei, eine zu übertragende Nachricht so zu verändern, dass nur der Empfänger, aber kein Dritter diese lesen, d.h. entschlüsseln, kann.

Der Empfänger realisiert diese Entschlüsslung (Dechiffrierung, Decodierung) mit einem sog. Schlüssel, d.h. einer Information, die in der Regel nur er und der Sender besitzt und die notwendig und hinreichend ist, die Nachricht wieder lesbar zu machen.

Hierzu sind zahlreiche Verschlüsslungsverfahren bekannt. Prinzipiell wird bei einer Verschlüsslung aus dem Schlüssel k, dem Klartext m, ein Geheimtext c erzeugt, so dass für die Verschlüsslung gilt:

$$c = f(k, m)$$

Zu dieser Funktion f muss es nun eine umkehrbare Funktion f' geben, so dass für die Entschlüsslung gilt:

$$m = f'(k, c)$$

wobei k in der Regel der gemeinsame, geheime Schlüssel für Sender und Empfänger ist.

Eine wichtige Art der Verschlüsslung wird als symmetrische Verschlüsslung bezeichnet, bei der sowohl Sender als auch Empfänger - aber im günstigsten Falle nur diese - den geheimen Schlüssel k kennen. Für symmetrische Verfahren sind beispielsweise sog. Blockchiffren und Stromchiffren bekannt. Obwohl symmetrische Verschlüsslungsverfahren sehr leistungsfähig sind, sind sie nur anwendbar, wenn sowohl Sender als auch Empfänger den geheimen Schlüssel besitzen, so dass gerade die Übermittlung, d.h. der Austausch der Schlüssel zum Beispiel auf postalischen oder elektronischen Weg einen Angriffspunkt darstellt.

Weiterhin sind sogenannte asymmetrische Verschlüsslungsverfahren bekannt, bei dem jedem Teilnehmer des Systems ein privater (geheimer) Schlüssel d und ein öffentlicher Schlüssel e zugeteilt wird. Der asymmetrische Verschlüsslungsalgorithmus f berechnet für jeden Klartext m unter Verwendung des öffentlichen Schlüssels e einen Geheimtext c nach

$$c = f_e(m)$$

und die Umkehrfunktion f' weist mit Hilfe des privaten Schlüssels d diesem Geheimtext c wieder den Klartext m zu, wobei für die korrekte Entschlüsslung gilt:

$$m' = m = f_d(f_e(m))$$

Sowohl einige symmetrische aber insbesondere asymmetrische Verschlüsslungsverfahren beruhen in der Regel auf mathematischen Algorithmen und sind nicht durch physikalische Effekte oder Eigenschaften geschützt. Ein physikalisch gestützte, geheime Übertragung von Nachrichten wäre beispielsweise die Verwendung von spezieller Tinte u.a., wie es in der Vergangenheit üblich war. Heutige Übertragung von geheimen Nachrichten basiert oftmals auf der Verschlüsslung mittels mathematischer Algorithmen.

Bei asymmetrischen Verschlüsslungsverfahren, den sog. Public-Key-Verfahren, basiert die mathematische Verschlüsslungsidee beispielsweise darin, sogenannte mathematische Einwegfunktion zu verwenden, Funktionen, die schwer umkehrbar sind. Eine der-

artige Einwegfunktion ist beispielsweise die Faktorisierung grosser Zahlen: Während die Multiplikation von zwei sehr grossen Primzahlen p und q trivial ist, so ist ihre Umkehrung, also die Faktorisierung der entstandenen Zahl n zurück in die beiden Primzahlen p und q sehr aufwendig. Die grösste bis zum Jahr 2003 faktorisierte Zahl hatte beispielsweise 155 Ziffern und es wird geschätzt, dass die Zerlegung einer Zahl n von 220 Ziffern mit den besten heute bekannten Verfahren mehrer Tausende Jahre dauern kann [ebenda]. Damit galten diese Public-Key-Verfahren bis in die jüngste Vergangenheit als relativ sicher.

Für alle Verschlüsslungsverfahren sind nun Angriffe bekannt, die das Ziel haben, die verschlüsselte Botschaft c zu entschlüsseln oder den Schlüssel k alleine aus Kenntnis eines Klartexte m und/oder eines Geheimtextes c zurückzurechnen oder den Schlüssel direkt abzufangen, d.h. bei den bekannten Angriffen versucht man durch Abfangen eines Geheimtextes mit dazugehörigen Klartext, den Schlüssel zu berechnen oder den Schlüssel, der bei symmetrischen Verfahren irgendwann ausgetauscht werden muss, abzufangen.

Die Angriffe werden typischer Weise in folgende Arten unterschieden:

- Ciphertext-only attack: Angreifer will aus Kenntnis einiger Gehheimtexte die zugehörigen Klartexte oder den verwendeten Schlüssel k bestimmen
- Known-plaintext attack: Angreifer will aus einigen bekannten Klartexten und dazugehörigen Geheimtexten den Schlüssel k bestimmen
- Chosen-plaintext attack: Angreifer kennt die Verschlüsslungsfunktion f, kann damit bestimmt Klartexte selbst verschlüsseln, kennt aber nicht den Schlüssel k und will k berechnen.
- Chosen-ciphertext attack: Angreifer kennt die Entschlüsslungsfunktion f', kann damit bestimmt Geheimtexte selbst entschlüsseln, kennt aber nicht den Schlüssel k und will k berechnen.

Es ist bekannt, dass alle heute verwendeten asymmetrischen Verschlüsslungs-verfahren theoretisch aufgedeckt werden können, da sie auf mathematischen Eigenschaften beruhen, die durch Dritte zum Entschlüsseln ausgenutzt werden können, auch wenn

die Entschlüsslung wie oben erwähnt mit herkömmlichen Computern oder Computernetzwerken sehr lange, beispielsweise Tausende Jahre, dauern kann.

Insbesondere sind erste Vorschläge gemacht worden, die Entschlüsslung durch den Einsatz von sog. Quantencomputern extrem zu beschleunigen. Die theoretische Idee dahinter ist, dass Quantencomputern Millionen von Rechenoperation gleichzeitig durchführen können, da Quanten, informationstheoretisch sog. Qubits, gleichzeitig mehrere Zustände einnehmen und bei der Verarbeitung von Qubits gleichzeitig mehrere Zustände berechnet werden. Damit lassen sich mathematische Algorithmen und damit auch Faktorisierungen grosser Zahlen oder Entschlüsslungsverfahren um Grössenordnungen schneller umsetzen.

Im Jahre 1994 konnte Shor beweisen, dass mit speziellen mathematischen Verfahren, die auf einem Quantencomputer ablaufen würden beispielsweise der RSA-Algorithmus, einem der bekanntesten asymmetrischen Verschlüsslungsverfahren, nicht mehr sicher ist und dechiffriert werden kann.

Obwohl gegenwärtig noch keine wirklich leistungsfähigen Quantencomputer existieren, auf dem z. B. der Shor-Algorithmus laufen kann und die zum Entschlüsseln von Nachrichten eingesetzt werden, so besteht jedoch ein grosser Bedarf an neuen Verschlüsslungsverfahren, die die Sicherheit der Nachrichtenübertragung, selbst bei dem späteren Einsatz etwaiger Quantencomputer entscheidend erhöhen. Dies ist insbesondere deshalb wichtig, da erste lauffähige Quantencomputer realisiert wurden. Beispielsweise wurde im Jahre 2001 im IBM-Almaden Research Center mit einem 7-bit Quantencomputer die Zahl 15 in ihre Primfaktoren zerlegt.

Die Suche nach neuen asymmetrischen Verschlüsslungsverfahren oder neuen Methoden zum geheimen Schlüsselaustausch bei symmetrischen Verschlüsslungsverfahren ist deshalb eine aktuell wichtige Aufgabe, obwohl schon 1917 durch Mauborgne und Vernam bewiesen werden konnte, dass absolute Sicherheit bei der Nachrichtenübertragung durch folgende drei Bedingungen erreicht wird:

1. Die Länge des Schlüssels k entspricht der Länge des Klartextes m

2. Jeder Schlüssel k besteht aus einer absolut zufälligen Zeichenfolge
3. Jeder Schlüssel k darf nur einmal verwendet werden und muss daraufhin sicher vernichtet werden.

Ein Verfahren was auf diesen Prinzipien beruht heisst One-Time-Pad-Verfahren. Es ist bekannt, dass diese idealen One-Time-Pad-Verfahren perfekte Verfahren sind, deren Sicherheit sogar theoretisch bewiesen werden kann.

Allerdings ist es gegenwärtig in der Praxis nahezu unmöglich für jede Nachrichtenübertragung zwischen Sender und Empfänger einen neuen Zufallsschlüssel zu generieren und zwischen Sender und Empfänger auszutauschen.

In manchen Bereichen wie zum Beispiel Banken werden verkürzte Schlüssel, z.B. TAN-Nummern, verwendet, die nach jeder Übertragung ungültig werden. Der Austausch der neuen Schlüssel, der zwischen Sender und Empfänger auf diese Weise permanent erfolgen muss, könnte unter Umständen aber abgefangen werden, so dass die Sicherheit beeinträchtigt wird.

Da Nachrichten, die beispielsweise mit One-Time-Pad-Verfahren codiert sind, nicht oder jedenfalls nur sehr schwer zu entschlüsseln sind, muss und wird sich ein Angreifer auch insbesondere darauf konzentrieren, in den Besitz des Schlüssels k zu gelangen. Die Generierung und der Austausch der Schlüssel zwischen Sender und Empfänger ist damit der kritischste Punkt der gesamten Nachrichtenübertragung, weshalb neuere Verfahren, wie beispielsweise die Quantenkryptographie, zur abhörsicheren Übertragung von Schlüsseln entwickelt wurden.

Auf dem Gebiet der Quantenkryptographie ist bekannt, dass beispielsweise die Polarisationszustände von Photonen, die durch Glasfaserkabel übertragen werden, geeignet sind, Quantenkryptographieaufgaben durchzuführen. Nachteilig bei diesen bekannten Verfahren ist der hohe technische Aufwand und die prinzipielle Begrenzung der Möglichkeiten der Nachrichtenübertragung, da Sender und Empfänger mit einem Glasfaserkabel verbunden sein müssen, um die polarisierten Photonen auszuwerten.

Zur quantenmechanischen und abhörsicheren Schlüsselübermittlung zwischen einem Sender und einem Empfänger wurden spezielle Protokolle der Quantenkryptographie entwickelt. Bekannt ist das sog. BB84-Protokoll zur Quantenkryptographie.

Die grundlegende Idee der Quantenkryptographie besteht darin, Eigenschaften von Quanten, beispielsweise die Polarisationsrichtung von Photonen, und ihre Überlagerung geschickt auszunutzen. Aus der Quantentheorie ergibt sich, dass beispielsweise Photonen, die vertikal polarisiert wurden mit einer 50prozentigen Wahrscheinlichkeit auch ein um 45 Grad dazu gedrehtes Polarisationsgitter passieren, d.h. dass 50% der Photonen nach dem vertikalen Gitter das nachfolgende, gedrehte Gitter tatsächlich auch passieren. Diese Eigenschaft von Quanten wird in dem bekannten BB84-Protokoll ausgenutzt, vereinfacht wie folgt:

Durch eine zufällige Auswahl eines Polarisationsschemas1 (senkrecht, waagerecht) und eines Schemas2 (45 Grad rechst, links) beim Sender und der Messung der Polarisationsrichtung der passierten Photonen und Zuordnung der Polarisationsrichtung zu den Zahlen Null oder Eins - beispielsweise bei Schema1: vertikal =1, waagerecht = 0; und Schema2: rechts = 1, links = 0 - entsteht beim Sender eine zufällige Zahlenfolge von Nullen und Einsen. Der Empfänger misst nun seinerseits mit zwei Detektoren, die er zufällig abwechselt, für die empfangenen Photonen deren Polarisationsrichtung. Dabei entspricht Detektor1 dem Schema1 und Detektor2 dem Schema2. Dadurch entsteht auch beim Empfänger eine zufällige Folge von Nullen und Einsen, je nachdem welche Polarisationsrichtung gemessen wurde.

Danach verständigen sich Sender und Empfänger über eine normale öffentliche Leitung bei welchem Photon welches Schema angewendet wurde. Alle Photonen und damit Ergebnisse, die bei dem Sender und Empfänger unterschiedliche Schemata verwendet haben, was zwangsläufig passieren muss, da sowohl Sender als auch Empfänger die Auswahl unabhängig voneinander zufällig ausführten, werden verworfen. Übrig bleibt damit eine Zahlenfolge von Nullen und Einsen, die bei Sender und Empfänger identisch sind. Sollte ein Dritter die gesendeten Photonen abhören, so erkennt der Sender und Empfänger das daran, das die verbleibenden Qubits, von denen S und E zufällig einige zum Vergleich auswählen, nicht identisch sind. Man geht beispielsweise davon aus,

dass dann, wenn mehr als 14% fehlerhafter Qubits zwischen Sender und Empfänger (bei gleichen Schemata) vorliegen, ein dritter abgehört hat. Damit kann das Abhören erkannt werden und der Schlüssel muss verworfen werden. Basierend auf diesen und anderen ähnlichen Verfahren sind Einrichtungen und Verfahren zur Quantenkryptographie entwickelt worden.

Neben dem BB84-Protokoll existieren andere Protokoll-Verfahren, bei dem eine externe Quelle sowohl Sender als auch Empfänger mit verschränkten Photonen versorgt.

Bei allen Verfahren bleibt jedoch eine signifikante Reichweitenbeschränkung.

Bekannt ist die quantenkryptographische Übertragung mittels Glasfaserkabel über 67 Kilometer zwischen Genf und Lusanne.

Andere bekannte Verfahren sind der Einsatz von Richtfunkstrecken, also die Übertragung durch Luft, was die Anwendungsmöglichkeiten weiter erhöht.

Das Problem dieser bekannten Verfahren ist, dass man die Qubits nicht verstärken kann, da die Verstärkung den Quantenzustand verändert. Es ist deshalb üblich, die Qubits durch Glasfaserkabel zwischen Sender und Empfänger zu versenden. Dadurch sind allerdings die Entfernungen zwischen Sender und Empfänger begrenzt, gegenwärtig liegt die maximale Entfernung bei ca. 100 km.

Nachteilig bei all den bekannten quantenkryptographischen Verfahren ist somit neben den sehr hohen technischen Aufwand für Glasfaserkabel oder Richtfunkstrecken, die prinzipielle Entfernungsbegrenzung, die daher rührt, dass zwischen Sender und Empfänger Qubits ausgetauscht werden müssen, da diese die Information für den Schlüssel beinhalten. Die bekannten Verfahren sind damit aber nicht geeignet, mit geringen technischen Mitteln über sehr grosse Entfernungen Schlüssel zu übertragen.

Ein weiterer Nachteil der klassischen Quantenkryptographie besteht in der Verifikation der Schemata zwischen Sender und Empfänger, um die zufällige Zeichenfolge festzu-

legen und in der Festlegung der zulässigen Fehlerrate, um zu erkennen, ob Dritte den Schlüssel abgehört haben.

Der Ansatz der abhörsicheren Übertragung von Nachrichten durch den Einsatz von One-Time-Pad-Verfahren basierend auf der quantenkryptographischen Schlüsselübertragung ist damit gegenwärtig noch unzureichend gelöst.

Durch den kommenden Einsatz von Quantencomputern zur extrem schnellen Decodierung von Public-Key-Verfahren gibt es weiterhin einen sehr grossen Bedarf an weiter entwickelten Verschlüsslungsverfahren insbesondere den einfachen, schnellen und abhörsicheren Schlüsselaustausch für symmetrische Verschlüsslungsverfahren.

Die Aufgabe der Erfindung besteht darin, ein Verfahren zur Verschlüsselung zu entwickeln, bei dem ein einfacher, schneller, jederzeit möglicher, permanenter und abhörsicherer Austausch von Schlüsseln zwischen Sender einer Nachricht und Empfänger der Nachricht erfolgt, um beispielsweise durch ein sog. One-Time-Pad-Verfahren eine Übertragung mit maximaler Sicherheit zu gewährleisten. Eine weitere Aufgabe der Erfindung ist damit, dass der Empfänger automatisch erkennen soll, wann der Schlüssel durch Dritte unbefugt empfangen wurde.

Die Aufgabe ist mit den Merkmalen des Anspruchs1 gelöst.

Eine weitere Aufgabe besteht in der Schaffung einer Vorrichtung zur Verschlüsselung von Nachrichten, resp. Daten, insbesondere zur GS-Kryptographie GS – Global Scaling). Diese Aufgabe ist mit den Merkmalen des Anspruchs 13 gelöst.

Basierend auf einer GS-Synchronisation wird zwischen Sender und Empfänger synchron ein geheimer, zufälliger und beliebig langer Einmalschlüssel erzeugt bzw. ausgetauscht, in dem gekoppelte lokale Zufallsprozesse zur Erzeugung eines Schlüssels verwendet werden, der dann geeignet ist, beispielsweise basierend auf einem One-Time-Pad-Verfahren verschlüsselte Nachrichten über herkömmliche Medien auszutauschen.

Vorteilhafte Ausgestaltungen sind in den jeweiligen Unteransprüchen angegeben.

Ein sehr einfaches Beispiel zur Verwendung des Schlüssels k wird am Beispiel eines speziellen symmetrischen Verschlüsslungsverfahrens, der Stromchiffre, beschrieben.

Es ist bekannt, dass bei einer Stromchiffre der Klartext m zeichenweise verschlüsselt wird, indem ein Schlüsselstrom k erzeugt wird, der die gleiche Länge wie der Klartext m hat. Die Verschlüsslung wird so realisiert, dass jeweils ein Klartextzeichen aus m mit einem Schlüsselzeichen aus k verknüpft wird. Beim bekannten One-Time-pad-Verfahren, dem Prototypen des Stromchiffres, liegt sowohl die Nachricht m als auch der Schlüssel k als eine gleichlange Folge von Bits vor.

Für die Realisierung des Verfahrens wird die Nachricht m in einen Folge von Bits umgewandelt und der Schlüssel k ist einen geheime, nur dem Sender und Empfänger bekannte, zufällige Folge von Bits. Die Verschlüsslung f erfolgt beispielsweise derart, dass entsprechende Bits des Klartextes und des Schlüssels miteinander modulo2 bzw. XOR (0+0=0; 1+0=1; 0+1=1;1+1=0) addiert werden.

Die Entschlüsslung erfolgt beispielsweise dadurch, dass der Empfänger die verschlüsselte Nachricht c mit seinem Schlüssel k, der dem des Senders identisch ist, modulo2 (XOR) addiert und somit den Klartext m zurück erhält.

$$m = f'(k,c) = mod_2 (mod_2(k,m))$$

Wird der Schlüssel k jeweils für nur eine einzige Verschlüsslung und Entschlüsslungsnachricht verwendet, so sind alle bekannten Attacken nicht in der Lage eine nachhaltige Entschlüsslung durchzuführen, denn selbst wenn der Schlüssel k durch Abfangen eines Klartextes m und Geheimtextes c berechnet werden kann, so ist er bei der nächsten Nachrichtenübertrag zur Decodierung ungeeignet, da ein völlig neuer Schlüssel k verwendet wird.

Der Austausch des Schlüssels basiert auf Grundlage von Global Scaling.

Global Scaling (GS) ist ein eingeführter physikalischer Begriff, der verdeutlicht, dass Häufigkeitsverteilungen physikalischer Grössen wie z.B. Massen, Temperaturen, Gewichte und Frequenzen realer Systeme logarithmisch skaleninvariant sind. Die Publikationen von Hartmut Müller im Ehlers-Verlag über Global Scaling werden hierbei ausdrücklich zum Offenbarungsgehalt dieser Patentanmeldung gerechnet.

Mit Hilfe des GS lassen sich damit insbesondere diejenigen physikalischen Werte berechnen, die in realen Prozessen, insbesondere Zufallsprozesse bevorzugt eingenommen werden.

Diese bevorzugten Werte können durch eine Kettenbruchzerlegung nach L. Euler ermittelt werden, denn nach Euler ist bekannt, dass jede reelle Zahl x durch ihren Kettenbruch entsprechend Gleichung (1) dargestellt werden kann:

$$x = n_0 + z / (n_1 + z / (n_2 + z / (n_3 + z / (n_4 + z / (n_5 + ..))))) \quad (1)$$

Die Grösse z stellt dabei den sog. Teilzähler dar, dessen Wert nach GS für nachfolgende Frequenzanalysen auf den Wert 2 festgelegt wird.

Da die Skaleninvarianz in logarithmischen Massstäben auftritt, werden im GS-Verfahren alle Analysen von zur Basis e logarithmierten Grössen durchgeführt. Damit entsteht Gleichung (2)

$$\ln x = n_0 + 2 / (n_1 + 2 / (n_2 + 2 / (n_3 + 2 / (n_4 + 2 / (n_5 + ..))))) \quad (2)$$

Die jeweiligen Zahlenwerte hängen von den zugrundeliegenden Masseinheiten ab. In GS werden die auszuwertenden Grössen ins Verhältnis zu physikalischen Konstanten y, den sogenannten Eichmassen, gesetzt. Diese Konstanten sind allerdings nur innerhalb einer vorgegebenen Präzision bekannt, weshalb es obere und untere Grenzwerte für diese Konstanten gibt.

Dadurch entsteht die Gleichung (3) als wichtigste Grundgleichung des GS, die durch eine Phasenverschiebungen um $\varphi = 3/2$ erweitert werden kann, was für die Erläuterungen der Erfindung aber nicht relevant ist:

$$\ln (x/y) = n_0 + 2 / (n_1 + 2 / (n_2 + 2 / (n_3 + 2 / (n_4 + 2 / (n_5 + ..))))) \qquad (3)$$

Die ganzzahligen Teilnenner $[n_0,n_1,n_2...]$ müssen aufgrund der Konvergenzbedingung für Kettenbrüche ihrem absoluten Betrag nach stets grösser als der Zähler sein und sind stets durch 3 teilbare ganze Zahlen.

Durch Anwendung der Gleichung (3) kann eine vorgegebene physikalische Grösse, z.B. eine Frequenz nach der GS-Kettenbruchmethode zerlegt und in einen sog. Kettenbruch-Code umgewandelt werden. Dies soll beispielhaft durch eine GS-Kettenbruchbruchzerlegung für eine Frequenz f_0 beschrieben werden.

In GS wird als physikalische Konstante y zur Berechnung von Frequenzen der Wert 1,4254869e24 Hz verwendet.

Nach Gleichung (3) ergibt sich eine Kettenbruchzerlegung und die Berechnung der Teilnenner n_0, n_1, n_2, n_3, n_4 usw. Die Berechnung der Frequenzwerte durch Kettenbrüche nach Gleichung (3) wurde beispielhaft mit dem Werkzeug GSC3000 professional des Institutes für Raum-Energie-Forschung GmbH, Wolfratshausen, durchgeführt und ist in Fig. 1 exemplarisch für die Frequenz f_0=2032 Hz dargestellt. Die Frequenz 2032 Hz entspricht dem sogenannten GS-Kettenbruchcode [-48; 9086]. Der Teilnenner $n_0 = -48$, der Teilnenner $n_1 = 9086$ bzw. $n_1 = 9036$, je nach Grenzwert der verwendeten Konstante y für die Frequenz.

Da der Teilnenner n_1 in diesem Beispiel (n_1=9086) gross und damit der gesamte Quotient ab n_1 verschwindet gering ist, liegt die Frequenz 2032 Hz in der Nähe des Wertes n_0 ($n_0 = -48$) und wird deshalb auch als sogenannte GS-Knotenpunkt-frequenz bezeichnet. Weitere GS-Knotenpunktfrequenzen nach Gleichung (3) sind beispielsweise 5 Hz, 101 Hz, 40804 Hz, 16461 kHz.

Eine Einrichtung zur Informationsverarbeitung, z.B. von Daten oder Signalen besteht aus einem Sender S und einem Empfänger E zur Analyse und Manipulation eines gekoppelten Zufallsprozesses.

Die Einrichtung und das Verfahren nutzen gekoppelte Zufallsprozesse, insbesondere gekoppelte Rauschprozesse als Informationsträger.

Es gibt eine Vielzahl von Möglichkeiten, das erfindungsgemässe Verfahren, die Einrichtung und die Baugruppen bzw. Einheiten auszugestalten bzw. weiterzubilden. Dazu wird verwiesen sowohl auf die den unabhängigen Patentansprüchen nachgeordneten Ansprüche als auch auf die Beschreibung der in der Zeichnung dargestellten bevorzugten Ausführungsbeispiele.

Nach S. Shnoll treten mehr oder weniger starke Kopplungseffekte von Zufallsprozessen auf, wenn diese zeitgleich und synchron ausgeführt werden, d.h. bei gleichzeitig durchgeführten Messungen an Zufallsprozessen weisen die Häufigkeitsverteilungen der physikalischen Messwerte identische Feinstrukturen auf. Die Muster der (nicht geglätteten) Histogramme der Messwerte mehrerer gleichzeitig durchgeführter Zufallsprozesse stimmen überein oder sind ähnlich. Die Darstellung von nichtgeglätteten Histogrammen bezeichnet man im Global Scaling auch als Feinstruktur des Histogrammes.

Ein hohes Mass der Übereinstimmung der Feinstruktur erkennt man daran, dass die Histogramme der zugrundeliegenden Zufallsprozesse auch in ihren kleineren Ausprägungen sehr ähnlich sind, dass also nicht nur ihre statistischen Kenngrössen wie Mittelwerte, Varianzen usw. übereinstimmen, sondern auch die Häufigkeiten bestimmter Messwerte in den jeweiligen Histogrammen sehr häufig übereinstimmen. Diese Übereinstimmung analysiert man nach GS allerdings nur bei nichtgeglätteten Histogrammen.

Die Ähnlichkeit der Feinstrukturen von Histogrammen oder der Ähnlichkeit des Zeitverlaufes oder der Ähnlichkeit der Änderungsgeschwindigkeit des Zeitverlaufes zweier Zufallsprozesses wird nun als Mass der tatsächlichen Synchronizität von Zufallsprozessen definiert. Im folgenden werden Zufallsprozesse mit einem hohen Mass der Übereinstimmung als gekoppelte Zufallsprozesse bezeichnet.

Die Erfindung wird in zwei Ausführungsbeispielen an Hand einer Zeichnung näher beschrieben. In der Zeichnung zeigen die

Fig. 1: Werkzeug GSC 3000 zur GS-Analyse von Frequenzen
Fig. 2: Schema zur Datenübertragung
Fig. 3: Sende- und Empfangseinheit
Fig. 4: Hintergrundrauschen eines Halbleiterbauelementes
Fig. 5: Harmonische Komponenten des Hintergrundrauschens
Fig. 6: Synchrone harmonische Komponenten des Hintergrundrauschens beim Sender (obere Zelle) und Empfänger (obere Zelle)
Fig. 7: Übertragung einer verschlüsselten Nachricht (Beispiel Zeichen „E").

Hierbei nutzt das

- Ausführungsbeispiel I Phänomene gekoppelter lokaler Zufallsprozesse unter Ausnutzung von Erkenntnissen der GS-Theorie zum Senden und Empfangen eines Schlüssels k von einem Sender S zu einem Empfänger E, die gemäss Stand der Technik mit einem quantenphysikalischen Modell erklärt werden können und das
- Ausführungsbeispiel II gekoppelte lokale Zufallsprozesse beim Sender und Empfänger unter Ausnutzung von Erkenntnissen der GS-Theorie zum synchronen Auslesen einer externen Quelle, beispielsweise des globalen weissen Rauschens mit dem die lokalen Zufallsprozesse in S und E unter geeigneten Bedingungen synchron sind.

Ausführungsbeispiel I

Für die Übertragung eines Schlüssels von einem Sender S (1) zu einem Empfänger E (2) werden in beiden technischen Endgeräten S und E Zufallsprozesse erzeugt, die – wenn sie zeitgleich und synchron ablaufen bzw. abgetastet werden - nach Shnoll und o.g. Definition als gekoppelte Zufallsprozesse bezeichnet werden.

Sender und Empfänger werden bei diesem Verfahren durch technische Endgeräte realisiert, die erstens eine technische Rauschquelle beinhalten oder den Anschluss einer

technischen Rauschquelle zulassen und zweitens die nachfolgenden Verarbeitungsschritte 1-8 in Echtzeit durchführen können. Zwischen Sender und Empfänger liegt eine Übertragungsstrecke 5 für gekoppelte Zufallsprozesse.

Sende- und Empfangseinheit werden in Fig. 3 detaillierter ausgeführt.

Für die Sendereinrichtung 3, 4, 6, 7 und Empfängereinrichtung 8 bis 11 wird jeweils ein handelsüblicher Computer, zum Beispiel ein Laptop verwendet. Das heisst, im weiteren Verlauf wird die Erzeugung 3, 4, GS-Modulation 6, Einkopplung 7, Auskopplung 8 und GS-Demodulation 9 sowie Information 10 des Ausgangssignals 11 von gekoppelten Zufallsprozessen in einer Übertragungsstrecke 5 für gekoppelte Zufallsprozesse basierend auf den Rauschprozessen der soundkarte von zwei handelsüblichen Computern (Sender 1 bzw. Empfänger 2) dargestellt, siehe auch spezifische Offenbarung der DE 102004008444.0 der Anmelderin.

Die Übertragung von Schlüsseln k über gekoppelte Zufallsprozesse wird nun erfindungsgemäss mit nachfolgenden Verfahrensschritten 1 bis 8 gelöst. Die Endgeräte sind dabei handelsübliche Computer. Das Verfahren ist aber auch für andere Endgeräte, andere Abtastfrequenzen f_0 und andere Zufallsprozesse anwendbar.
Das Verfahren ist insbesondere für jeden technisch erzeugten und manipulierbaren Zufallsprozess, z.B. basierend auf externen oder internen Rauschgeneratoren, Halbleiterbauelementen, Prozessoren, Modems usw. anwendbar.

Die Nummer hinter den Teilüberschriften der Verfahrensschritte gibt das betreffende Bezugszeichen gemäss Figur 3 an, bei dem der Verfahrensschritt detailliert ausgeführt wird.

Das Ausführungsbeispiel I lässt sich weiterhin in verschiedenen technischen Varianten realisieren, von dem beispielhaft zwei Verfahren, Beispiel I.a und Beispiel I.b im Detail dargestellt werden:

Ausführungsbeispiel I.a

Im Ausführungsbeispiel I.a werden für Empfänger 1 und Empfänger 2 jeweils ein handelsüblicher Computer, zum Beispiel ein Laptop mit integrierter Soundkarte verwendet. Das heisst, im weiteren Verlauf wird die Erzeugung (3, 4) und Verarbeitung (6), von gekoppelten Zufallsprozessen (5) basierend auf den Rauschprozessen der Soundkarte von zwei handelsüblichen Computern S (1) bzw. E (2) dargestellt.

1. Ankopplung an einen Rauschprozess (3, 4)

Abstimmung eines Senders und Empfängers auf eine gemeinsames Frequenzband (z.B. von 5Hz bis 16,4 MHz) eines technischen Rauschprozesses.

Zur Erzeugung des Rauschprozess kann beispielsweise die Soundkarte eines handelsüblichen Computers oder Laptops verwendet werden. Das Frequenzband des Rauschens liegt dadurch beispielsweise zwischen 100 Hz und 15 kHz. Weitere technische Rauschquellen wären z.B. Halbleiterelemente oder Computerprozessoren. Ein typisches Rauschsignal einer technischen Rausquelle ist in Fig. 4 in ihrem Zeitverlauf dargestellt.

Auf die Rauschsignale der Soundkarte wird mittels Software, beispielsweise mittels Windowsbefehle zugegriffen und die jeweiligen Rauschpegel werden einer nachgeschalteten Auswertesoftware zur Verfügung gestellt.

2. Abtastung des Rauschprozesses zur Erzeugung von Zufallszahlen (3, 4)

Um den Rauschprozess weiterzuverarbeiten, werden durch eine Abtastung des Rauschsignals Zufallszahlen erzeugt. Die Abtastung der Rauschprozesse beim Sender und Empfänger erfolgt erfindungsgemäss mit einer GS-Knotenpunktfrequenz f_0 und führt damit zur Erzeugung einer GS-Zeitfolge von Zufallszahlen Z.

Eine geeignete Knotenpunktfrequenz für die Abtastung von Rauschsignalen der Soundkarte ist beispielsweise f_0 = 2031,55 Hz. Andere Knotenpunktfrequenzen können mittels Gleichung (3) ermittelt werden.

Danach erfolgt die Umwandlung des GS-Abtastsignales in eine normierte, einheitenlose Folge von Zahlenwerten (Z) gegebenenfalls des Wertebereiches N, beispielsweise durch Restklassenbildung R modulo N (Modulo-Operator) gemäss der Formel $Z \equiv Z$ modulo N, wobei N eine Ganze Zahl ist.

Dadurch entsteht beim Sender S die Zufallszahlenfolge Z_S und beim Empfänger E die Zufallszahlenfolge Z_E. Durch die Abtastung ist beispielsweise nachfolgende Folge von Zufallszahlen entstanden und auf den Monitoren des Senders und Empfängers angezeigt:

$$Z_S = \{... 10\ 23\ 2500\ 249\ 28\ 378\ 40456 ...\}$$
$$Z_E = \{... 45\ 789\ 4581\ 45\ 3\ 6782\ 2360 ...\}$$

Die beiden Zufallszahlenfolgen Z_S bzw. Z_E beim Sender bzw. Empfänger sind aber in der Regel ohne technische Vorkehrungen zeitlich nicht synchron.

Um eine Synchronizität und damit Kopplung beider Zufallsprozesse zu erreichen, muss - wie in Shnoll dargestellt - eine exakte zeitliche Synchronizität beider Prozesse im Sender und Empfänger hergestellt werden. Deshalb werden die Rauschprozesse beim Sender und Empfänger zeitlich synchron, d.h. stets zu gleichen Zeitpunkten abgetastet.

Damit entstehen die Zufallszahlen beim Sender und Empfänger zeitlich synchron. Technisch kann die synchrone Abtastung beispielsweise durch die Steuerung über eine externe Funkuhr auf beiden Endgeräten realisiert werden. Die Präzision des synchronen Taktgebers sollte mindestens eine Grössenordnung genauer als die Abtastfrequenz sein.

Dadurch entstehen beim Sender und Empfänger im synchronen Takt der Periode $\triangle t_S = 1/f_0 = t_{i+1} - t_i$ beispielsweise folgende Zufallszahlen, die softwaretechnisch auch auf den Computerbildschirm dargestellt werden können:

$$Z_S = \{...11(t_{i+0})\ 80(t_{i+1})\ 3421(t_{i+2})\ 345(t_{i+3})\ 245(t_{i+4})\ 4512(t_{i+5})\ 5071(t_{i+6})...\}$$
$$Z_E = \{...2345(t_{i+0})\ 479(t_{i+1})\ 23(t_{i+2})\ 346(_{i+3})\ 11(_{i+4})\ 6593(t_{i+5})\ 5031(t_{i+6})...\}$$

Die weitere Beschreibung der Erfindung wird in den folgenden Verfahrensschritten 3-8 dargelegt, wobei diese Schritte erfindungsgemäss innerhalb der Abtastperiode $\triangle t_S$ realisiert werden müssen.

Wurden beispielsweise beim Sender und Empfänger die letzen Zufallszahlen aus dem Rauschen jeweils zum gleichen Zeitpunkt t_{n-1} ermittelt, müssen die Verarbeitungsschritte auf Senderseite durchgeführt werden, noch ehe die Ermittlung der aktuellen Zufallszahl aus dem Rauschen $Z_E(t_n)$ beim Empfänger zum Zeitpunkt t_n erfolgt.
Es gilt daher folgende Gleichung:

$$t_n = t_{n-1} + \triangle t_S$$

Für die o.g. Abtastfrequenz f_0 von 2031,55 Hz ergibt sich im Beispiel die Abtastperiode $\triangle t_S = 1/f_0 = 4{,}92e\text{-}4$ Sekunden, innerhalb derer die Verarbeitungs-schritte durchgeführt werden müssen. Dies ist mit handelsüblichen Computern möglich.

Ausführungsbeispiel I.b

Das Ausführungsbeispiel I.b nutzt die Timerfunktion eines Computers und kann alternativ zur Umsetzung der beschriebenen Schritte 1 und 2 verwendet werden. Das heisst, die Erzeugung und Verarbeitung von gekoppelten Zufallsprozessen kann basierend auf den zeitlichen Fluktuationen der Timerfunktion eines Computers realisiert werden.

Das Basic Input Output System (BIOS) eines Computers realisiert die Schnittstelle zwischen Hardware und Betriebssystem (Windows, Dos). Der BIOS-Datenbereich 0040:0000 – 0040:00FF kann über Befehlszeilen des Betriebssystems direkt ausgelesen werden. Unter der Adresse 006C im Segment 0040 speichert das BIOS den 32-bit-Wert des Zählers der Systemuhr.

Dieser Wert wird im BIOS bei jedem Timer-Aufruf mehrmals pro Sekunde erhöht. Die Geschwindigkeit dieses Akkumulationsprozesses (Akkumulationsrate) unterliegt zeitlichen Schwankungen, die einen physikalischen Rauschprozess generieren. Die Verar-

beitung dieses Rauschprozesses erfolgt erfindungsgemäss in den bereits beschriebenen Schritten 1 und 2.

3. Ableitung der Zufallszahlenfolge (3, 4)

Im weiteren Verlauf wird im Sender und etwas zeitversetzt im Empfänger nach L. Euler eine Ableitung der GS-Zeitfolge von Zufallszahlen Z_S und Z_E der Form f'(x) = lim ((f(x+dx) – f(x)) / dx) mit dx --> 0 realisiert.

Für nichtanalytische Funktionen, wie sie die Zufallszahlenfolgen Z_S und Z_E darstellen, wird nach Euler allerdings dx = 1 gesetzt, dadurch entsteht Gleichung (4).

$$f'(x) = \lim ((f(x+dx) - f(x)) / dx) \text{ mit } dx = 1 \qquad (4)$$

Damit entsteht beim Sender und Empfänger eine neue Zufallsfolge $f_S\{\}$ bzw. $f_E\{\}$ von Änderungsgeschwindigkeiten der Zufallszahlen aus Z_S bzw. Z_E. Diese Änderungsgeschwindigkeiten von Zufallszahlen kann auch als Frequenz f interpretiert werden, wobei die Abtastperiode $\triangle t_S$ zur Erzeugung Z_S bzw. Z_E den zeitlichen Massstab bestimmt.

Fig. 5 stellt ein mögliches Ergebnis $f_S\{\}$ der Ableitung des Signals Z_S aus einem Rauschprozess nach Fig. 4 dar.

Beispielsweise entstand innerhalb eines vorgegebenen Frequenzbandes von $[n_0, n_1-1]$ bis $[n_0, n_1+1]$ durch eine Ableitung nach Gleichung (4) auf der Folge Z_S beim Sender folgende Reihe von Änderungsgeschwindigkeiten bzw. Frequenzen:

$$f_S\{\} = \{... \; 1883{,}93(t_{k+0}) \quad 1885{,}15(t_{k+1}) \quad \mathbf{1889{,}87}(t_{k+2}) \quad 1885{,}51(t_{k+3}) \; ...\}.$$

Für den Empfänger berechnet sich innerhalb des gleichen vorgegebenen Frequenzbandes eine ähnliche Folge von Frequenzwerten $f_E\{\}$.

4. Suche nach GS-Frequenzen (3, 4)

In dieser Folge von Frequenzwerten $f_S\{\}$ bzw. $f_E\{\}$ sucht man beim Sender nach einer Global Scaling Frequenz, die durch einen GS-Kettenbruch-Code der Struktur $[n_0, n_1, n_2]$ dargestellt werden kann.

Dies wird dadurch realisiert, indem man für jede ermittelte Frequenz aus der Folge $f_S\{\}$ beim Sender nach Gleichung (3) eine Kettenbruchanalyse durchführt und die dazugehörigen Teilnenner n_0, n_1, n_2 usw. bestimmt.

Beispielsweise wird innerhalb des vorgegebenen Frequenzbandes von [-48, -26] bis [-48, -28], d.h. von 1881,13 Hz (Kettenbruch-Code: [-48, -26]) bis 1891,50 Hz (Kettenbruch-Code: [-48, -28]) in der Folge $f_S\{\}$ die Frequenz f_R= 1889,87 Hz ermittelt, für die ein Kettenbruch-Code der Struktur $[n_0, n_1, n_2]$ existiert.

Der Kettenbruch-Code für f_R = 1889,87 Hz ist gleich [-48, -27, -3].

Der Teilnenner n_2 ist in diesem Beispiel –3.

Nach GS wird dabei beim Sender und Empfänger innerhalb des Frequenzbandes die gleiche Frequenz f_R gefunden, d.h. beide ursprüngliche Zufallszahlenfolgen Z_S und Z_E haben in dem vorgegebenen Frequenzband genau eine gemeinsame GS-Änderungsgeschwindigkeit ihrer Zufallszahlen.

Diese wird im folgenden als Resonanzfrequenz f_R beider Zufallszahlenfolgen Z_S und Z_E bezeichnet.

5. GS Modulation auf Senderseite (6)
Beim Sender erfolgt die GS Modulation beispielsweise durch eine Veränderung des Teilnenners n_2, beispielsweise durch eine Vorzeichenumkehr von n_2. Dadurch ergibt sich auf Senderseite folgender neuer Kettenbruchcode $[n_0, n_1, -n_2]$ und durch Umkehrung von Gleichung (3) eine neue Frequenz f_R'.

Im Beispiel wird der zu f_R= 1889,87 Hz gehörende GS-Kettenbruch [-48, -27, -3] zu [-48, -27, +3] verändert, d.h. der Teilnenner n_2=-3 wird durch Vorzeichenumkehr auf

n'_2=+3 gesetzt. Daraus ergibt sich nach umgekehrter Anwendung von Gleichung (3) die neue Frequenz f_R' = 1882,97 Hz.

Auch diese Frequenz f_R' stellt mathematisch eine Änderungsgeschwindigkeit der Zufallszahlen dar und durch die Umkehrung der Ableitung nach L. Euler aus Gleichung (4) wird darauf basierend im Sender die neue Zufallszahl $Z'_S(t_n)$ berechnet, die im folgenden beim Sender zum Zeitpunkt t_n in den Rauschprozess eingekoppelt wird.

Da alle Verfahrensschritte innerhalb der Abtastperiode $\triangle t_S$ durchgeführt wurden, ist auf Senderseite die manipulierte Zufallszahl $Z'_S(t_n)$ berechnet wurden, noch ehe beim Sender oder Empfänger über den Rauschprozess eine neue Zufallszahl generiert wurde.

Die Umkehrung von Gleichung (4) ist deshalb möglich, da die Ableitung von Gleichung (4) ein eindeutiges deterministisches Verfahren darstellt. Aus dem gleichen Grunde ist auch Gleichung (3) umkehrbar.

Im Beispiel ist die neue Zufallszahl $Z'_S(t_n)$ = 192 entstanden und es ergibt sich zum Zeitpunkt t_n folgende Reihe von Zufallszahlen:

$$Z_S = \{...11(t_{i+0})\ 80(t_{i+1})\ 3421(t_{i+2})\ 345(t_{i+3})\ 245(t_{i+4})\ 4512(t_{i+5})\ 50712(t_{i+6})...\ 192(t_n)\}$$

6. Einkopplung bzw. physikalische Erzeugung des neu berechneten Rauschwertes (7)
Die neu berechnete Zufallszahl $Z'_S(t_n)$ wird in einen dimensionsbehafteten Rauschpegelwert umgerechnet und innerhalb der Abtastperiode in den Zufallsprozess eingekoppelt. Diese Umrechung ist möglich, da das Verfahren der Umrechung des Rauschpegelwertes in Zufallszahlen aus den vorhergehenden Verfahrensschritten bekannt und umkehrbar ist.

Im Beispiel der Erzeugung der Zufallszahlen mittels des Rauschens einer Soundkarte wird somit die neue Zufallszahl ($Z'_S(t_n)$ = 192) auf Senderseite in einen Rauschwert umgewandelt und über die Soundkarte physikalisch ausgegeben.

Durch diese Einkopplung des zu $Z'_S(t_n)$ gehörenden Rauschpegelwertes wurde das Rauschen auf Senderseite moduliert.

7. Auskopplung bzw. Demodulation auf Empfängerseite (8, 9)
Da die Zufallsprozesse des Senders und Empfängers durch die GS-Knotenpunktfrequenz synchronisiert wurden und durch zeitliche Synchronizität miteinander gekoppelt sind und ganz bestimmte, gleiche Resonanzfrequenzen bzw. Änderungsgeschwindigkeiten aufweisen, hat sich kurzzeitig auch der Rauschprozess auf Empfängerseite verändert.

Insbesondere sind sie physikalisch durch verschränkte Quantenzustände miteinander gekoppelt, da die Resonanzfrequenzen beider Zufallsprozesse einem Quant der Frequenz f_R entsprechen.

Das Rauschsignal im Empfänger wird zum Zeitpunkt t_n durch Abtastung mit f_0 ausgekoppelt und nach dem gleichen Verfahren wie auf Senderseite in Zufallszahlen umgewandelt.

Es erscheint auf Empfängerseite zum Abtastzeitpunkt t_n mit hoher Wahrscheinlichkeit die im Sender eingespeiste Zufallszahl (im Beispiel $Z'_E(t_n) = 192$), auf jeden Fall aber eine Zufallszahl $Z'_E(t_n)$, die bei der späteren Ableitung der Folge Z_E nach L. Euler (Gleichung (4)) beim Empfänger die definierte Resonanzfrequenz f_R' verursacht.

Im weiteren wird beschrieben, wie diese senderseitig manipulierte Resonanzfrequenz f_R' auf Empfängerseite gefunden und decodiert wird.

Erfindungsgemäss analysiert der Empfänger für das mit dem Sender vorher abgestimmte Frequenzband von $[n_0, n_1\text{-}1]$ bis $[n_0, n_1+1]$ und basierend auf der neuen ermittelten Zufallszahl $Z'_E(t_n)$ alle vorhandenen Frequenzen innerhalb des Frequenzbandes durch eine GS Analyse und bestimmt die eindeutige Frequenz f'_R, für die der Kettenbruch-Code $[n_0, n_1, -n_2]$ existiert.

Für diese Frequenz f'_R wird der Teilnenner n_2 bestimmt.

Beispielsweise wird basierend auf der zuletzt empfangenen Zufallszahl innerhalb des mit dem Sender vereinbarten Frequenzbandes von 1881,13 Hz (Kettenbruch-Code: [-48, -26]) bis 1891,50 Hz (Kettenbruch-Code: [-48, -28]) der Folge $f_E\{\}$ die gemeinsame Frequenz f'_R= 1882,969 Hz gefunden, für die ein Kettenbruch-Code der Struktur [n_0, n_1, n_2] existiert. Der Kettenbruch-Code für f'_R = 1882,969 Hz ist gleich [-48, -26, +3]. Der Teilnenner n_2 ist damit +3.

8. Decodierung der übertragenen Information (10)
Durch Vergleich des ermittelten Kettenbruch-Codes mit dem nach GS bestimmten Code kann der Empfänger nun erkennen, ob der n_2-Wert auf Senderseite manipuliert wurde.

Beispielsweise kann nach GS das erwartete Vorzeichen von n_2 alleine aus der Kombination von Abtastperiode $\triangle t_S$, n_0 und n_1 rechnerisch bestimmt werden, denn durch n_0 und n_1 wird eindeutig das Frequenzband festgelegt, indem die erwartete Global Scaling Resonanzfrequenz f_R des Zufallsprozesses vorhanden sein muss.

Im Beispiel von $\triangle t_S$ =4,92e-4 Sekunden, n_0 = -48 und n_1= -27 wird auf Empfängerseite eine Frequenz f_R mit dem zugehörigen Kettenbruchcode [-48, -27, -n_2] erwartet, was für den nichtmodulierten Fall im Sender auf Empfängerseite auch zutrifft.

Im Beispiel der dargestellten Modulation ergab im Empfänger die Analyse aller Frequenzen innerhalb des mit dem Sender vereinbarten Frequenzbandes aber nur die Frequenz f'_R = 1882,969 Hz, für die ein Kettenbruch-Code der Struktur [n0, n1, n_2] existiert. Und der Kettenbruch-Code für f'_R = 1882,969 Hz lautet [-48, -26, +3].
Der Teilnenner n_2 ist damit +3.

Da auf Empfängerseite aber ein n_2-Wert von –3 erwartet wurde, hat der Empfänger erkannt, dass auf Senderseite der n_2-Wert der Resonanzfrequenz f_R moduliert wurde. Damit erkennt der Empfänger die Manipulation auf Senderseite, wenn diese vorhanden ist.

Erfindungsgemäss wird die Manipulation aus Senderseite mit dem Bitwert 1 und die Nichtmanipulation mit dem Bitwert 0 codiert.

Damit ist zwischen Sender und Empfänger über den zugrundeliegenden, gekoppelten Rauschprozess durch GS Modulation und GS Demodulation einer gemeinsamen Resonanzfrequenz f_R ein Bit an Information übertragen worden.

Durch die Möglichkeit der Übertragung eines Bits des Schlüssels k sind somit beliebig lange Schlüssel vom Sender S zum Empfänger E übertragbar.

Die technische Übertragungsrate über den hier dargestellten Zufallsprozess ist durch die Abarbeitungsgeschwindigkeit der Verfahrensschritte 1-8 und durch die Abtastfrequenz f_0 determiniert und begrenzt. Eine Erhöhung der Übertragungsrate ist beispielsweise durch die Verwendung anderer Abtastfrequenzen f_0, schnellerer Computer, einer verbesserten GS Modulation des Kettenbruchwertes n_2 (bzw. höherer Elemente des Kettenbruches n_3, n_4 usw.) oder der parallelen Nutzung mehrerer Übertragungskanäle möglich.

Ausführungsbeispiel II

Die Ankopplung von Sender S und Empfänger E an einen lokalen Zufallsprozess, beispielsweise einen thermischen Rauschprozess eines Halbleiterbauelementes erfolgt gemäss Ausführungsbeispiel I, Verfahrensschritte 1-3.

Damit entsteht beim Sender und Empfänger erneut eine neue Zufallsfolge $f_S\{\}$ bzw. $f_E\{\}$ von Zufallszahlen bzw. Änderungsgeschwindigkeiten der Zufallszahlen aus Z_S bzw. Z_E. Diese Änderungsgeschwindigkeiten von Zufallszahlen kann auch als Frequenz f interpretiert werden, wobei die Abtastperiode $\triangle t_S$ zur Erzeugung Z_S bzw. Z_E den zeitlichen Massstab bestimmt.

Fig. 5 stellt wiederum ein mögliches Ergebnis $f_S\{\}$ der Ableitung des Signals Z_S aus einem Rauschprozess nach Fig. 4 dar. Für den Empfänger berechnet sich innerhalb des

gleichen vorgegebenen Frequenzbandes eine ähnliche Folge von Frequenzwerten $f_E\{\}$, basierend auf einem lokalen Zufallsprozess.

Beispielsweise entsteht dadurch beim Sender und Empfänger folgender nahezu synchroner Zufallsprozess, der einer synchronen Änderungsgeschwindigkeit ihrer unterlagerten Rauschprozesse entspricht und als Folge von Zahlen verstanden werden kann. In der Ordinate stehen dafür die Frequenzwerte, die als Zahlen abstrahiert werden können (Fig. 6).

Durch Festlegung geeigneter Schwellwerte lassen sich aus den synchronen harmonischen Komponenten identische Zahlenfolgen f'_S und f'_E berechnen, die als dekadische Zahlen oder als Bitmuster ausgegeben werden können, siehe Fig. 6:

Damit werden auch in diesem Ausführungsbeispiel sowohl im Sender S als auch im Empfänger E beliebig lange, identische Zahlenfolgen generiert, die im weiteren als Schlüssel k verwendet werden.

Durch das erfindungsgemässe Verfahren, welches in zwei Ausführungsbeispielen beschrieben wurde, kann zwischen einem Sender S und einem Empfänger E ein Schlüssel ausgetauscht werden, der nur dem Sender und Empfänger bekannt ist und deshalb zur symmetrischen Verschlüsslung verwendet werden kann.

Im Empfänger wird der Schlüssel k zum Verschlüsseln der Nachricht m gemäss
$c = f(k,m)$ und im Sender zum Entschlüsseln gemäss
$m = f'(k,c)$ verwendet. Damit können Nachrichten m zwischen Sender und Empfänger über herkömmlich Medien ausgetauscht werden und sind dennoch nicht dechiffrierbar. Sie sind insbesondere dann nicht dechiffrierbar, wenn der Schlüssel k_1 nur für eine einzige Übertragung verwendet wird und danach ein erneuter Schlüssel k_2 verwendet wird.

Da der Schlüsselaustausch von k in den Ausführungsbeispielen als physikalisches Modell der Verschränkung von Quantenzuständen beispielsweise von Photonen verstanden werden kann, da sie dieselben physikalischen Effekte aufweisen, erkennt der Emp-

fänger den Fall, dass der Sender nicht mit dem gewünschten Empfänger E sondern einem Dritten E' synchron geht und mit diesem den Schlüssel austauscht.

Im Ausführungsbeispiel I entsteht die Synchronizität durch gezielte Manipulation des gewählten Kettenbruchkodes $[n_0, n_1, n_2,...]$, was mathematisch einer Manipulation von verschränkten Quantenzuständen entspricht und deshalb nicht unbemerkt abgehört werden kann.

Im Ausführungsbeispiel II entsteht die Synchronizität durch hohe Präzision beim auslesen der lokalen Zufallsprozesse. Nur wenn die Zeitpunkte des Auslesens beim Sender undbeim Empfänger exakt zum gleichen Zeitpunkt erfolgen, wobei der Begriff „exakt" je nach Anwendung und Bandbreite zu wählen ist, entsteht eine Synchronisierung infolge der Verfahrensschritte ab Schritt 3.

Das exakte Auslesen stellt also einen quantenphysikalischen Messprozess dar. Werden beispielsweise 3 oder mehr Einrichtungen verwendet, die exakt den gleichen Zeitpunkt der Rauschprozesse abtasten, so gibt es genau zwei, die die Synchronizität erreichen. Diese Prozesse bleiben dann zur Erzeugung des Schlüssels synchron, bis der Abbruch durch den Nutzer erzwungen wird.

Der dritte oder weitere Messprozess kann nicht auch zu den beiden synchron werden. Sollte also in beabsichtigter Weise ein unbefugter Dritter mit dem Sender synchron gehen, da er den exakten Zeitpunkt des Abtastens kennt, erhält der Empfänger eine nichtsynchrone Zahlenfolge, die nicht als Schlüssel verwendet werden kann. Durch Anwendung des nachfolgend beschriebenen Protokolls GSKT04 werden Sender und Empfänger erkannt und der Synchronisierungsprozess müsste erneut gestartet werden.

Damit kann er den Sender umgehend darüber informieren und einen neuen Schlüsselaustausch beginnen.

Haben S und E einen gemeinsamen, geheimen und hinreichend langen Schlüssel k ausgetauscht, sind zahlreiche Verschlüsslungsalgorithmen realisierbar, wobei die ein-

fachste Variante die modulo2 bzw. XOR-Operation zwischen Schlüssel k und Klartext m ist.

Zu einem vereinbarten Zeitpunkt t_0 wird beim Sender und Empfänger der Schlüssel k = {11001011} generiert mit dem die Nachricht, im Beispiel der Buchstabe „E", m = {E} = {10100101} verschlüsselt wird. Durch f = XOR (k,m) entsteht die Geheimnachricht c = { 01101110} und wird beim Empfänger mit der Funktion f' = XOR (k,c) decodiert. Dadurch entsteht wieder die Originalnachricht m'={E}, siehe Fig. 7. Bezugszeichen 30 ist hierbei der Schlüssel zur Chiffrierung und 40 der zur Dechiffrierung. Zu übertragen ist der Klartext 31 des Buchstaben „E" in ASCII. Der verschlüsselte Text 32 wird dechiffriert und ist wieder als Klartext 41 des Buchstaben in ASCII lesbar.

Weitere Möglichkeiten der Verschlüsslung mit dem Schlüssel k sind, diesen Schlüssel nicht XOR zur Nachricht m zu verwenden, sondern den Schlüssel für eine Funktion f beispielsweise zur Bytesubstitution oder zyklischen Verschiebung von Bits oder Bytes der Nachricht oder beliebig anderen Transformationen zu verwenden, die beim Empfänger umkehrbar sind.

Da der synchrone Schlüssel k für Sender und Empfänger nur dann entsteht, wenn beide Einrichtungen zum gleichen Zeitpunkt und synchron die Zufallsprozesse verarbeiten, muss der Zeitpunkt und die Abtastfrequenz für beide Einrichtungen bekannt sein. Die erste Vereinbarung über den Zeitpunkt könnte aber gegebenenfalls abgehört werden, so dass ein Dritter zu exakt diesem Zeitpunkt versuchen kann, den Schlüssel abzufangen bzw. mit auszulesen.

Erfindungsgemäss tauschen Sender und Empfänger deshalb zu Beginn der Schlüsselübertragung basierend auf vereinbarten i Bits des Schlüssels k eine beiden bekannte Nachricht $m_{KENNUNG}$ aus, die durch Verschlüsslung mit k beim Sender und Empfänger identisch sein muss, wenn k identisch ist.

Ist bzw. war der Empfänger bei der Schlüsselübertragung nicht synchron mit dem Sender, besitzt er eine andere Zufallszahlenfolge k', die er als Schlüssel k' interpretiert. Durch Entschlüsslung der vom Sender übermittelten geheimen Nachricht $c_{KENNUNG}$ ent-

steht dann aber nicht der vereinbarte Klartext $m_{KENNUNG}$, d.h. $m_{KENNUNG)} <> f(k', c_{KENNUNG})$, so dass der Empfänger den Sender den Abbruch der Synchronisierung über herkömmliche Nachrichtenwege mitteilt. Danach versuchen Sender und Empfänger erneut, synchron einen Schlüssel zu generieren, bis beim Empfänger der vereinbarte Klartext $m_{KENNUNG}$ empfangen wird. Damit ist der Schlüssel k zwischen Sender und Empfänger synchron und kann durch Dritte nicht mehr abgefangen werden.

Die Generierung des Schlüssels k kann dabei unmittelbar vor bzw. während der Nachrichtenübertragung oder zu einem beliebig anderen, beiden Seiten bekannten Zeitpunkt erfolgen.

Am Ende der mit k verschlüsselten Nachrichtenübertragung wird der nächste exakte Zeitpunkt der synchronen Schlüsselgenerierung übertragen, so dass i.a. nur Sender und Empfänger die exakten Koordinaten der nächsten Schlüsselgenerierung kennen und die Wahrscheinlichkeit einer Fremdsynchronization verringert werden kann. Ansonsten muss gemäss des o.g. Verfahrensschrittes der Schlüsselaustausch solange wiederholt werden, bis Sender und Empfänger den bekannten und vereinbarten Klartext $m_{KENNUNG}$ austauschen und damit der Schlüssel k beider identisch ist.

Wenn ein Dritter den Schlüssel k empfängt, dass dieser glaubt er habe den Synchronschlüssel des Senders erhalten, denn das empfangen stellt nach dem quantenphysikalischen Modell einen Messvorgang dar, der nicht mehr umkehrbar ist. Damit ist o.g. Verfahren geeignet auch den ersten und damit kritischen Beginn einer Schlüsselgenerierung zu realisieren, auch wenn Unbefugte den genauen Zeitpunkt der Synchronisierung erfahren haben, welcher mit exakt derselben Frequenz $[n_0, n_1, n_2, ...]$ zu exakt denselben Zeitpunkten erfolgen müsste, was unwahrscheinlich ist. Falls solch ein Unbefugter den Schlüssel empfängt, merkt es der Empfänger nach dem o. g. Verfahren der Kennungsübertragung und der Schlüsselaustausch beginnt von vorn. Die nächsten exakten Zeitpunkte der Schlüsselgenerierung werden dechiffriert übertragen, sodass ein Abhören nicht mehr möglich ist.

Um die Sicherheit des Schlüsselaustausches zu verbessern wird ein Protokoll GSKT04 definiert, bei dem der Sender nach einer verabredeten Zykluszeit weiterhin und zyklisch

einen definierten Klartext $m_{KENNUNG1}$, zum Beispiel den Namen des Senders sendet, der beim Empfänger nach dem Entschlüsseln mit seinem Schlüssel als Klartext auch entstehen muss und dem Empfänger die Sicherheit gibt, mit dem richtigen Schlüssel k zu entschlüsseln. Da es immer nur ein einziges Paar von Sender und Empfänger geben kann, die durch die GS Synchronisation den selben Schlüssel k erhalten, ist damit sicher gestellt, dass bei richtiger Erkennung des Klartextes $m_{KENNUNG1} = f'(k,c)$ innerhalb einer kurzen Zykluszeit Sender und Empfänger weiterhin den selben Schlüssel benutzen und deshalb aus physikalischer Sicht kein Dritter diesen Schlüssel besitzen und die Nachricht entschlüsseln kann.

Eine weitere Möglichkeit besteht in dem direkten Vergleich ausgewählter j Bits zwischen Sender und Empfänger. Übersteigt die Fehlerrate einen vorher definierten Wert, wird der gesamte Schlüssel verworfen.

Damit ist eine nach gegenwärtig bekannten Verfahren - physikalisch begründete -, vollkommen draht- und kabellose, nicht entschlüsselbare Nachrichtenübertragung gewährleistet.

Die Generierung von geheimen, einmaligen Schlüsseln zwischen Sender und Empfänger wird durch Effekte basierend auf der GS Kommunikation realisiert und die Nachrichtenübertragung der Nutzinformation erfolgt dann über herkömmliche Wege, aber verschlüsselt mit dem geheimen Schlüssel k, der, da i.a. nur einmal verwendet wird, das Entschlüsseln unmöglich bzw. nahezu unmöglich macht.

Der geringe Aufwand der Schlüsselübertragung und damit der Verschlüsslung beispielsweise wie im Ausführungsbeispiel von nur zwei handelsüblichen Laptops beschrieben, lässt eine effiziente Verschlüsslung von Nachrichten und damit ein weites Anwendungsspektrum beispielsweise in der Industrie und im Bankenwesen zu.

Um den Nachteil der langen Schlüssel zu vermeiden, da beim One-Time-Pad, der Schlüssel genauso lang sein muss wie die Nachricht, lässt sich das Verfahren beispielsweise auch für Blockchiffren ausbauen und verwenden.

Das Verfahren hat damit alle Vorteile der modernsten bekannten quantenkryptographischen Verfahren und gegenüber diesen zusätzlich den Vorteil, dass es ohne jeglicher Verkablung zwischen Sender und Empfänger, also ohne Glasfaserverbindung, auskommt, da der Schlüsselaustausch über gekoppelte Zufallsprozesse, beispielsweise die Kopplung von lokalen thermischen Rauschprozessen mit dem globalen Hintergrundrauschen erfolgt.

Da auch die Übertragung über das Hintergrundrauschen mittels gekoppelter Zufallsprozesse durch quantenphysikalische Modelle, insbesondere der Verschränkung von Quanten erklärt werden kann und diese Effekte nutzt bzw. dieselben phänomänologischen Effekte aufweist, kann jedes Mithören durch Dritte erkannt werden, da sich dadurch der Schlüssel verändert und dies über das Protokoll GSKT04 jederzeit feststellbar ist.

Patentansprüche

1. Verfahren zur Verschlüsslung von Daten bei dem der geheime Schlüssel durch Global Scaling Kryptographie basierend auf Resonanzfrequenzen gekoppelter Zufallsprozesse übertragen werden und diese Schlüssel zur Verschlüsslung von Nachrichten verwendet werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Modulation, Datenübertragung und Demodulation auf Basis von technischen Rauschprozessen erfolgt.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass für die Modulation, Übertragung und Demodulation stationäre oder mobile digitale Sende- und Empfangsgeräte verwendet werden.

4. Verfahren nach Anspruch 1 bis 3, dadurch gekennzeichnet, dass für die Modulation, Übertragung und Demodulation stationäre oder mobile, handelsübliche Computer mit integrierter oder externer Rauschquelle verwendet werden.

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Übertragung über stationäre oder mobile analoge und daraus ableitbare Sende- und Empfangsgeräte erfolgt.

6. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass die Übertragung für medizinische Zwecke genutzt wird.

7. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass die Übertragung für die Übermittlung von Passwörtern, PIN-Codes oder anderer sicherheitsrelevanter Anwendungen genutzt wird.

8. Verfahren zur Verschlüsselung von Daten oder Signalen nach Anspruch 1, unter Verwendung einer Sendeeinheit mit einem Modulator zur Modulation der Information und mit einem Einkoppler zum Einkoppeln der Information in einen Zufallsprozess, einer Empfangseinheit mit einem Demodulator zur Demodulation der Information und einem Auskoppler zum Auskoppeln der Information aus dem Zufallsprozess, dadurch gekennzeichnet, dass die Datenübertragung über gekoppelte Zufallsprozesse erfolgt.

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass als Modulator und Demodulator ein Global-Scaling-Modulator bzw. ein Global-Scaling-Demodulator verwendet wird.

10. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass als Signal oder Signalerzeugungselement für den Ein- und Auskoppler und/oder den Modulator/Demodulator ein Rausch- oder Zufallssignal eines Rausch- oder Zufallsignalerzeugungselementes oder –prozesses verwendet wird, vorzugsweise technische Rausch- oder Zufallssignale oder -prozesse wie thermisches oder weisses Rauschen oder Rausch- oder Zufallssignalelemente wie eine Rauschdiode.

11. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass mindestens ein Element des Kettenbruchcodes $[n_0, n_1, n_2, n_3,..]$ der Resonanzfrequenz f_R moduliert wird, beispielsweise durch Vorzeichenumkehr.

12. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass es folgende Verfahrensschritte umfasst:

- Erzeugung eines Rauschsignals in der Sende- und Empfangseinheit (S, E), vorzugsweise eines elektrischen Rauschsignales
- Abtastung des Rauschsignals mit einer GS-Knotenpunktfrequenz f_0, vorzugsweise einer n0-Frequenz zur Erzeugung eines Abtastsignals
- Umwandlung des GS-Abtastsignales in ein normiertes, einheitenloses Abtastsignal in Form von Zahlenwerten (Z), vorzugsweise durch Restklassen-

bildung R modulo N (Modulo-Operator) gemäss der Formel Z ≡Z mod G, wobei G eine Ganze Zahl ist und den gemessenen Rauschpegel darstellen kann.

- Ableitung der Zahlenfolgen Z_S und Z_E nach L. Euler zur Erstellung einer Folge von Frequenzen f_S und f_E.
- Ermittlung der Resonanzfrequenz f_R innerhalb eines vorgegeben Frequenzbandes
- Modulation der Resonanzfrequenz f_R beispielsweise durch Vorzeichenumkehr des Elementes n_2 aus dem Kettenbruchcode $[n_0, n_1, n_2]$
- Demodulation und Decodierung der sendeseitig vorgenommenen Veränderungen in der Empfängereinheit.

13. Einrichtung zur Verschlüsselung von Daten oder Signalen, bestehend aus einer Sendeeinheit mit einem Modulator zur Modulation der Information und mit einem Einkoppler zum Einkoppeln der Information in eine Trägerwelle, einer Empfängereinheit mit einem Demodulator zur Demodulation der Information und einem Auskoppler zum Auskoppeln der Information aus den Zufallsprozessen, insbesondere für ein Verfahren nach einem der Ansprüche 1-12 dadurch gekennzeichnet, dass die Übertragung über gekoppelte Zufallsprozesse erfolgt.

14. Einrichtung nach Anspruch 13 dadurch gekennzeichnet, dass der Modulator und Demodulator ein GS-Modulator bzw. ein GS-Demodulator ist.

15. Einrichtung nach Anspruch 13 dadurch gekennzeichnet, dass die Sendeeinheit und/oder die Empfangseinheit eine Rausch- oder Zufallssignalerzeugungseinheit aufweist, vorzugsweise ein elektrisches oder elektronisches Rauschsignalerzeugungselement, z.B. eine Rauschdiode.

16. Einrichtung nach Anspruch 13 dadurch gekennzeichnet, dass die Rausch- oder Zufallssignalerzeugungseinheit oder deren Signale Bestandteil des Modulators und/oder des Einkopplers sind.

17. Einrichtung nach Anspruch 13 dadurch gekennzeichnet, dass sie eine GS-Abtasteinheit aufweist, so dass das Rauschsignal mit einer GS-Frequenz abtastbar ist, um einen GS-getakteten Zufallsprozesse zu erhalten.

18. Einrichtung nach Anspruch 17 dadurch gekennzeichnet, dass die Abtastfrequenz eine GS-Knotenpunkt-Frequenz ist, vorzugsweise eine reine n0-Frequenz.

19. Einrichtung nach Anspruch 13 dadurch gekennzeichnet, dass sie ein handelsübliches Gerät enthält, vorzugsweise einen stationären Rechner (Computer), einen mobilen Rechner, z.B. Laptop oder ein Mobiltelephon.

20. Einrichtung nach Anspruch 13 dadurch gekennzeichnet, dass die Empfangseinheit ein medizinisches, therapeutisches oder diagnostisches Gerät enthält, vorzugsweise einen Herzschrittmacher.

21. Modulator bzw. Demodulator zur Modulation oder Demodulation der Information für eine Einrichtung zur Verschlüsselung von Daten oder Signalen, die aus einer Sendeeinheit mit einem Modulator zur Modulation der Information und mit einem Einkoppler zum Einkoppeln der Information in einen Zufallsprozess, einer Empfängereinheit mit einem Demodulator zur Demodulation der Information und einem Auskoppler zum Auskoppeln der Information aus dem Zufallsprozess besteht, insbesondere für ein Verfahren nach einem der Ansprüche 1-12, dadurch gekennzeichnet, dass der Modulator oder Demodulator ein Global-Scaling-Modulator bzw. Global-Scaling-Demodulator ist.

22. Modulator bzw. Demodulator nach Anspruch 21 dadurch gekennzeichnet, dass er ein Bauelement oder eine Einheit ist, die natürliche Rausch- oder Zufallssignale GS-moduliert bzw. GS-demoduliert, vorzugsweise mindestens eine Global-Scaling-Resonanzfrequenz zweier gekoppelter Zufallsprozesse.

23. Verwendung eines Rausch- oder Zufallsprozesses, Rausch- oder Zufallsprozesssignals oder Bauelementes zur Rausch- oder Zufallssignalerzeugung zur drahtlo-

sen Informationsübertragung eines Nutzsignals mittels gekoppelter Zufallsprozesse.

24. Verwendung eines Prozesses nach Anspruch 23, dadurch gekennzeichnet, dass der Rausch- oder Zufallsprozess oder das Rausch- oder Zufallsprozesssignal oder das Bauelement zur Rausch- oder Zufallssigalerzeugung zur Ein- oder Auskopplung aus den Zufallsprozessen und/oder zur Modulation oder Demodulation des Nutzsignales verwendet wird.

25. Verwendung nach Anspruch 23, dadurch gekennzeichnet, dass das Rausch- oder Zufallssignal eines Mobiltelephons oder eines stationären oder mobilen Rechners, z.B. eines Laptops, verwendet wird.

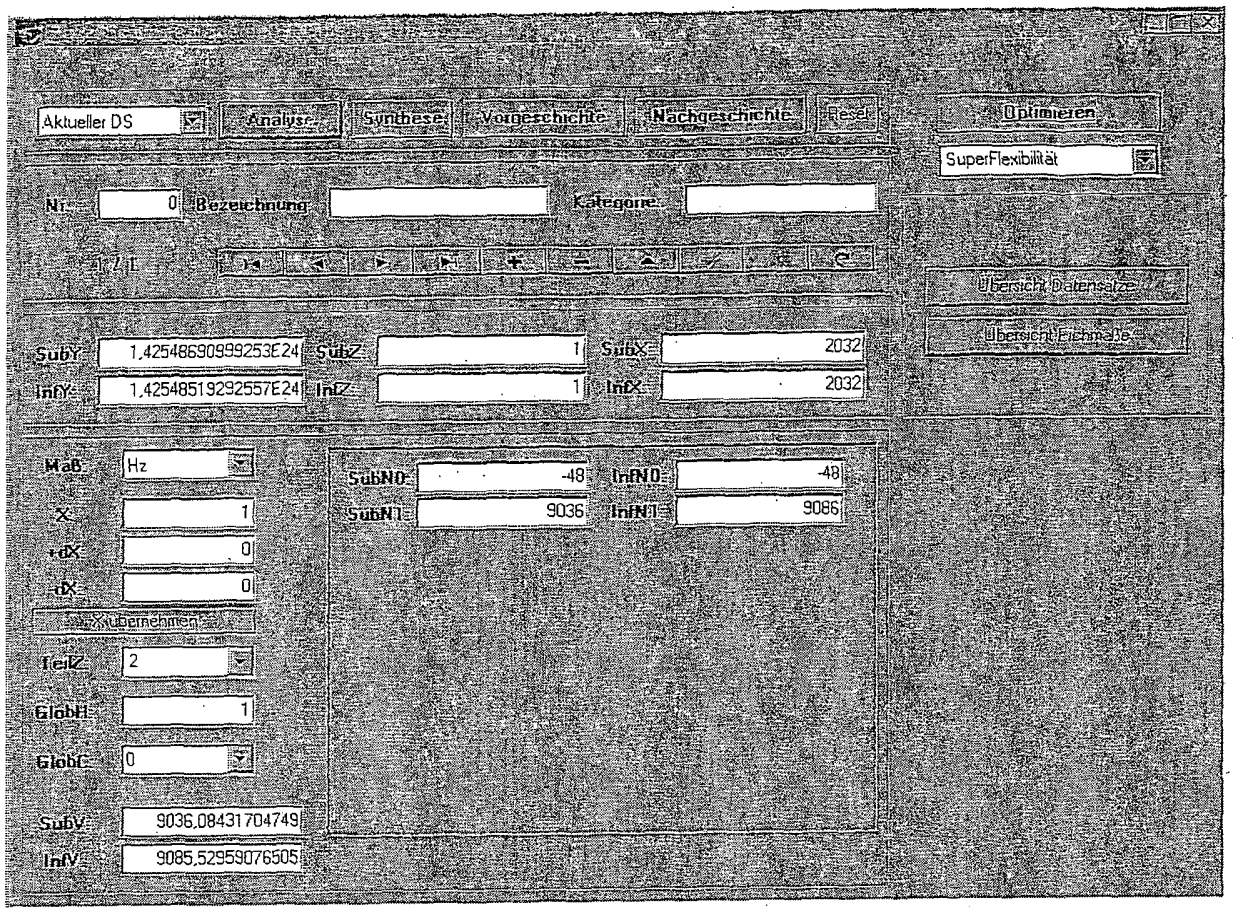

Aktueller DS
Analyse
Synthese
Vorgeschichte
Nachgeschichte
Reset
Optimieren
SuperFlexibilität
Nr
0
Bezeichnung
Kategorie
Übersicht Datensätze
Übersicht Fachmaße
SubY
1,42548690999253E24
SubZ
1
SubX
2032
InfY
1,42548519292557E24
InfZ
1
InfX
2032
MaB
Hz
SubN0
-48
InfN0
-48
X
1
SubN1
9036
InfN1
9086
+dX
0
-dX
0
Übernehmen
TeilZ
2
GlobH
1
GlobC
0
SubV
9036,08431704749
InfV
9085,52959076505

Fig. 1:

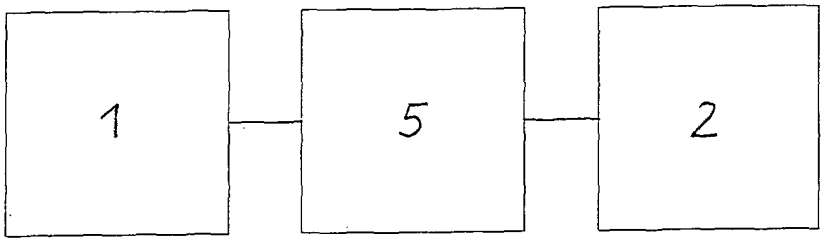

1
5
2

Fig. 2:

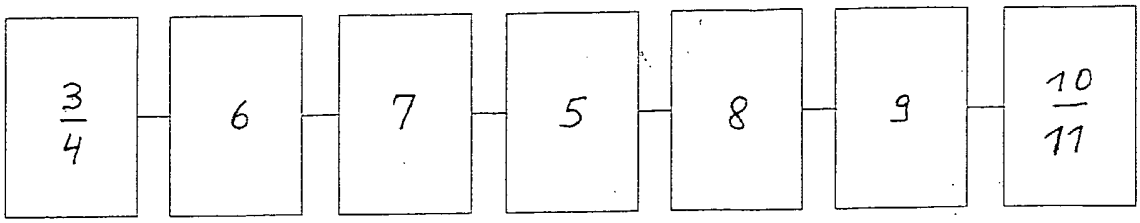


Fig. 3:

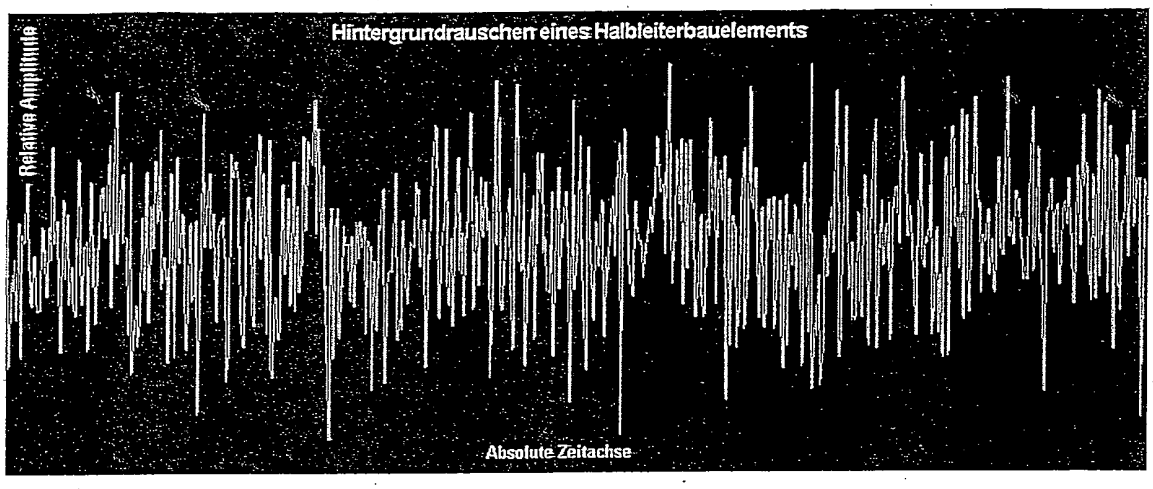

Hintergrundrauschen eines Halbleiterbauelements
Relative Amplitude
Absolute Zeitachse

Fig. 4:


Harmonische Komponenten des Hintergrundrauschens
Relative Frequenz
Relative Zeitachse

Fig. 5:

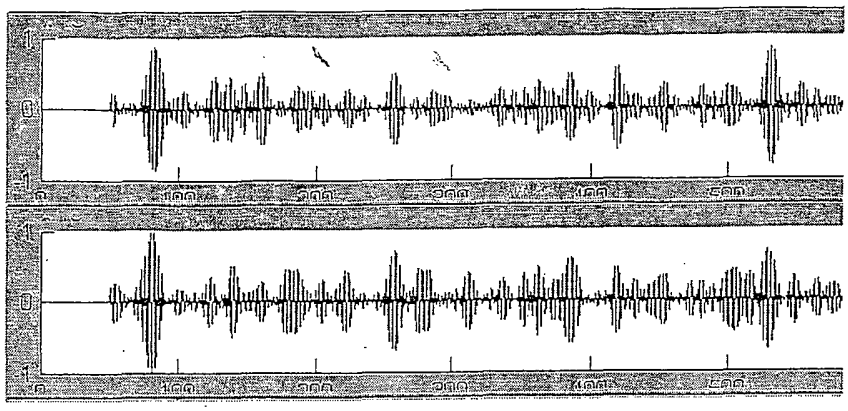


Fig. 6

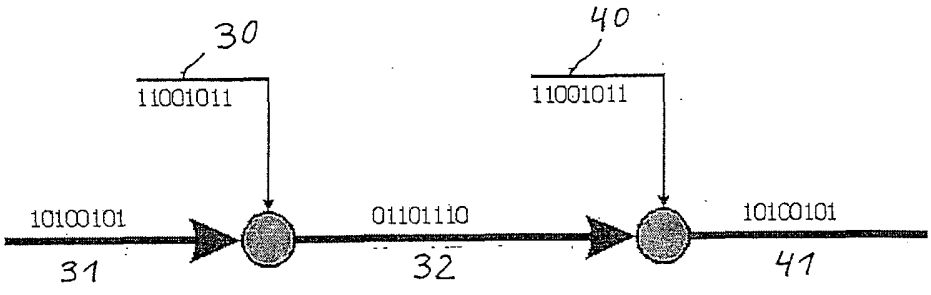

30
11001011
40
11001011
10100101
31
01101110
32
10100101
41

Fig. 7

INTERNATIONAL SEARCH REPORT

International Application No
PCT/CH2005/000427

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/18

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MUELLER H: "EPOCHALE ENTDECKUNG: TELEKOMMUNIKATION OHNE ELEKTROSMOG " RAUM & ZEIT, VERLAG, UNION VPM. WIESBADEN, DE, vol. 114, November 2001 (2001-11), pages 99-108, XP009045424 ISSN: 0722-7949 page 108, column 3, line 20 - column 4, last line	1
X	US 4 688 257 A (ERICKSON) 18 August 1987 (1987-08-18) abstract column 5, line 14 - line 38 column 6, line 64 - column 7, line 23	23,24

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 September 2005	05/10/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

INTERNATIONAL SEARCH REPORT

International Application No
PCT/CH2005/000427

C.(Continuation) *DOCUMENTS CONSIDERED TO BE RELEVANT*

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/176578 A1 (LAPAT RONALD H ET AL) 28 November 2002 (2002-11-28) paragraph '0021! - paragraph '0029! paragraph '0057! - paragraph '0062! -----	23,24
E	WO 2005/081433 A (GLOBAL SCALING TECHNOLOGIES AG; OTTE, RALF; MUELLER, HARTMUT; NATHANSE) 1 September 2005 (2005-09-01) the whole document -----	23,25
A	GB 2 388 279 A (PETER * COURTNEY; CHRISTOPHER * WHITE) 5 November 2003 (2003-11-05) page 10, line 15 - line 16 -----	2,10,15, 25

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/CH2005/000427

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4688257 A	18-08-1987	NONE	
US 2002176578 A1	28-11-2002	NONE	
WO 2005081433 A	01-09-2005	DE 102004008444 A1	08-09-2005
GB 2388279 A	05-11-2003	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internales Aktenzeichen
PCT/CH2005/000427

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/18

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L H04K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, INSPEC, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	MUELLER H: "EPOCHALE ENTDECKUNG: TELEKOMMUNIKATION OHNE ELEKTROSMOG " RAUM & ZEIT, VERLAG, UNION VPM. WIESBADEN, DE, Bd. 114, November 2001 (2001-11), Seiten 99-108, XP009045424 ISSN: 0722-7949 Seite 108, Spalte 3, Zeile 20 - Spalte 4, letzte Zeile	1
X	US 4 688 257 A (ERICKSON) 18. August 1987 (1987-08-18) Zusammenfassung Spalte 5, Zeile 14 - Zeile 38 Spalte 6, Zeile 64 - Spalte 7, Zeile 23	23,24

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
27. September 2005	05/10/2005

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

INTERNATIONALER RECHERCHENBERICHT

Internales Aktenzeichen
PCT/CH2005/000427

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2002/176578 A1 (LAPAT RONALD H ET AL) 28. November 2002 (2002-11-28) Absatz '0021! - Absatz '0029! Absatz '0057! - Absatz '0062!	23,24
E	WO 2005/081433 A (GLOBAL SCALING TECHNOLOGIES AG; OTTE, RALF; MUELLER, HARTMUT; NATHANSE) 1. September 2005 (2005-09-01) das ganze Dokument	23,25
A	GB 2 388 279 A (PETER * COURTNEY; CHRISTOPHER * WHITE) 5. November 2003 (2003-11-05) Seite 10, Zeile 15 - Zeile 16	2,10,15, 25

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/CH2005/000427

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 4688257	A	18-08-1987	KEINE	
US 2002176578	A1	28-11-2002	KEINE	
WO 2005081433	A	01-09-2005	DE 102004008444 A1	08-09-2005
GB 2388279	A	05-11-2003	KEINE	