PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro
INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation [7] :
H04L 9/08

A1

(11) Internationale Veröffentlichungsnummer: **WO 00/22775**

(43) Internationales Veröffentlichungsdatum: 20. April 2000 (20.04.00)

(21) Internationales Aktenzeichen: PCT/EP99/07051

(22) Internationales Anmeldedatum: 22. September 1999 (22.09.99)

(30) Prioritätsdaten:
198 47 941.7 9. Oktober 1998 (09.10.98) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DEUTSCHE TELEKOM AG [DE/DE]; Friedrich–Ebert–Allee 140, D–53113 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: SCHWENK, Jörg [DE/DE]; Südwestring 27, D–64807 Dieburg (DE).

(74) Gemeinsamer Vertreter: DEUTSCHE TELEKOM AG; Rechtsabteilung (Patente), PA1, D–64307 Darmstadt (DE).

(81) Bestimmungsstaaten: HU, IL, JP, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

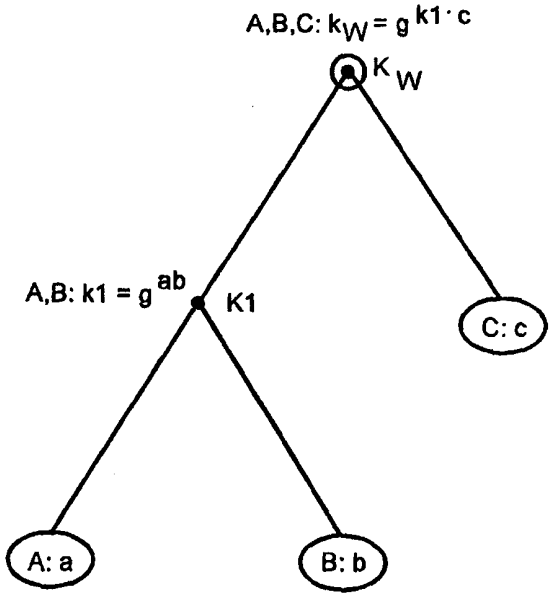
Veröffentlicht
Mit internationalem Recherchenbericht.

(54) Title: METHOD FOR ESTABLISHING A COMMON CRYPTOGRAPHIC KEY FOR N SUBSCRIBERS

(54) Bezeichnung: VERFAHREN ZUM ETABLIEREN EINES GEMEINSAMEN KRYPTOGRAFISCHEN SCHÜSSELS FÜR N TEILNEHMER

(57) Abstract

The aim of the invention is to provide a method which also enables subscribers to be easily deleted from or added to the key directory after the group key has been established. According to the invention, a terminal node of a binary–structured tree is allocated to each of the n subscribers (I), said tree having exactly n terminal nodes and having a depth [$\log_2 n$]. A secret (i) is generated for each subscriber (I) and allocated to the particular terminal node of the tree to which the subscriber (I) is allocated. Secrets are then established for all of the nodes (K) of the tree in succession, in the direction of the roots of the tree. Two already known secrets are always amalgamated into one new, joint secret using the DH method. The last node K_W contains the joint key for all n subscribers. The inventive method can be used particularly advantageously for producing a cryptographic key for a group of subscribers whose number is subject to changes.



(57) Zusammenfassung

Das Verfahren soll so ausgebildet werden, daß auch nach dem Etablieren des Gruppenschlüssels ohne großen Aufwand Teilnehmer aus dem Schlüsselverzeichnis gelöscht oder hinzugefügt werden können. Erfindungsgemäß wird jedem der n Teilnehmer (I) jeweils ein Blatt eines binär strukturierten Baumes, der genau n Blätter und die Tiefe [$\log_2 n$] besitzt, zugeordnet. Für jeden Teilnehmer (I) wird ein Geheimnis (i) generiert und dem Blatt des Baumes zugeordnet wird, dem auch der jeweilige Teilnehmer (I) zugeordnet ist. Nacheinander werden in Richtung der Baumwurzel für alle Knoten (K) des Baumes Geheimnisse etabliert, wobei immer zwei bereits bekannte Geheimnisse über das DH–Verfahren zu einem neuen gemeisamen Geheimnis zusammengefaßt werden. Der letzte Knoten K_W enthält den gemeinsamen Schlüssel aller n Teilnehmer. Das erfindungsgemäße Verfahren läßt sich vorteilhaft zur Erzeugung eines kryptografischen Schlüssels für eine Gruppe von Teilnehmern einsetzen, deren Teilnehmerzahl Änderungen unterworfen ist.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

Verfahren zum Etablieren eines gemeinsamen kryptografischen Schlüssels für n Teilnehmer

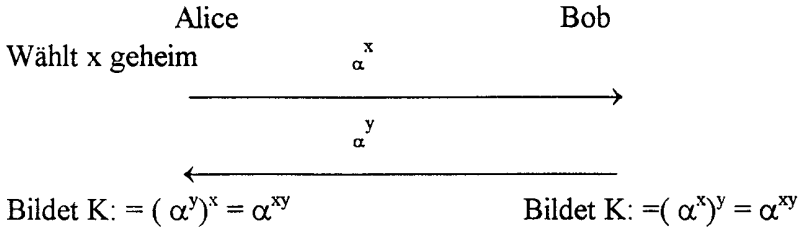
Beschreibung:

Das erfindungsgemäße Verfahren dient der Erzeugung und dem Etablieren eines gemeinsamen kryptografischen Schlüssels für n Teilnehmer zur Gewährleistung der Geheimhaltung von Nachrichten, die über unsichere Kommunikationskanäle ausschließlich an die n Teilnehmer übertragen werden sollen.

Zum Schutz der Vertraulichkeit und Integrität der Kommunikation zwischen zwei oder mehr Personen werden die Mechanismen der Verschlüsselung und Authentisierung eingesetzt. Diese erfordern allerdings das Vorhandensein einer gemeinsamen Information bei allen Teilnehmern. Diese gemeinsame Information wird als kryptographischer Schlüssel bezeichnet.

Ein bekanntes Verfahren zum Etablieren eines gemeinsamen Schlüssels über unsichere Kommunikationskanäle ist das Verfahren von Diffie und Hellman (DH-Verfahren; vergleiche W. Diffie und M. Hellman, New Directions in Cryptography, IEEETransactions on Information Theory, IT-22(6):644-654, November 1976).

Grundlage des Diffie-Hellmann-Schlüsselaustauschs (DH76) ist die Tatsache, daß es praktisch unmöglich ist, Logarithmen modulo einer großen Primzahl p zu berechnen. Dies machen sich Alice und Bob in dem unten abgebildeten Beispiel zunutze, indem sie jeweils eine Zahl x bzw. y kleiner als p (und teilerfremd zu p-1) geheim wählen. Dann senden sie sich (nacheinander oder gleichzeitig) die x-te (bzw. y-te) Potenz einer öffentlich bekannten Zahl α zu. Aus den empfangenen Potenzen können sie durch erneutes Potenzieren mit x bzw. y einen gemeinsamen Schlüssel $K := \alpha^{xy}$ berechnen. Ein Angreifer, der nur α^x und α^y sieht, kann daraus K nicht berechnen. (Die einzige heute bekannte Methode dazu bestünde darin, zunächst den Logarithmus z. B. von α^x zur Basis α modulo p zu berechnen und dann α^y damit zu potenzieren.)



Beispiel für Diffie-Hellmann-Schlüsselaustausch

Das Problem bei dem im Beispiel beschriebenen DH-Schlüsselaustausch besteht darin, daß Alice nicht weiß, ob sie tatsächlich mit Bob oder mit einem Betrüger kommuniziert. In IPSec wird dieses Problem durch den Einsatz von Public-Key-Zertifikaten gelöst, in denen durch eine vertrauenswürdige Instanz die Identität eines Teilnehmers mit einem öffentlichen Schlüssel verknüpft wird. Dadurch wird die Identität eines Gesprächspartners überprüfbar.

Der DH-Schlüsselaustausch kann auch mit anderen mathematischen Strukturen realisiert werden, z. B. mit endlichen Körpern GF(2^n) oder elliptischen Kurven. Mit diesen Alternativen kann man die Performance verbessern. Dieses Verfahren ist allerdings nur zur Vereinbarung eines Schlüssels zwischen zwei Teilnehmern geeignet.

Es wurden verschiedene Versuche unternommen, das DH-Verfahren auf drei oder mehr Teilnehmer zu erweitern (Gruppen DH). (Einen Überblick über den Stand der Technik bietet M. Steiner, G. Tsudik, M. Waidner, Diffie-Hellman Key Distribution Extended to Group Communication. Proc. 3rd ACM Conference on Computer and Communications Security, März 1996, Neu Delhi, Indien.)

Eine Erweiterung des DH-Verfahren auf drei Teilnehmer A, B und C wird z. B. durch nachfolgende Tabelle beschrieben. (Berechnung jeweils mod p):

	$A \rightarrow B$	$B \rightarrow C$	$C \rightarrow A$
1. Runde	g^a	g^b	g^c
2. Runde	g^{ca}	g^{ab}	g^{bc}

Nach Durchführung dieser beiden Runden kann jeder der drei Teilnehmer den geheimen Schlüssel g^{abc} mod p berechnen.

Bei allen diesen Erweiterungen tritt mindestens eines der drei folgenden Probleme auf:

- Die Teilnehmer müssen in einer bestimmten Art und Weise geordnet sein, im obigen Beispiel z. B. als Kreis.
- Die Teilnehmer haben gegenüber der Zentrale keinen Einfluß auf die Auswahl des Schlüssels.
- Die Rundenzahl ist abhängig von der Teilnehmerzahl

Ein weiteres Verfahren zum gemeinsamen Etablieren eines Schlüssels ist aus DE 195 38 385.0 bekannt. Bei diesem Verfahren muß die Zentrale allerdings die geheimen Schlüssel der Teilnehmer kennen.

Weiterhin ist eine Lösung aus Burmester, Desmedt, A secure and efficient conference key distribution system, Proc. EUROCRYPT'94, Springer LNCS, Berlin 1994 bekannt, bei der zwei Runden zur Generierung des Schlüssels benötigt werden, wobei in der zweiten Runde durch die Zentrale für n Teilnehmer n Nachrichten der Länge p = ca. 1000 Bit gesendet werden müssen.
Bekannt ist auch ein als (n,t)-Threshold-Verfahren bezeichnetes kryptografisches Verfahren. Mit einem (n,t)-Threshold-Verfahren kann man einen Schlüssel k so in t Teile, die shadows genannt werden, zerlegen, daß dieser Schlüssel k aus je n der t shadows rekonstruiert werden kann (vgl. Beutelspacher, Schwenk, Wolfenstetter: Moderne Verfahren der Kryptographie (2. Auflage), Vieweg Verlag, Wiesbaden 1998).

Das vorliegende Verfahren soll das Etablieren eines gemeinsamen Gruppenschlüssels zwischen einer Zentrale und einer Gruppe von n Teilnehmern ermöglichen . Das Verfahren soll so ausgebildet werden, daß auch nach dem Etablieren des Gruppenschlüssels ohne großen Aufwand Teilnehmer aus dem Schlüsselverzeichnis gelöscht oder hinzugefügt werden können.

Die Aufgabenstellung wird durch eine Verfahren gelöst, bei welchem das Etablieren eines Gruppenschlüssels mit Hilfe einer Baumstruktur vorgenommen wird. Erfindungsgemäß wird dazu die Anzahl der an der Schlüsselvereinbarung beteiligten Teilnehmer n als binärer Baum mit n Blättern darstellen. Für jede natürliche Zahl n gibt es ein oder mehr

Darstellungen dieser Art. Die Anzahl der Blätter ist dabei mit der Anzahl der in das Verfahren einbezogenen Teilnehmer identisch. Das bedeutet, daß einer Anzahl von n Teilnehmern eine Anzahl von n Blätter eines binären Baumes mit der Tiefe $\lceil \log_2 n \rceil$ zugeordnet ist

Fig. 1 zeigt das Wirkprinzip des erfindungsgemäßen Verfahrens anhand der Baumstruktur einer Schlüsselvereinbarung für drei Teilnehmer A, B, C

Um einen gemeinsamen Schlüssel zu etablieren, gehen die Teilnehmer A, B und C wie folgt vor:

- Teilnehmer A und B führen ein DH-Verfahren mit nach dem Zufallsprinzip generierten Zahlen a und b durch. Sie erhalten den gemeinsamen Schlüssel $k1=g^{ab} \bmod p$, der dem gemeinsamen Knoten K1 zugeordnet wird.
- Teilnehmer A und B auf der einen und Teilnehmer C auf der anderen Seite führen ein zweites DH-Verfahren durch, welches auf dem gemeinsamen Schlüssel k1 der Teilnehmer A und B und auf einer nach dem Zufallsprinzip generierten Zahl c des Teilnehmers C beruht. Das Ergebnis ist der gemeinsame Schlüssel $k=g^{kl \cdot c} \bmod p$, der der Wurzel des Baumes K_W zugeordnet wird.

Das erfindungsgemäße Verfahren wird anhand von Ausführungsbeispielen näher erläutert.

In Fig. 2 ist die Baumstruktur für eine Schlüsselvereinbarung für vier Teilnehmer A, B, C und D dargestellt.

Fig 3 zeigt die Baumstruktur einer Schlüsselvereinbarung für 5 Teilnehmer A, B, C, D und E.

Fig. 4 zeigt, ausgehend von einer bereits bestehenden Baumstruktur nach Fig.2, ein Beispiel für die Erweiterung der Baumstruktur um einen Teilnehmer.

Fig. 5 zeigt, ausgehend von einer bereits bestehenden Baumstruktur nach Fig. 2, das Entfernen/Löschen eines Teilnehmers aus der Baumstruktur.

Nachfolgend wird anhand von Figur 2 ein Beispiel einer Schlüsselvereinbarung für vier Teilnehmer A, B, C und D beschrieben:

Um einen gemeinsamen Schlüssel für vier Teilnehmer (Fig.2) zu etablieren, gehen Teilnehmer A, B, C und D wie folgt vor:

- Teilnehmer A und B führen ein DH-Verfahren mit nach dem Zufallsprinzip generierten Zahlen a und b durch. Sie erhalten den gemeinsamen Schlüssel $k1=g^{ab} \bmod p$.
- Teilnehmer C und D führen ein DH-Verfahren mit zufällig gewählten Zahlen c und d durch. Sie erhalten den gemeinsamen Schlüssel $k2=g^{cd} \bmod p$.
- Teilnehmer A und B auf der einen und Teilnehmer C und D auf der anderen Seite führen gemeinsam ein zweites DH-Verfahren durch, in welches von Teilnehmer A und B der Schlüssel k1 und von Teilnehmer C und D der Schlüssel k2 einbezogen werden. Das Ergebnis ist der gemeinsame Schlüssel $k_W=g^{k1 \cdot k2} \bmod p$, welcher der Wurzel des Baumes K_W zugeordnet ist.

Nachfolgend wird anhand von Figur 3 ein Beispiel einer Schlüsselvereinbarung für fünf Teilnehmer A, B, C, D, und E beschrieben:

Um einen gemeinsamen Schlüssel zu etablieren, gehen die Teilnehmer A, B, C, D und E wie folgt vor:

- Teilnehmer A und B führen ein DH-Verfahren mit zufällig gewählten Zahlen a und b durch. Sie erhalten den gemeinsamen Schlüssel $k1=g^{ab} \bmod p$.
- Teilnehmer C und D führen ein DH-Verfahren mit zufällig gewählten Zahlen c und d durch. Sie erhalten den gemeinsamen Schlüssel $k2=g^{cd} \bmod p$.
- Teilnehmer A und B auf der einen Seite und Teilnehmer C und D auf der anderen Seite führen gemeinsam ein zweites DH-Verfahren durch, in welches von Teilnehmer A und B der gemeinsame Schlüssel k1 und von Teilnehmer C und D der gemeinsame Schlüssel k2 einbezogen werden.. Das Ergebnis ist ein gemeinsamer Schlüssel $k3=g^{k1 \cdot k2} \bmod p$ für die Teilnehmer A, B, C und D.
- Die Teilnehmer A, B, C und D auf der einen Seite und der Teilnehmer E auf der anderen Seite führen ein drittes DH-Verfahren durch, in welches der gemeinsame Schlüssel k3 der Teilnehmer A, B, C und D und eine für den Teilnehmer E generierte Zufallszahl e einbezogen werden. Das Ergebnis ist der gemeinsame Schlüssel $k_W=g^{k3 \cdot e} \bmod p$, der der Wurzel des Baumes K_W zugeordnet ist.

Aufgrund der Struktur des erfindungsgemäßen Verfahrens ist es möglich, neue Teilnehmer mit einzubeziehen bzw. einzelne Teilnehmer auszuschließen, ohne das ganze Verfahren für jeden Teilnehmer noch einmal durchführen zu müssen.

Das Einfügen eines neuen Teilnehmers wird anhand einer Baumstruktur mit vier Teilnehmern nach Fig. 4 näher erläutert: Ausgangssituation ist dabei eine Baumstruktur entsprechend Fig. 2 in welche eine neuer Teilnehmer bei Blatt B eingefügt werden soll. Bei Hinzunahme eines neuen Teilnehmers in eine bereits bestehende Baumstruktur, die über ein gemeinsames Geheimnis verfügt, werden zum Etablieren eines neuen gemeinsamen Schlüssels für n+1 Teilnehmer an einer geeigneten Stelle des binären Baumes (Blatt B vorgegeben) zwei neue Blätter B1 und B2 angefügt. Der neue Baum besitzt dann n+1 Blätter und die Tiefe $\lceil \log_2(n+1) \rceil$. Der bisher dem Blatt B zugeordnete Teilnehmer wird einem der neue Blätter B1 zugeordnet. Der neue Teilnehmer wird dem anderen noch freien Blatt B2 zugeordnet. Das bisherige Blatt B wird zu einem Knoten K1 für die Blätter B1 und B2. Ausgehend von den neuen Blättern B1 und B2 werden bis hin zur Wurzel des Baumes nur in den Knoten K neue Geheimnisse etabliert, die im Rahmen der Baumstruktur auf dem Weg von den neuen Blättern B1 und B2 zur Wurzel des Baumes K_W liegen. Das sind im konkreten Fall die Knoten K1, K2 und K_W.

Ist die Anzahl der Teilnehmer eine Zweierpotenz, so erhöht sich die Tiefe des Baumes durch diesen Vorgang um 1 (vgl. vorhergehendes Beispiel). Ist die Anzahl der Teilnehmer keine Zweierpotenz, so kann durch geschickte Wahl des aufzuteilenden Blattes eine Vergrößerung der Tiefe vermieden werden, wie das folgende Beispiel zeigt:

Um beispielsweise einen vierten Teilnehmer zu drei Teilnehmern hinzuzufügen, geht man (ausgehend von der Situation nach Fig.1) wie folgt vor:

- Teilnehmer C führt mit dem neu hinzugekommenen Teilnehmer D ein DH-Verfahren mit zufällig generierten Zahlen c` und d durch (c` sollte sich von dem vorher gewählten c unterscheiden, dies muß aber nicht der Fall sein). Das Ergebnis ist $k2` = g^{c`d} \bmod p$.
- Teilnehmer A und Teilnehmer B auf der einen und Teilnehmer C und D auf der anderen Seite führen ein DH-Verfahren mit den Werten k1 und k2` durch. Das Ergebnis ist $k = g^{k1 \cdot k2`} \bmod p$.

Bei einer derartigen Konfiguration müssen die Teilnehmer A und B keinen neuen Schlüsseltausch durchführen. Generell müssen nur die Geheimnisse neu vereinbart werden, die im zugehörigen Baum auf dem Weg vom Blatt des neuen Teilnehmers zur Wurzel K_W liegen.

Das Ausschließen bzw. Löschen eines Teilnehmers wird anhand einer Baumstruktur mit vier Teilnehmern anhand von Figur 5 näher erläutert: Ausgangssituation ist dabei eine Baumstruktur entsprechend Fig. 2, aus der Teilnehmer B entfernt werden soll.
Beim Ausschließen bzw. beim Löschen eines Teilnehmers B aus einer bereits bestehenden Baumstruktur, die über ein gemeinsames Geheimnis verfügt, werden wie in Fig. 5 ausgeführt, sowohl das Blatt des zu entfernenden Teilnehmers B als auch das Blatt des dem gleichen gemeinsamen Knoten K1 zugeordneten Teilnehmers A entfernt. Der gemeinsame Knoten K1 wird zum neuen Blatt A´ des in der Baumstruktur verbleibenden Teilnehmers A. Ausgehend von den Blättern des Baumes bis zur Wurzel K_W werden nur in den Knoten K neue Geheimnisse etabliert, die vom neuen Blatt A´ im Rahmen der Baumstruktur in Richtung Wurzel K_W unmittelbar tangiert werden. Das ist im konkreten Fall nur der Wurzelknoten K_W. Bei einer derartigen Konfiguration müssen die Teilnehmer C und D keinen neuen Schlüsseltausch durchführen. Generell müssen auch hier nur die Geheimnisse neu vereinbart werden, die im zugehörigen Baum auf dem Weg vom Blatt des Partners des entfernten Teilnehmers zur Wurzel liegen.

Das Verfahren kann in vielfacher Hinsicht zweckmäßig weiter ausgestaltet werden:
Für die Bildung der diskreten Exponentialfunktion $x \rightarrow g^x$ bietet sich beispielsweise die Verwendung anderer Gruppen an.
Beim Hinzufügen oder Entfernen eines Teilnehmers kann beispielsweise vereinbart werden, daß für die notwendigen neuen Durchführungen des DH-Verfahrens nicht die alten Geheimnisse, sondern das Ergebnis einer (evtl. randomisierten) Einwegfunktion verwendet wird.

(3) Patentansprüche:

1. Verfahren zum Etablieren eines gemeinsamen kryptografischen Schlüssels für n Teilnehmer unter Anwendung des DH-Verfahrens,
dadurch gekennzeichnet,
-daß jedem der n Teilnehmer (I) jeweils ein Blatt eines binär strukturierten Baumes, der genau n Blätter und die Tiefe $\lceil \log_2 n \rceil$ besitzt, zugeordnet wird,
-daß für jeden Teilnehmer (I) ein Geheimnis (i) generiert und dem Blatt des Baumes zugeordnet wird, dem auch der jeweilige Teilnehmer (I) zugeordnet ist,
-daß nacheinander in Richtung der Baumwurzel für alle Knoten (K) des Baumes Geheimnisse etabliert werden, wobei ausgehend von den Blättern entsprechend der festgelegten Baumstruktur über die gesamte Hierarchie der Baumstruktur immer zwei bereits bekannte Geheimnisse über das DH-Verfahren zu einem neuen gemeinsamen Geheimnis zusammengefaßt und einem gemeinsamen Knoten (K) zu geordnet werden, so daß der letzte Knoten K_W und damit die Baumwurzel, als Geheimnis den gemeinsamen Schlüssel aller n Teilnehmer enthält.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,**
-daß bei Aufnahme eines neuen Teilnehmers in eine bestehende Baumstruktur, die bereits über ein gemeinsames Geheimnis verfügt, zum Etablieren eines gemeinsamen Schlüssel für n+1 Teilnehmer an geeigneter Stelle des binären Baumes einem Blatt (B) als Nachfolger zwei neue Blätter (B1 und B2) angefügt werden, so daß der neue Baum genau n+1 Blätter und die Tiefe $\lceil \log_2(n+1) \rceil$ besitzt,
-daß der dem bisherigen Blatt (B) zugeordnete Teilnehmer und der neue Teilnehmer jeweils einem der neuen Blätter (B1; B2) zugeordnet werden, wobei das bisherige Blatt B zu einem gemeinsamen Knoten für die neuen Blätter (B1;B2) wird,
-daß ausgehend von den neuen Blättern (B1;B2) bis zur Wurzel des Baumes nur in den Knoten neue Geheimnisse etabliert werden, die im Rahmen der Baumstruktur auf dem Weg von den Blättern B1 und B2 zur Baumwurzel liegen.

3. Verfahren nach Anspruch 1, **d a d u r c h g e k e n n z e i c h n e t**,

-daß bei Ausschließung eines Teilnehmers (B) aus einer bereits bestehenden Baumstruktur die bereits über ein Geheimnis verfügt, sowohl das Blatt des zu entfernenden Teilnehmers (B), als auch daß Blatt des dem gleichen gemeinsamen Knoten zugeordneten Teilnehmers (A) entfernt werden,

-daß der gemeinsame Knoten zum Blatt des nicht zu entfernende Teilnehmers A wird, und daß ausgehend von den Blättern des Baumes bis zur Wurzel nur in den Knoten neue Geheimnisse ertabliert werden, die im Rahmen der Baumstruktur auf dem Weg vom neuen Blatt (A) zur Baumwurzel liegen.

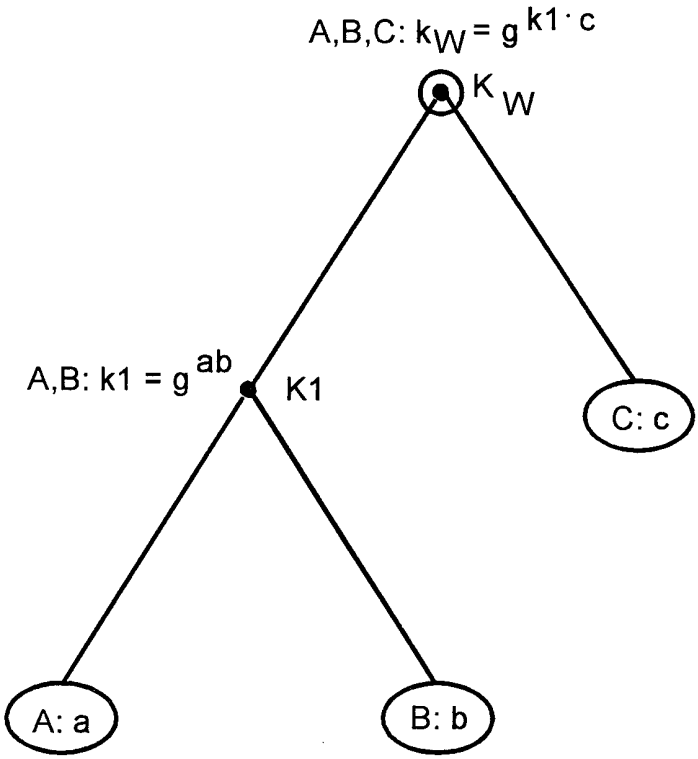


Fig. 1

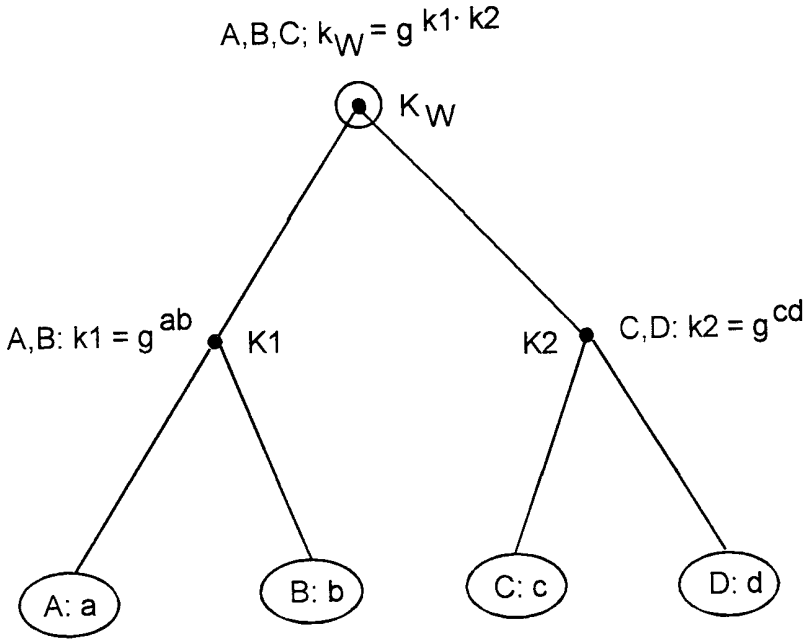

A,B,C; $k_W = g^{k1 \cdot k2}$
K_W
A,B: $k1 = g^{ab}$
K1
K2
C,D: $k2 = g^{cd}$
A: a
B: b
C: c
D: d

Fig. 2

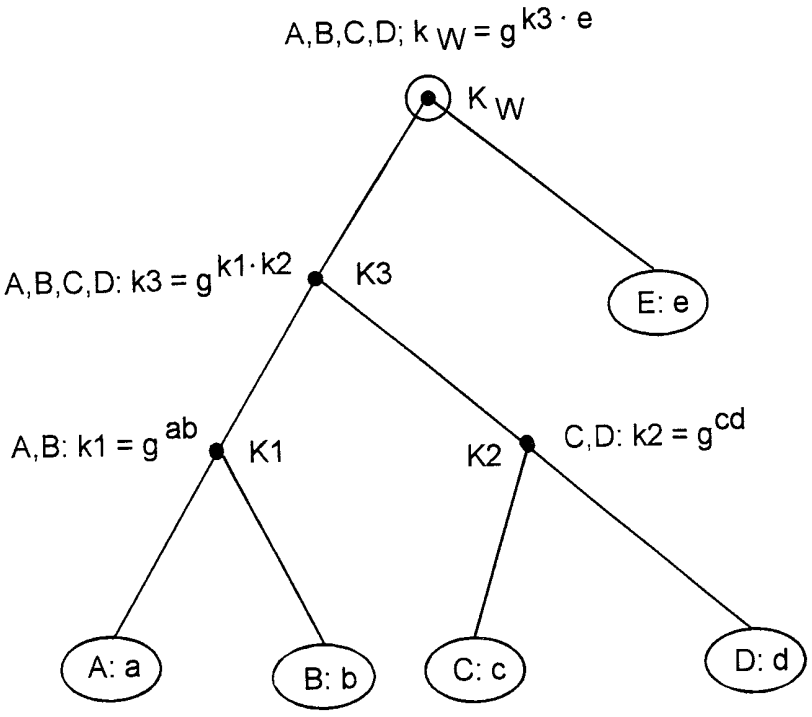

A,B,C,D; $k_W = g^{k3 \cdot e}$
K_W
A,B,C,D: $k3 = g^{k1 \cdot k2}$
K3
E: e
A,B: $k1 = g^{ab}$
K1
K2
C,D: $k2 = g^{cd}$
A: a
B: b
C: c
D: d

Fig. 3

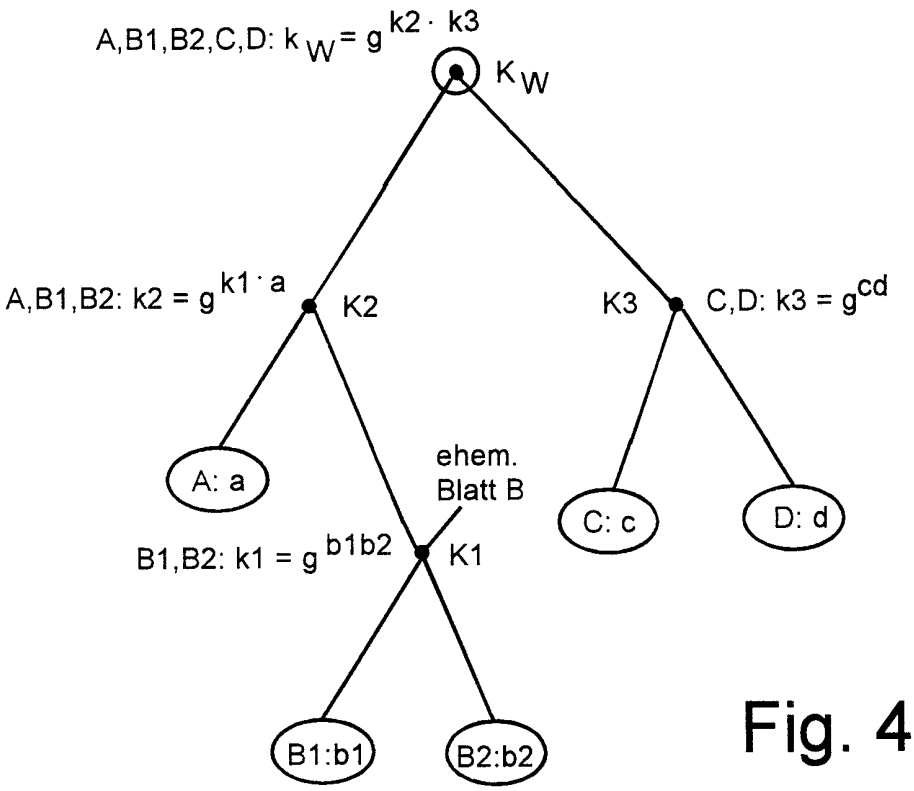

A,B1,B2,C,D: $k_W = g^{k2 \cdot k3}$
K_W
A,B1,B2: $k2 = g^{k1 \cdot a}$
K2
K3
C,D: $k3 = g^{cd}$
A: a
ehem.
Blatt B
C: c
D: d
B1,B2: $k1 = g^{b1b2}$
K1
B1:b1
B2:b2

Fig. 4

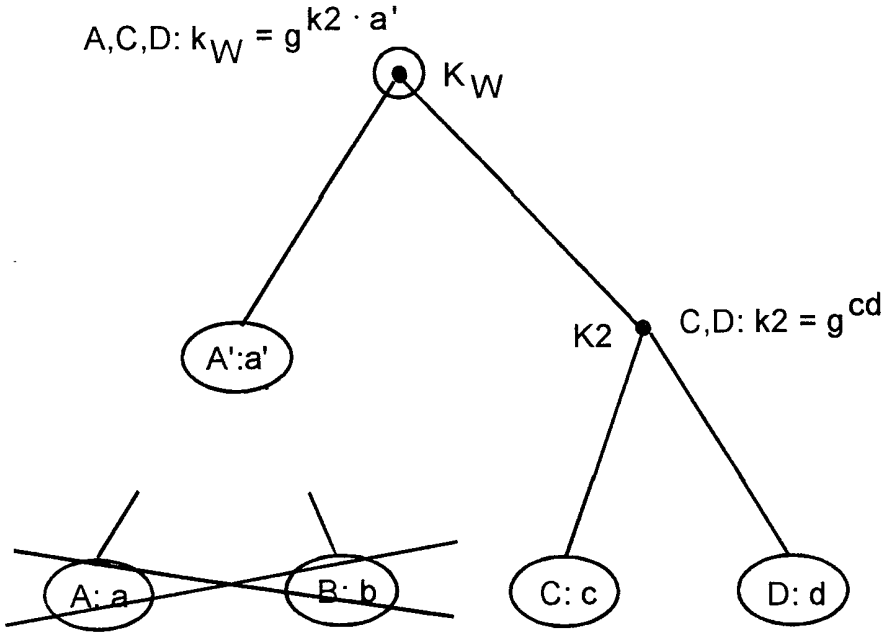

A,C,D: $k_W = g^{k2 \cdot a'}$
K_W
A':a'
K2
C,D: $k2 = g^{cd}$
A: a
B: b
C: c
D: d

Fig. 5

INTERNATIONAL SEARCH REPORT

Inte. .onal Application No
PCT/EP 99/07051

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08

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

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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DAVID A. MCGREW AND ALAN T. SHERMAN: "Key establishment in large dynamic groups using one-way function trees", 20. Mai 1998 (1998-05-20), Seiten 1-13 Verfügbar auf Internet: <http://www.cs.umbc.edu/{sherman/Papers/itse.ps> 23. Juni 1998 XP002126220 page 3 -page 4; figure 1 ---	1-3
A	DE 196 49 292 A (DEUTSCHE TELEKOM AG) 4 June 1998 (1998-06-04) column 3, line 23 -column 5, line 55; figure 1 ---	1-3

-/--

[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
20 December 1999	27/01/2000

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	Zucka, G

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte .ional Application No
PCT/EP 99/07051

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	BURMESTER M ET AL: "A secure and efficient conference key distribution system" ADVANCES IN CRYPTOLOGY - EUROCRYPT '94. WORKSHOP ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. PROCEEDINGS, PROCEEDINGS OF EUROCRYPT '94, PERUGIA, ITALY, 9-12 MAY 1994, pages 275-286, XP000852509 1995, Berlin, Germany, Springer-Verlag, Germany ISBN: 3-540-60176-7 cited in the application page 278, last paragraph -page 279, paragraph 1 ---	1-3
A	STEINER M ET AL: "Diffie-Hellman key distribution extended to group communication" 3RD ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, PROCEEDINGS OF 3RD ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, NEW DELHI, INDIA, 14-16 MARCH 1996,1996, pages 31-37, XP000620975 New York, NY, USA, USA ISBN: 0-89791-829-0 cited in the application page 34, column 2 -page 35, column 1 ---	1-3
A	EP 0 768 773 A (DEUTSCHE TELEKOM AG) 16 April 1997 (1997-04-16) cited in the application claim 1 ---	1
A	STEINER M ET AL: "CLIQUES: a new approach to group key agreement" PROCEEDINGS. 18TH INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS (CAT. NO.98CB36183), PROCEEDINGS OF 18TH INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS, AMSTERDAM, NETHERLANDS, 26-29 MAY 1998, pages 380-387, XP002126180 1998, Los Alamitos, CA, USA, IEEE Comput. Soc, USA ISBN: 0-8186-8292-2 page 382, column 1, last paragraph -page 385, column 1 -----	1-3

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte. ..ional Application No
PCT/EP 99/07051

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19649292 A	04-06-1998	NONE	
EP 0768773 A	16-04-1997	DE 19538385 A	17-04-1997
		AT 186432 T	15-11-1999
		AU 6572796 A	17-04-1997
		CA 2181972 A	15-04-1997
		DE 59603557 D	09-12-1999
		NO 962672 A	15-04-1997
		NZ 299014 A	24-09-1998
		US 5903649 A	11-05-1999

INTERNATIONALER RECHERCHENBERICHT

Inte. .onales Aktenzeichen
PCT/EP 99/07051

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/08

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L

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)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DAVID A. MCGREW AND ALAN T. SHERMAN: "Key establishment in large dynamic groups using one-way function trees", 20. Mai 1998 (1998-05-20), Seiten 1-13 Verfügbar auf Internet: <http://www.cs.umbc.edu/{sherman/Papers/itse.ps> 23. Juni 1998 XP002126220 Seite 3 -Seite 4; Abbildung 1 ---	1-3
A	DE 196 49 292 A (DEUTSCHE TELEKOM AG) 4. Juni 1998 (1998-06-04) Spalte 3, Zeile 23 -Spalte 5, Zeile 55; Abbildung 1 --- -/--	1-3

[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
20. Dezember 1999	27/01/2000

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	Zucka, G

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Inte. .onales Aktenzeichen
PCT/EP 99/07051

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	BURMESTER M ET AL: "A secure and efficient conference key distribution system" ADVANCES IN CRYPTOLOGY - EUROCRYPT '94. WORKSHOP ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. PROCEEDINGS, PROCEEDINGS OF EUROCRYPT '94, PERUGIA, ITALY, 9-12 MAY 1994, Seiten 275-286, XP000852509 1995, Berlin, Germany, Springer-Verlag, Germany ISBN: 3-540-60176-7 in der Anmeldung erwähnt Seite 278, letzter Absatz -Seite 279, Absatz 1 ---	1-3
A	STEINER M ET AL: "Diffie-Hellman key distribution extended to group communication" 3RD ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, PROCEEDINGS OF 3RD ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, NEW DELHI, INDIA, 14-16 MARCH 1996,1996, Seiten 31-37, XP000620975 New York, NY, USA, USA ISBN: 0-89791-829-0 in der Anmeldung erwähnt Seite 34, Spalte 2 -Seite 35, Spalte 1 ---	1-3
A	EP 0 768 773 A (DEUTSCHE TELEKOM AG) 16. April 1997 (1997-04-16) in der Anmeldung erwähnt Anspruch 1 ---	1
A	STEINER M ET AL: "CLIQUES: a new approach to group key agreement" PROCEEDINGS. 18TH INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS (CAT. NO.98CB36183), PROCEEDINGS OF 18TH INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS, AMSTERDAM, NETHERLANDS, 26-29 MAY 1998, Seiten 380-387, XP002126180 1998, Los Alamitos, CA, USA, IEEE Comput. Soc, USA ISBN: 0-8186-8292-2 Seite 382, Spalte 1, letzter Absatz -Seite 385, Spalte 1 -----	1-3

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internales Aktenzeichen
PCT/EP 99/07051

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 19649292 A	04-06-1998	KEINE	
EP 0768773 A	16-04-1997	DE 19538385 A	17-04-1997
		AT 186432 T	15-11-1999
		AU 6572796 A	17-04-1997
		CA 2181972 A	15-04-1997
		DE 59603557 D	09-12-1999
		NO 962672 A	15-04-1997
		NZ 299014 A	24-09-1998
		US 5903649 A	11-05-1999