

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

(19) Weltorganisation für geistiges
Eigentum

Internationales Büro

(43) Internationales
Veröffentlichungsdatum
20. August 2015 (20.08.2015)



(10) Internationale Veröffentlichungsnummer
WO 2015/121346 A1

(51) Internationale Patentklassifikation:
G06F 21/62 (2013.01)

(21) Internationales Aktenzeichen: PCT/EP2015/052959

(22) Internationales Anmeldedatum:
12. Februar 2015 (12.02.2015)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2014 101 710.2
12. Februar 2014 (12.02.2014) DE

(71) Anmelder: **UNISCON UNIVERSAL IDENTITY
CONTROL GMBH** [DE/DE]; Agnes-Pockels-Bogen 1,
80992 München (DE).

(72) Erfinder: **JÄGER, Hubert**; Habenschadenstr. 41a, 82049
Pullach (DE). **NGUYEN, Dau Khiem**; Agnes-Bernauer-
Str. 5, 80687 München (DE). **KARATZAS, Christos**;
Naupliastr. 33, 81547 München (DE).

(74) Anwalt: **2S-IP SCHRAMM SCHNEIDER
PATENTANWÄLTE - RECHTSANWÄLTE**; Postfach
86 02 67, 81629 München (DE).

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

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND SYSTEM FOR SAFEGUARDING DATABASE RELATIONS AGAINST UNAUTHORISED ACCESS

(54) Bezeichnung : VERFAHREN UND SYSTEM ZUM SICHERN VON DATENBANKRELATIONEN VOR UNBERECHTIGTEM ZUGRIFF

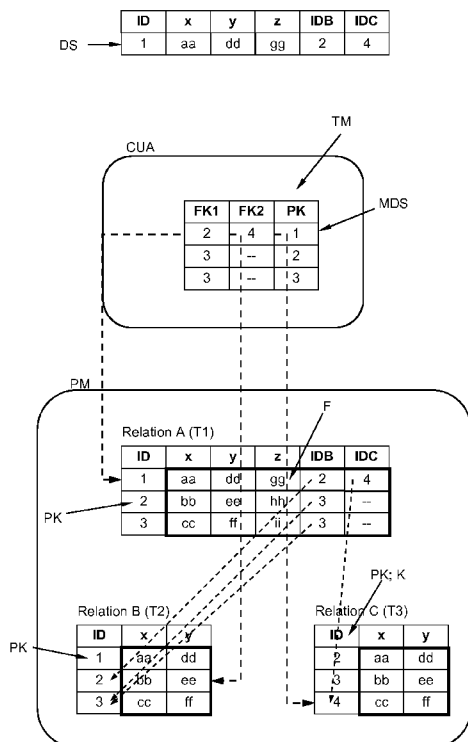


Fig. 3

(57) Abstract: The invention provides a method for safeguarding values of attributes of a data record that can be stored in a first relational database against unauthorised access, wherein a value of a foreign key attribute of the data record refers to a key for the first relation or for a second relation, and wherein – the value of the foreign key attribute is stored in a mapping relation, – the values of attributes of the data record that are not foreign key attributes are stored in the first relation, and – the mapping relation is stored in a volatile data memory. The invention also provides a method for setting up and/or restoring a mapping relation in a volatile data memory, wherein the mapping relation can be used to store values of foreign key attributes of a data record that is stored in a first relation of a database, wherein at least the values of the foreign key attributes in the first relation are cryptographically encrypted and can preferably be decrypted exclusively using a cryptographic key from the owner of the data record.

(57) Zusammenfassung: Bereitgestellt wird ein Verfahren zum Sichern von Werten von Attributen eines Datensatzes, der in einer ersten Relation einer Datenbank speicherbar

[Fortsetzung auf der nächsten Seite]

WO 2015/121346 A1



(84) **Bestimmungsstaaten** (soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,

CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— mit internationalem Recherchenbericht (Artikel 21 Absatz 3)

ist, vor einem unberechtigten Zugriff, wobei ein Wert eines Fremdschlüsselattributs des Datensatzes auf einen Schlüssel der ersten Relation oder einer zweiten Relation verweist, und wobei - der Wert des Fremdschlüsselattributs in einer Mapping-Relation gespeichert wird, - die Werte von Attributen, die keine Fremdschlüsselattribute sind, des Datensatzes in der ersten Relation gespeichert werden, und - die Mapping-Relation in einem flüchtigen Datenspeicher gespeichert wird. Bereitgestellt wird ferner ein Verfahren zum Herstellen und/oder Wiederherstellen einer Mapping-Relation in einem flüchtigen Datenspeicher, wobei in der Mapping-Relation Werte von Fremdschlüsselattributen eines Datensatzes, der in einer ersten Relation einer Datenbank gespeichert ist, speicherbar sind, wobei zumindest die Werte der Fremdschlüsselattribute in der ersten Relation kryptographisch verschlüsselt sind und vorzugsweise ausschließlich mit einem kryptographischen Schlüssel des Besitzers des Datensatzes entschlüsselbar sind.

Verfahren und System zum Sichern von Datenbankrelationen vor unberechtigtem Zugriff

5

Gegenstand der Erfindung

Die Erfindung betrifft ein Verfahren zum Sichern von Werten von Fremdschlüssel-
attributen eines Datensatzes vor einem unberechtigten Zugriff sowie ein Verfahren
zum Herstellen und/oder Wiederherstellen solcher Fremdschlüsselattribute in ei-
nem flüchtigen Datenspeicher aus einer Datenbank. Ferner betrifft die Erfindung
ein System, das angepasst ist, Werte von Fremdschlüsselattributen eines Datensat-
zes vor unberechtigtem Zugriff zu sichern und Werte von Fremdschlüsselattributen
in einem flüchtigen Datenspeicher wiederherzustellen.

Hintergrund der Erfindung und Stand der Technik

Es ist bekannt, Daten bzw. Datensätze in einer Datenbank kryptografisch zu ver-
schlüsseln. Hierdurch soll ein unberechtigter Zugriff auf die in der Datenbank ge-
speicherten Datensätze verhindert werden. Allerdings werden die Daten in der Da-
tenbank von dem Betreiber der Datenbank mit einem dem Datenbankbetreiber be-
kannten kryptografischen Schlüssel verschlüsselt und bei einem Zugriff auf die Da-
ten mit einem ebenfalls dem Datenbankbetreiber bekannten kryptografischen
Schlüssel entschlüsselt. Der Datenbankbetreiber hat also die Möglichkeit, jederzeit
auf die Daten in der Datenbank zuzugreifen, selbst wenn der Datenbankbetreiber
nicht Inhaber der Daten ist.

Damit einher geht ein weiterer Nachteil, dass der Datenbankbetreiber nicht nur die Datensätze einzelner Relationen (Datenbanktabellen) lesen kann, sondern auch die gegebenenfalls zwischen zwei oder mehreren Relationen vorhandenen Verknüpfungen lesen und auswerten kann, sodass der Datenbankbetreiber aus diesen Verknüpfungen auch Rückschlüsse, beispielsweise über ein Nutzerverhalten, ableiten kann. Beispielsweise können in einer ersten Relation personenbezogene Nutzerdaten und in einer zweiten Relation die Stammdaten für ein elektronisches Postfach gespeichert sein. In einer ersten Relation können Informationen gespeichert sein (als Fremdschlüssel auf die zweite Relation), die angeben, auf welches Postfach der zweiten Relation der jeweilige Nutzer Zugriff hat. Die Werte der Fremdschlüssel werden zusammen mit dem Datensatz, zu dem die Werte gehören, in der Datenbank gespeichert, d.h. die Werte der Fremdschlüssel und die Werte der Nicht-Schlüsselattribute bilden gegebenenfalls zusammen mit einem Primärschlüssel einen einzelnen Datensatz, der in einer Relation bzw. Datenbanktabelle gespeichert wird.

Haben beispielsweise zwei Nutzer der ersten Relation Zugriff auf ein und dasselbe Postfach in der zweiten Relation, so kann der Betreiber der Datenbank hieraus die Information ableiten, dass diese beiden Nutzer in Kontakt stehen und möglicherweise über dieses Postfach Informationen austauschen. Diese zusätzlichen Informationen werden auch Metadaten genannt.

Durch das Verschlüsseln der Datenbank alleine kann demnach nicht verhindert werden, dass der Betreiber der Datenbank an diese oder ähnliche Metainformationen, die sich aus den Beziehungen zwischen zwei oder mehreren Relationen in der Datenbank ergeben, gelangt.

Aufgabe der Erfindung

Aufgabe der vorliegenden Erfindung ist es daher, Verfahren und Systeme bereitzustellen, mit denen effektiv und effizient verhindert werden kann, dass einerseits unberechtigte Personen und andererseits die Betreiber von Datenbanken an Metainformationen, die sich aus den Beziehungen zweier oder mehrerer Datenbankrelationen ergeben, gelangen können.

Erfindungsgemäße Lösung

- 10 Diese Aufgabe wird erfindungsgemäß durch die Verfahren, das System und ein Computerprogrammprodukt nach den unabhängigen Ansprüchen gelöst. Vorteilhafte Ausgestaltungen und Weiterbildungen der Erfindung sind in den jeweiligen abhängigen Ansprüchen angegeben.
- 15 Bereitgestellt wird demnach ...

[Ansprüche und deren Vorteile werden hier noch eingefügt]

20 Kurzbeschreibung der Figuren

Einzelheiten und Merkmale der Erfindung sowie konkrete Ausgestaltungen der Erfindung ergeben sich aus der nachfolgenden Beschreibung in Verbindung mit der Zeichnung. Es zeigt:

25

- Fig. 1 ein erstes Beispiel einer Datenstruktur zur Verdeutlichung der erfindungsgemäßen Verfahren;
- Fig. 2 ein zweites Beispiel einer Datenstruktur zur Verdeutlichung einer zweiten Variante der erfindungsgemäßen Verfahren; und

Fig. 3 ein drittes Beispiel einer Datenstruktur zur Verdeutlichung einer dritten Variante der erfindungsgemäßen Verfahren.

5

Detaillierte Beschreibung der Erfindung

Fig. 1 zeigt eine Datenstruktur, mit der in vorteilhafter Weise Werte von Fremdschlüsselattributen eines Datensatzes DS vor einem unberechtigten Zugriff gesichert werden können.

10

Anhand des Datensatzes DS wird das erfindungsgemäße Verfahren zum Sichern von Werten von Fremdschlüsselattributen vor einem unberechtigten Zugriff näher beschrieben. Der Datensatz umfasst hier einen Primärschlüssel (Spalte ID), drei Attribute, die keine Primär- oder Fremdschlüsselattribute sind (Spalten x, y und z),
15 ein Fremdschlüsselattribut (Spalte IDB), mit dem ein Datensatz in der Relation B referenziert wird, und ein weiteres Fremdschlüsselattribut (Spalte IDC), mit dem ein Datensatz in der Relation C referenziert wird.

20

Das System, in dem dieser Datensatz und die Referenzen dieses Datensatzes auf die Relationen B und C für den Zugriff durch eine hier nicht gezeigte Anwendung gespeichert werden, umfasst einen flüchtigen Datenspeicher CUA und einen nicht-flüchtigen Datenspeicher bzw. permanenten Datenspeicher PM. Der flüchtige Datenspeicher CUA ist Bestandteil einer gesicherten und versiegelten Infrastruktur, mit der gewährleistet wird, dass kein unberechtigter Zugriff auf den flüchtigen Datenspeicher CUA möglich ist. Die gesicherte und versiegelte Infrastruktur kann eine
25 Anzahl redundanter und verteilter Rechnerressourcen umfassen, welche jeweils eine Anzahl sogenannter Trusted-Plattform-Module (TPM), Leistungsschalter zur Unterbrechung der Stromversorgung der gesamten Rechnerressourcen, elektromechanische Schlösser, eine Anzahl von Sensoren, mit denen der Zugang zu den
30 Rechnerressourcen überwacht werden kann, umfassen können.

In dem flüchtigen Datenspeicher CUA wird erfindungsgemäß eine Mapping-Relation TM gespeichert, wobei die Mapping-Relation TM eine Datenbanktabelle einer in dem flüchtigen Datenspeicher CUA gespeicherten Datenbank sein kann. Bei dieser Datenbank kann es sich beispielsweise um eine In-Memory-Datenbank handeln, die ihre Daten in dem flüchtigen Datenspeicher CUA speichert. Die in dem flüchtigen Datenspeicher CUA gespeicherten Daten können in einem weiteren hier nicht gezeigten flüchtigen Datenspeicher repliziert werden, wobei dieser weitere flüchtige Datenspeicher Bestandteil einer weiteren gesicherten und versiegelten Infrastruktur sein kann.

10

In dem flüchtigen Datenspeicher CUA können auch kryptografische Schlüssel gespeichert werden, die für das Verschlüsseln bzw. Entschlüsseln des Datensatzes DS vorgesehen sein können.

15 Gemäß der vorliegenden Erfindung wird jedenfalls die Mapping-Relation TM ausschließlich in dem flüchtigen Datenspeicher CUA gespeichert, sodass nach einer Unterbrechung der Stromversorgung die Mapping-Relation TM vollständig gelöscht wird. Sofern auch die kryptografischen Schlüssel in dem flüchtigen Datenspeicher CUA gespeichert sind, werden nach einer Stromunterbrechung auch diese
20 vollständig gelöscht. Das Löschen der Mapping-Relation TM kann etwa dann erforderlich sein, wenn sich jemand unberechtigt bzw. unbefugt Zutritt bzw. Zugang zu einer Rechnerressource verschafft, die Bestandteil der versiegelten Infrastruktur ist.

25 Um einen unberechtigten Zutritt zur versiegelten Infrastruktur feststellen zu können, ist es vorgesehen, dass die Rechnerressourcen der versiegelten Infrastruktur mit einer sogenannten Versiegelungsüberwachungseinrichtung (sealing control) verbunden sind, welche die elektromechanischen Komponenten überwacht. Stellt die Versiegelungsüberwachungseinrichtung einen unbefugten Zugang zu einer
30 Rechnerressource fest, kann sie die Stromversorgung zu der kompromittierten Rechnerressource und zu dem flüchtigen Datenspeicher CUA unterbrechen. Damit

ist gewährleistet, dass sich aus einer kompromittierten Rechnerressource und aus dem flüchtigen Datenspeicher CUA keinerlei Daten der Mapping-Relation TM herstellen lassen können und ein Zugriff auf die in dem flüchtigen Datenspeicher CUA gespeicherten kryptografischen Schlüssel verhindert wird. Die Versiegelungsüberwachungseinrichtung kann auch angepasst sein, um unberechtigte Zugriffe über ein Datennetz auf die versiegelte Infrastruktur zu erkennen. Auch in diesem Fall werden die kompromittierten Rechnerressourcen und der flüchtige Datenspeicher CUA von der Stromversorgung getrennt.

Erfindungsgemäß werden die Rechnerressourcen der versiegelten Infrastruktur und die flüchtigen Datenspeicher in der versiegelten Infrastruktur auch dann von der Stromversorgung unterbrochen, wenn an bzw. in der versiegelten Infrastruktur Wartungsarbeiten durchgeführt werden müssen. Damit ist gewährleistet, dass auch der Betreiber der versiegelten Infrastruktur bzw. der Betreiber der Datenbank in der die Mapping-Relation TM gespeichert wird, keinen Zugriff auf die Mapping-Relation TM erhält.

Ferner ist es erfindungsgemäß vorgesehen, dass eine Anwendung, beispielsweise eine Softwareanwendung, die auf die in der Mapping-Relation TM gespeicherten Daten zugreifen muss, ausschließlich in der versiegelten Infrastruktur ausgeführt wird. Damit kann bei entsprechend zertifizierten Anwendungen auch gewährleistet werden, dass die Anwendungen keine der in der Mapping-Relation TM gespeicherten Daten unbefugt nach außen geben können.

In dem permanenten bzw. nichtflüchtigen Datenspeicher PM werden die Nutzdaten bzw. Stammdaten des Datensatzes DS gespeichert, wobei für eine Speicherung dieser Daten ein Datenbankmanagementsystem vorgesehen sein kann. Um einen unberechtigten Zugriff auf die Fremdschlüsselattribute des Datensatzes DS in dem nichtflüchtigen Speicher PM zu verhindern, ist es vorgesehen, dass die Fremdschlüsselattribute ausschließlich in der Mapping-Relation TM in dem flüchtigen Speicher CUA gespeichert werden.

Ein zusätzliches Speichern dieser Fremdschlüsselattribute in dem nichtflüchtigen bzw. permanenten Speicher PM ist erfindungsgemäß lediglich dazu vorgesehen, um die Mapping-Relation TM in dem flüchtigen Datenspeicher CUA wieder her-
5 zustellen, falls der flüchtige Datenspeicher CUA beispielsweise aufgrund eines erkannten Kompromittierungsversuches von der Stromversorgung getrennt wurde. Mit zusätzlichen Sicherungsmaßnahmen, die nachfolgend näher beschrieben werden, ist allerdings gewährleistet, dass der Betreiber der in dem permanenten Speicher PM gespeicherten Datenbank keinen Zugriff auf die Werte dieser Fremd-
10 schlüsselattribute hat.

Bei dem in Fig. 1 gezeigten Beispiel einer Datenstruktur zum Sichern von Werten von Fremdschlüsselattributen eines Datensatzes vor einem unberechtigten Zugriff weist eine in dem nichtflüchtigen bzw. permanenten Speicher PM vorgesehene Da-
15 tenbank drei Relationen (Relation A, Relation B und Relation C) auf. Eine Relation wird umgangssprachlich auch als Tabelle bzw. Datenbanktabelle bezeichnet. In der Relation A ist der Datensatz DS gespeichert. Der in der Relation A gespeicherte Datensatz DS (Datensatz mit der ID = 1) weist einen Fremdschlüssel IDB mit dem Wert 2 und einen weiteren Fremdschlüssel IDC mit dem Wert 4 auf. Mit dem
20 Fremdschlüssel IDB wird die Relation B referenziert, wobei in dem vorliegenden Beispiel durch den Wert des Fremdschlüssels IDB der Datensatz mit der ID = 2 in Relation B referenziert wird. Mit dem zweiten Fremdschlüssel IDC wird die Relation C referenziert, wobei mit dem Wert 4 des Fremdschlüssels IDC der Datensatz mit der ID = 4 in der Relation C referenziert wird. Bei den Referenzen bzw. Ver-
25 knüpfungen zwischen den Relationen B und C und der Relation A handelt es sich um sogenannte 1:n-Verknüpfungen, wobei das erfindungsgemäße Verfahren bzw. die hierfür notwendigen Datenstrukturen auch für 1:1-Verknüpfungen bzw. n:m-Verknüpfungen anwendbar ist.

30 Zu dem in der Relation A gespeicherten Datensatz DS wird ein Mapping-Datensatz MDS in der Mapping-Relation TM gespeichert. Die Mapping-Relation TM weist

in dem in Fig. 1 gezeigten Beispiel sechs Attribute bzw. sechs Spalten auf. In einer Spalte RK1 wird eine erste Relationskennung gespeichert, wobei diese Relationskennung angibt, zu welcher Relation der Mapping-Datensatz MDS gehört. Mit dem Wert A wird beispielsweise angegeben, dass der Mapping-Datensatz MDS zur Relation A gehört.

In einer weiteren Spalte ist eine erste Spaltenkennung SK1 gespeichert, die angibt, welches Fremdschlüsselattribut der in der ersten Relationskennung RK1 angegebenen ersten Relation in dem Mapping-Datensatz MDS gespeichert ist.

In einer weiteren Spalte SK ist der Wert des durch die erste Spaltenkennung SK1 referenzierten Fremdschlüssels in der von der ersten Relationskennung RK1 referenzierten Relation gespeichert.

In einer weiteren Spalte PK ist der Wert des Primärschlüsselattributes des in der Relation A gespeicherten Datensatzes DS gespeichert.

Mit den Attributen RK1, SK1, SK und PK kann demnach ein Wert eines bestimmten Fremdschlüsselattributes eines bestimmten Datensatzes in einer bestimmten Relation identifiziert werden. Bei dem in Fig. 1 gezeigten Beispiel wird durch den ersten Mapping-Datensatz MDS der Wert des Fremdschlüsselattributes IDB des Datensatzes mit der ID = 1 in der Relation A identifiziert bzw. referenziert.

Durch das Vorsehen der ersten Relationskennung RK1 und der ersten Spaltenkennung SK1 in der Mapping-Relation TM können Werte von Fremdschlüsselattributen unterschiedlicher Relationen und Werte unterschiedlicher Fremdschlüsselattribute einer Relation in einer einzigen Mapping-Relation TM gespeichert werden. Weil die Mapping-Relation TM in dem nicht flüchtigen Speicher CUA gespeichert ist, beispielsweise als Datenbanktabelle einer In-Memory-Datenbank, kann die Zu-

griffszeit auf einen bestimmten Mapping-Datensatz MDS, insbesondere bei Vorsehen geeigneter Indexstrukturen, auch bei einer sehr großen Anzahl von Mapping-Datensätzen gering gehalten werden.

- 5 Der von dem ersten Mapping-Datensatz MDS in der Mapping-Relation TM referenzierte Datensatz in der Relation A ist durch den von der Mapping-Relation TM zur Relation A verlaufenden gestrichelten Pfeil angegeben. Der von dem Fremdschlüsselattribut in dem ersten Mapping-Datensatz MDS referenzierte Datensatz in der Relation B ist durch den von dem Fremdschlüsselattribut zur Relation B verlaufenden gestrichelten Pfeil dargestellt.
- 10

Eine in Fig. 1 nicht gezeigte Anwendung, die in der versiegelten Infrastruktur zur Ausführung gebracht wird und die auf den ersten Datensatz in der Relation A zugreifen möchte und hierbei die Fremdschlüssel der Fremdschlüsselattribute IDB und IDC auflösen möchte, beispielsweise durch einen sogenannten Join einer SQL-Abfrage, ermittelt die Werte der Fremdschlüsselattribute des ersten Datensatzes der Relation A in der Mapping-Relation TM, indem die Anwendung die diesen Fremdschlüsselattributen zugeordneten Mapping-Datensätze MDS in der Mapping-Relation TM ermittelt. In dem in Fig. 1 gezeigten Beispiel würde für den ersten Datensatz der Relation A für das Fremdschlüsselattribut IDB der ersten Mapping-Datensatz in der Mapping-Relation TM und für das Fremdschlüsselattribut IDC der vierte Mapping-Datensatz in der Relation TM ermittelt werden.

15

20

Mit den so ermittelten Mapping-Datensätzen stehen der Anwendung die Werte der Fremdschlüsselattribute IDB und IDC des ersten Datensatzes der Relation A zur Verfügung, sodass die Anwendung einen entsprechenden Join einer SQL-Anfrage erstellen kann. Damit können also Beziehungen zwischen Datensätzen mehrerer Relationen aufgelöst werden, ohne dass die Werte der Fremdschlüsselattribute in den Relationen selbst gespeichert werden müssen. Weil die Werte der Fremdschlüsselattribute eines Datensatzes nicht in den Relationen gespeichert werden müssen, ist gewährleistet, dass selbst wenn eine unberechtigte Person oder der Betreiber der

25

30

- in dem nichtflüchtigen Datenspeicher PM gespeicherten Datenbank Zugriff auf die in den Relationen gespeicherten Daten hat, diese keine Information über die Beziehungen zwischen den in den Relationen gespeicherten Datensätzen erhält. Damit ist ferner gewährleistet, dass aus den Beziehungen zwischen den in den Relationen gespeicherten Datensätzen keine Metainformationen abgeleitet bzw. gewonnen werden können, die beispielsweise Rückschlüsse auf das Verhalten oder Aktivitäten bestimmter Personen ermöglichen würden. Wären beispielsweise bei dem in Fig. 1 gezeigten Beispiel in der Relation A Benutzerdaten gespeichert, wobei in dem Fremdschlüsselattribut IDB ein dem jeweiligen Benutzer zugeordnetes Postfach gespeichert ist, könnte beispielsweise der Betreiber der Datenbank die Information erlangen, dass den Benutzern mit der ID 2 und 3 dasselbe Postfach (mit der ID = 3) zugeordnet ist, was den Betreiber der Datenbank nahelegen würde, dass diese Benutzer in irgendeiner Form in Kontakt stehen und gegebenenfalls über das ihnen zugeordnete Postfach Nachrichten austauschen. Ohne die Angabe der Fremdschlüsselattribute in den Datensätzen der Relation A erhält der Betreiber der Datenbank weder die Information, welches Postfach welchem Benutzer zugeordnet ist, noch kann er aus einer solchen Zuordnung irgendwelche Metainformationen oder Rückschlüsse ableiten.
- 20 In dem in Fig. 1 gezeigten Beispiel einer Datenstruktur sind die Fremdschlüsselattribute bzw. die Werte der Fremdschlüsselattribute IDB und IDC ebenfalls in der Relation A in dem nichtflüchtigen Datenspeicher PM gespeichert. Das Speichern der Werte der Fremdschlüsselattribute in den Relationen in dem nichtflüchtigen Datenspeicher PM ist ausschließlich dazu vorgesehen, um die Mapping-Relation
- 25 TM in dem flüchtigen Datenspeicher CUA gegebenenfalls wiederherstellen zu können, falls beispielsweise die Stromversorgung zu dem flüchtigen Datenspeicher CUA unterbrochen wurde. Das Wiederherstellen der Mapping-Relation TM in dem flüchtigen Datenspeicher CUA wird mit Bezug auf Fig. 4 näher beschrieben.
- 30 Um zu gewährleisten, dass der Betreiber der in dem nichtflüchtigen Datenspeicher gespeicherten Datenbank keinen Zugriff auf die Werte der Fremdschlüsselattribute

IDB und IDC hat, ist es erfindungsgemäß vorgesehen, dass zumindest die Werte der Fremdschlüsselattribute kryptografisch verschlüsselt sind, wobei für das Verschlüsseln der Fremdschlüsselattribute ausschließlich kryptografische Schlüssel der Besitzer der jeweiligen Datensätze verwendet werden. Damit ist gewährleistet, dass
5 auch der Betreiber der Datenbank die verschlüsselten Attribute eines Datensatzes nicht entschlüsseln kann.

Zusätzlich zu den Werten der Fremdschlüsselattribute können auch weitere Attribute, die keine Fremdschlüsselattribute oder Schlüsselattribute sind, kryptografisch
10 mit einem Verschlüsselungsschlüssel des jeweiligen Inhabers des Datensatzes verschlüsselt werden. In dem in Fig. 1 gezeigten Beispiel sind die kryptografisch verschlüsselten Attribute durch einen fetten Rahmen gekennzeichnet, wobei nicht nur Attribute der Relation A, die Fremdschlüsselattribute enthält, verschlüsselt sind, sondern auch Attribute der Relationen B und C.

15 Erfindungsgemäß nicht verschlüsselt sind hingegen die Werte der Primärschlüssel PK der jeweiligen Datensätze in den Relationen, weil aus diesen Werten ohnehin keinerlei Information abgeleitet werden kann. Ferner wird dadurch gewährleistet, dass für das Erzeugen eines Join einer SQL-Abfrage die Werte der Primärschlüsselattribute nicht erst entschlüsselt werden müssen, was einen erheblichen Geschwindigkeitsvorteil mit sich bringt.

Fig. 2 zeigt eine alternative Datenstruktur für das Sichern von Werten von Fremdschlüsselattributen eines Datensatzes vor einem unberechtigten Zugriff. Die Relationen A, B und C sind hier identisch zu dem in Fig. 1 gezeigten Beispiel einer
25 erfindungsgemäßen Datenstruktur, d.h. diese drei Relationen weisen dieselben Attribute und dieselben Attributswerte auf, wie in Fig. 1.

Die in Fig. 2 gezeigte erfindungsgemäße Datenstruktur unterscheidet sich von der in Fig. 1 gezeigten Datenstruktur in der Struktur der Mapping-Relation TM in dem
30 flüchtigen Datenspeicher CUA. Ein weiterer Unterschied liegt darin, dass bei dem

in Fig. 2 gezeigten Beispiel einer erfindungsgemäßen Datenstruktur für jede Relation in dem nichtflüchtigen Datenspeicher PM, die Fremdschlüsselattribute aufweist, in dem flüchtigen Datenspeicher CUA jeweils eine Mapping-Relation TM vorgesehen ist. Weisen beispielsweise drei Relationen in dem nichtflüchtigen Datenspeicher PM Fremdschlüsselattribute auf, so sind in dem flüchtigen Datenspeicher CUA ebenfalls drei Mapping-Relationen vorgesehen. Weil in dem in Fig. 2 gezeigten Beispiel in dem nichtflüchtigen Datenspeicher PM lediglich die Relation A Fremdschlüsselattribute (IDB und IDC) aufweist, ist in dem flüchtigen Datenspeicher CUA nur eine Mapping-Relation TM vorgesehen.

10

Im Unterschied zu der in Fig. 1 gezeigten Mapping-Relation, in der die Werte aller Fremdschlüsselattribute aller Relationen gespeichert sind, sind in einer Mapping-Relation gemäß Fig. 2 nur die Attributswerte der Fremdschlüsselattribute einer einzigen Relation gespeichert. Hierfür weist die Mapping-Relation TM drei Attribute bzw. Spalten auf. In einer ersten Spalte ist eine erste Spaltenkennung SK1 gespeichert, die angibt, auf welches Fremdschlüsselattribut sich der jeweilige Mapping-Datensatz MDS in der Mapping-Relation TM bezieht. Beispielsweise bezieht sich der erste Mapping-Datensatz MDS in der Mapping-Relation TM auf das Fremdschlüsselattribut IDB in der Relation A. Weil für jede Relation mit Fremdschlüsselattributen genau eine Mapping-Relation TM in dem flüchtigen Speicher CUA vorgesehen ist und weil bekannt ist, welche Mapping-Relation in dem flüchtigen Datenspeicher CUA welcher Relation in dem nichtflüchtigen Datenspeicher PM zugeordnet ist, kann in den Mapping-Relationen auf ein Attribut, das diese Zuordnung angibt, verzichtet werden.

25

In einer weiteren Spalte der Mapping-Relation TM wird der Wert des in der ersten Spaltenkennung SK1 angegebenen Fremdschlüsselattributs gespeichert. In einer dritten Spalte wird der Wert des Primärschlüsselattributs PK der Relation A gespeichert, sodass jedem Mapping-Datensatz MDS in der Mapping-Relation TM genau ein Datensatz in der Relation A zugeordnet ist. Über diese eindeutige Zuordnung

30

kann eine Applikation beispielsweise ermitteln, welchen Wert das Fremdschlüsselattribut IDB des Datensatzes mit dem Primärschlüssel PK = 1 hat.

5 Durch das Vorsehen der ersten Spaltenkennung SK1 kann in der Mapping-Relation TM für jeden Wert der Fremdschlüsselattribute der Relation A ein Mapping-Datensatz MDS gespeichert werden. Beispielsweise sind in den ersten drei Mapping-Datensätzen die Werte des Fremdschlüsselattributes IDB und in dem vierten Datensatz der Wert des Fremdschlüsselattributes IDC gespeichert.

10 Das Erzeugen eines Join für eine SQL-Abfrage erfolgt in der Weise, wie bereits mit Bezug auf Fig. 1 erläutert.

Fig. 3 zeigt eine weitere Alternative einer Datenstruktur zum Sichern von Werten von Fremdschlüsselattributen eines Datensatzes vor einem unberechtigten Zugriff.

15 Die in dem nichtflüchtigen Datenspeicher PM gespeicherten Relationen A, B und C sind hinsichtlich ihrer Struktur und ihres Inhalts identisch zu den in Fig. 1 und Fig. 2 gezeigten Relationen A, B und C.

Wie bei Fig. 2 ist auch bei dem Beispiel nach Fig. 3 in dem flüchtigen Datenspeicher CUA für jede Relation in dem nichtflüchtigen Datenspeicher PM, die Fremdschlüsselattribute aufweist, eine Mapping-Relation TM in dem flüchtigen Datenspeicher CUA vorgesehen. Im Unterschied zu dem in Fig. 2 gezeigten Beispiel sind allerdings bei dem in Fig. 3 gezeigten Beispiel einer Datenstruktur die Werte aller Fremdschlüsselattribute eines Datensatzes der Relation A in einem einzigen Mapping-Datensatz MDS in der Mapping-Relation TM gespeichert. Weil sämtliche Attributswerte der Fremdschlüsselattribute der Datensätze der Relation A in einem einzigen Mapping-Datensatz MDS gespeichert sind, kann bei der in Fig. 3 gezeigten Mapping-Relation TM auf die erste Spaltenkennung SK1 verzichtet werden.

30 Mit dem Primärschlüssel PK wird eine Zuordnung des Mapping-Datensatzes MDS zu einem Datensatz in der Relation A hergestellt. In weiteren Spalten SK1 und SK2

der Mapping-Relation TM sind die Werte der Fremdschlüsselattribute IDB und IDC für den jeweiligen durch den Fremdschlüssel PK identifizierten Datensatz der Relation A gespeichert. Die Anzahl der Spalten zum Speichern von Werten zu Fremdschlüsselattributen in der Mapping-Relation TM variiert demnach in Abhängigkeit von der Anzahl der der jeweiligen Mapping-Relation zugeordneten Relation in dem nichtflüchtigen Datenspeicher.

Mit **Fig. 4** wird anhand eines in der Relation A gespeicherten Datensatzes das erfindungsgemäße Verfahren zum Herstellen und/oder Wiederherstellen einer Mapping-Relation TM in dem flüchtigen Datenspeicher CUA näher erläutert.

Wie vorstehend mit Bezug auf Fig. 1 erläutert, können die in dem flüchtigen Datenspeicher CUA gespeicherten Mapping-Relationen TM in einen redundanten flüchtigen Datenspeicher repliziert werden, wobei der redundante flüchtige Datenspeicher entweder in derselben versiegelten Infrastruktur oder in einer anderen versiegelten Infrastruktur vorgesehen sein kann.

Für den Fall, dass der flüchtige Datenspeicher CUA beispielsweise im Falle einer Kompromittierung oder im Falle von Wartungsarbeiten von der Stromversorgung getrennt wird und damit sämtliche Daten in dem flüchtigen Datenspeicher CUA gelöscht werden, können die Mapping-Relationen aus dem redundanten flüchtigen Datenspeicher in den flüchtigen Datenspeicher CUA kopiert werden. Werden allerdings sämtliche flüchtigen Datenspeicher von der Stromversorgung getrennt, ist es notwendig, die Mapping-Relationen in den flüchtigen Datenspeicher und gegebenenfalls in den redundanten flüchtigen Datenspeichern aus den in dem permanenten Datenspeicher PM gespeicherten Relationen wiederherzustellen.

In Fig. 4 ist eine Relation A in dem nicht flüchtigen Datenspeicher PM gezeigt, die einen Datensatz aufweist, für den ein entsprechender Mapping-Datensatz in der Mapping-Relation TM wiederhergestellt werden soll.

Der Datensatz in der Relation A weist einen Primärschlüssel ID, zwei Fremdschlüsselattribute IDB und IDC und drei Attribute x, y und z, die keine Fremdschlüsselattribute und keine Schlüsselattribute sind, auf. In dem in Fig. 4 gezeigten Beispiel sind die Fremdschlüsselattribute und die Nichtschlüsselattribute mit einem kryptografischen Schlüssel des Besitzers des Datensatzes verschlüsselt worden. Erfindungsgemäß ist es aber nur notwendig, dass die Werte der Fremdschlüsselattribute mit dem Schlüssel des Besitzers des Datensatzes kryptografisch verschlüsselt sind.

In einem ersten Schritt S1 wird der Datensatz der Relation A in den flüchtigen Datenspeicher CUA der versiegelten Infrastruktur kopiert. Dies ist notwendig, weil für das Herstellen bzw. Wiederherstellen der Mapping-Relation der Datensatz, jedenfalls aber die Werte der Fremdschlüsselattribute des Datensatzes entschlüsselt werden müssen, wobei das Entschlüsseln des Datensatzes in der gesicherten und versiegelten Infrastruktur vorgenommen wird. Dadurch ist gewährleistet, dass die Werte der Fremdschlüsselattribute ausschließlich im flüchtigen Datenspeicher CUA der versiegelten Infrastruktur in unverschlüsselter Form vorliegen. Würde die versiegelte Infrastruktur bzw. der flüchtige Datenspeicher CUA während eines Wiederherstellungsvorganges der Mapping-Relation TM kompromittiert werden, würden auch die unverschlüsselten Werte der Fremdschlüsselattribute unverzüglich gelöscht werden.

In einem weiteren Schritt S2 wird der in den flüchtigen Datenspeicher CUA kopierte Datensatz entschlüsselt, wobei für das Entschlüsseln des Datensatzes der dem Besitzer des Datensatzes zugeordnete kryptografische Schlüssel (Entschlüsselungsschlüssel) verwendet wird. Wichtig ist hierbei, dass der dem Besitzer des Datensatzes zugeordnete kryptografische Schlüssel zum Entschlüsseln des Datensatzes ausschließlich in der versiegelten Infrastruktur bzw. in dem flüchtigen Datenspeicher CUA gespeichert ist.

Weil der kryptografische Schlüssel zum Entschlüsseln des Datensatzes nur von dem Besitzer des kryptografischen Schlüssels verwendet werden kann (weil der Besitzer

des kryptografischen Schlüssels beispielsweise für die Verwendung des Schlüssels ein Passwort eingeben muss), kann der Datensatz in dem flüchtigen Datenspeicher CUA auch nur dann entschlüsselt werden, wenn der Besitzer des Datensatzes an dem System angemeldet ist. Der Betreiber der versiegelten Infrastruktur bzw. der Betreiber der in dem nichtflüchtigen Datenspeicher PM gespeicherten Datenbank kann demnach ohne Hilfe der Besitzer der in den jeweiligen Relationen gespeicherten Datensätze die Mapping-Relationen in dem flüchtigen Datenspeicher CUA nicht herstellen, weil weder der Betreiber der versiegelten Infrastruktur noch der Betreiber der Datenbank die hierfür notwendigen kryptografischen Schlüssel der Besitzer der Datensätze verwenden kann. Demnach kann weder der Betreiber der versiegelten Infrastruktur noch der Betreiber der Datenbank beispielsweise in einem Batch-Job die gesamten Mapping-Relationen wieder herstellen. Das Wiederherstellen der Mapping-Relationen in dem flüchtigen Datenspeicher CUA kann nur sukzessive erfolgen, indem jeweils für jene Datensätze in der Datenbank die Mapping-Datensätze in den Mapping-Relationen wieder hergestellt werden, die einem eingeloggten bzw. sich dem System gegenüber authentifizierten Besitzer bzw. Nutzer zugeordnet sind.

Nach dem Schritt S2 liegt der Datensatz in dem flüchtigen Speicher CUA in unverschlüsselter Form vor. In einem nächsten Schritt S3 werden aus dem entschlüsselten Datensatz jene Werte extrahiert, die für das Erzeugen eines entsprechenden Mapping-Datensatzes in der Mapping-Relation TM benötigt werden. Bei dem in Fig. 4 gezeigten Beispiel sind dies die Werte des Primärschlüssels ID und die Werte der Fremdschlüsselattribute IDB und IDC. Weist die wiederherzustellende Mapping-Relation TM die in Fig. 1 oder Fig. 2 gezeigte Datenstruktur auf, müssen die hierfür erforderlichen zusätzlichen Attributswerte in dem Schritt S3 ebenfalls ermittelt werden. Beispielsweise wäre es bei der in Fig. 4 gezeigten Datenstruktur notwendig, dass in dem Schritt S3 auch die erste Spaltenkennung SK1 ermittelt wird, um einen entsprechenden Mapping-Datensatz in die in Fig. 2 gezeigte Mapping-Relation einfügen zu können.

Nachdem die für den in die Mapping-Relation einzufügenden Mapping-Datensatz erforderlichen Attributswerte ermittelt worden sind, werden die Attribute bzw. wird der so gebildete Mapping-Datensatz MDS in die Mapping-Relation TM in dem Schritt S4 eingefügt. Anschließend können sämtliche nicht mehr benötigte Daten, beispielsweise der entschlüsselte Datensatz in dem flüchtigen Datenspeicher CUA gelöscht werden.

Die Schritte S1 bis S4 werden für jeden Datensatz in sämtlichen Relationen, die Fremdschlüsselattribute aufweisen, wiederholt.

10

Vor dem Kopieren des Datensatzes in den flüchtigen Datenspeicher CUA in dem Schritt S1 oder vor dem Entschlüsseln des in den flüchtigen Datenspeicher kopierten Datensatzes in dem Schritt S2 kann geprüft werden, ob für diesen Datensatz bereits ein Mapping-Datensatz in der entsprechenden Mapping-Relation TM vorhanden ist. Ist kein entsprechender Mapping-Datensatz vorhanden, wird das Wiederherstellungsverfahren fortgesetzt. Anderenfalls kann das Wiederherstellungsverfahren abgebrochen werden.

Nachdem sämtliche Mapping-Relationen in dem flüchtigen Datenspeicher CUA wieder hergestellt worden sind, kann es vorteilhaft sein, die in dem flüchtigen Datenspeicher CUA vorhandenen Mapping-Relationen in einen oder mehrere redundante flüchtige Datenspeicher zu kopieren.

Die Schritte S1 bis S4 kommen auch zur Ausführung, wenn in einer Relation in dem nichtflüchtigen Datenspeicher PM ein neuer Datensatz hinzugefügt wird. Für diesen neu hinzugefügten Datensatz muss ebenfalls ein Mapping-Datensatz in der entsprechenden Mapping-Relation angelegt werden, damit auch die Werte der Fremdschlüsselattribute des neuen Datensatzes vor einem unberechtigten Zugriff gesichert sind.

30

Ändert sich ein Wert eines Fremdschlüsselattributes eines Datensatzes in dem nichtflüchtigen Speicher PM, so muss der geänderte Wert des Fremdschlüsselattributes auch in dem entsprechenden Mapping-Datensatz geändert werden. Hierfür können die Verfahrensschritte S1 bis S3 in identischer Weise wie beim Wiederherstellen der Mapping-Relation ausgeführt werden. In dem Schritt S4 wird allerdings
5 anstelle einer Einfüge-Operation eine Update-Operation durchgeführt, mit der ein bestehender Mapping-Datensatz durch den in dem Schritt S3 erzeugten Mapping-Datensatz ersetzt wird. Vorzugsweise ist es vorgesehen, dass nur dann eine solche Aktualisierung von Mapping-Datensätzen durchgeführt wird, wenn sich in einem
10 Datensatz auch ein Wert eines Fremdschlüsselattributes geändert hat. Ändert sich hingegen nur ein Wert eines Nicht-Schlüsselattributes wird keine Aktualisierung der Mapping-Relationen durchgeführt.

Die vorliegende Erfindung erlaubt es also, Werte von Fremdschlüsselattributen von
15 Datensätzen, die in einer Datenbank speicherbar sind, effektiv und effizient vor einem unberechtigten Zugriff zu sichern, indem die Werte der Fremdschlüsselattribute der Datensätze ausschließlich in einem flüchtigen Datenspeicher gespeichert werden, wobei dieser flüchtige Datenspeicher Bestandteil einer gesicherten und versiegelten Infrastruktur ist. Für das Auflösen von Fremdschlüsselattributen eines
20 Datensatzes muss eine Applikation auf den flüchtigen Datenspeicher in der versiegelten Infrastruktur zugreifen, wobei auch die Applikation in der versiegelten Infrastruktur ausgeführt wird, sodass gewährleistet werden kann, dass auch diese Applikation keine Informationen über die Werte der Fremdschlüsselattribute nach außen geben kann. Lediglich für das Wiederherstellen der in dem flüchtigen Speicher
25 gespeicherten Mapping-Relationen sind die Werte der Fremdschlüsselattribute zusätzlich in den Datensätzen gespeichert, wobei die Mapping-Relationen nur dann aus den Datensätzen hergestellt werden müssen, wenn neben dem flüchtigen Datenspeicher auch sämtliche redundanten flüchtigen Datenspeicher gelöscht wurden.

30 Um zu gewährleisten, dass auf die in den Datensätzen gespeicherten Werte der Fremdschlüsselattribute kein unberechtigter Zugriff erfolgen kann, sind zumindest

die Werte der Fremdschlüsselattribute mit einem kryptografischen Schlüssel verschlüsselt, der dem Besitzer des Datensatzes gehört bzw. zugeordnet ist. Damit kann auch der Betreiber der Datenbank nicht auf die Werte der Fremdschlüsselattribute in den Datensätzen zugreifen.

Bezugszeichen:

	CUA	flüchtiger Datenspeicher (Clean-Up Area)
5	CUA2	redundanter flüchtiger Datenspeicher
	DS	Datensatz in der ersten bzw. zweiten Relation T1, T2
	F	Attribute der ersten bzw. zweiten Relation T1, T2, die keine Fremdschlüsselattribute sind
	FK, FK1, FK2	Fremdschlüsselattribute
10	K	Schlüssel des Datensatzes DS (z.B. Primärschlüssel oder zusammengesetzter Primärschlüssel)
	MDS	Mapping-Datensatz in der Mapping-Relation TM
	PK	Primärschlüsselattribut der ersten bzw. zweiten Relation T1, T2
	PM	nichtflüchtiger bzw. permanenter Datenspeicher
15	RK1	erste Relationskennung in der Mapping-Relation TM
	RK2	zweite Relationskennung in der Mapping-Relation TM
	S1 bis S4	Schritte des Wiederherstellungsverfahrens
	SK1	erste Spaltenkennung in der Mapping-Relation TM
	SK2	zweite Spaltenkennung in der Mapping-Relation TM
20	T1	erste Relation (Datenbanktabelle) einer Datenbank in dem nichtflüchtigen Datenspeicher PM
	T2	zweite Relation (Datenbanktabelle) einer Datenbank in dem nichtflüchtigen Datenspeicher PM
	TM	Mapping-Relation (Datenbanktabelle) einer Datenbank in dem
25		flüchtigen Datenspeicher CUA

Ansprüche

5

1. Verfahren zum Sichern von Werten von Attributen eines Datensatzes (DS), der in einer ersten Relation (T1) einer Datenbank speicherbar ist, vor einem unberechtigten Zugriff, wobei ein Wert eines Fremdschlüsselattributs (FK) des Datensatzes auf einen Schlüssel (K) der ersten Relation (T1) oder einer zweiten Relation (T2) verweist, und wobei

10

- der Wert des Fremdschlüsselattributs (FK) in einer Mapping-Relation (TM) gespeichert wird,
- die Werte einer Anzahl von Attributen (F), die keine Fremdschlüsselattribute sind, des Datensatzes in der ersten Relation (T1) gespeichert werden, und
- die Mapping-Relation (TM) in einem flüchtigen Datenspeicher (CUA) gespeichert wird.

15

2. Verfahren nach dem vorhergehenden Anspruch, wobei die erste Relation (T1) in einem nichtflüchtigen Datenspeicher (PM) gespeichert wird.

20

3. Verfahren nach einem der vorhergehenden Ansprüche, wobei in der Mapping-Relation (TM) zusätzlich zum Wert des Fremdschlüsselattributs (FK) der Wert eines Primärschlüsselattributs (PK) des Datensatzes (DS) gespeichert wird, wobei der Wert des Fremdschlüsselattributs (FK) und der Wert des Primärschlüsselattributs (PK) des Datensatzes (DS) einen Mapping-Datensatz (MDS) in der Mapping-Relation (TM) bilden.

25

4. Verfahren nach dem vorhergehenden Anspruch, wobei das Primärschlüsselattribut (PK) des Datensatzes (DS) aus einer Anzahl von Schlüsselattributen des Datensatzes (DS) gebildet wird.
5. Verfahren nach einem der vorhergehenden Ansprüche, wobei bei mehreren ersten Relationen (T1), in denen Datensätze (DS) speicherbar sind, die Werte von Fremdschlüsselattributen umfassen, in der Mapping-Relation (TM) zu jedem Mapping-Datensatz (MDS) zusätzlich gespeichert werden:
 - eine erste Relationskennung (RK1), die eine Information darüber umfasst, zu welcher ersten Relation (T1) der mehreren ersten Relationen der jeweilige Mapping-Datensatz (MDS) zugeordnet ist, und
 - eine erste Spaltenkennung (SK1), die eine Information darüber umfasst, zu welchem Fremdschlüsselattribut (FK) des Datensatzes (DS) der in dem jeweiligen Mapping-Datensatz (MDS) gespeicherte Wert des Fremdschlüsselattributs zugeordnet ist.
6. Verfahren nach einem der Ansprüche 1 bis 4, wobei bei mehreren ersten Relationen (T1), in denen Datensätze (DS) speicherbar sind, die Werte von Fremdschlüsselattributen umfassen, für jede der ersten Relationen (T1) in dem flüchtigen Datenspeicher (CUA) eine Mapping-Relation (TM) erzeugt wird, in der die Werte der Fremdschlüsselattribute (FK) der jeweiligen Datensätze (DS) gespeichert werden, wobei zusätzlich zum Wert des Fremdschlüsselattributs (FK) der Wert eines Primärschlüsselattributs (PK) des jeweiligen Datensatzes (DS) gespeichert wird.
7. Verfahren nach dem vorhergehenden Anspruch, wobei in der Mapping-Relation (TM) zu jedem Mapping-Datensatz (MDS) zusätzlich eine erste Spaltenkennung (SK1) gespeichert wird, die eine Information darüber umfasst, zu welchem Fremdschlüsselattribut (FK) des Datensatzes (DS) der in

dem jeweiligen Mapping-Datensatz (MDS) gespeicherte Wert des Fremdschlüsselattributs zugeordnet ist.

8. Verfahren nach einem der vorhergehenden Ansprüche 5 bis 7, wobei in der Mapping-Relation (TM) zu jedem Mapping-Datensatz (MDS) zusätzlich gespeichert werden:
 - eine zweite Relationskennung (RK2), die eine Information darüber umfasst, welche zweite Relation (T2) von mehreren zweiten Relationen von dem Wert des Fremdschlüsselattributs des Mapping-Datensatzes (MDS) referenziert wird, und
 - eine zweite Spaltenkennung (SK2), die eine Information darüber umfasst, welcher Schlüssel (K) von dem Wert des Fremdschlüsselattributs des Mapping-Datensatzes (MDS) in der zweiten Relation (T2) referenziert wird.
9. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Wert des Fremdschlüsselattributs (FK) des Datensatzes (DS) zusätzlich in der ersten Relation (T1) gespeichert wird, wobei der in der ersten Relation (T1) gespeicherte Wert des Fremdschlüsselattributs (FK) des Datensatzes (DS) kryptographisch verschlüsselt wird, vorzugsweise mit einem dem Besitzer des Datensatzes zugeordneten kryptographischen Schlüssel.
10. Verfahren nach dem vorhergehenden Anspruch, wobei zusätzlich zu dem Wert des Fremdschlüsselattributs (FK) ein Wert mindestens eines weiteren Attributs (F), das kein Fremdschlüsselattribut ist, des Datensatzes (DS) kryptographisch verschlüsselt wird.
11. Verfahren nach dem vorhergehenden Anspruch, wobei beim Erzeugen eines neuen Datensatzes (DS) zumindest die Werte der Fremdschlüsselattribute (FK) des neuen Datensatzes (DS) und die Werte der Primärschlüsselattribute (PK) des neuen Datensatzes (DS) in den Mapping-Relationen (TM)

gespeichert werden, und zumindest die Werte der Fremdschlüsselattribute (FK) in der ersten Relation (T1) kryptographisch verschlüsselt werden.

12. Verfahren nach dem vorhergehenden Anspruch, wobei die Mapping-Relationen (TM) zusätzlich in einem redundanten flüchtigen Datenspeicher (CUA2) gespeichert werden.
5
13. Verfahren zum Herstellen und/oder Wiederherstellen einer Mapping-Relation (TM) in einem flüchtigen Datenspeicher (CUA), wobei in der Mapping-Relation Werte von Fremdschlüsselattributen (FK) eines Datensatzes, der
10 in einer ersten Relation (T1) einer Datenbank gespeichert ist, speicherbar sind, wobei zumindest die Werte der Fremdschlüsselattribute (FK) in der ersten Relation (T1) kryptographisch verschlüsselt sind und vorzugsweise ausschließlich mit einem kryptographischen Schlüssel des Besitzers des Datensatzes entschlüsselbar sind, wobei
15
 - bei einem Zugriff des Besitzers des Datensatzes auf den Datensatz die Werte der verschlüsselten Fremdschlüsselattribute (FK) mit dem kryptographischen Schlüssel des Besitzers des Datensatzes entschlüsselt werden,
 - 20 - die entschlüsselten Werte der Fremdschlüsselattribute (FK) in einem Mapping-Datensatz (MDS) der Mapping-Relation (TM) gespeichert werden, und
 - zusätzlich zu den Werten der Fremdschlüsselattribute (FK) in dem Mapping-Datensatz (MDS) der Wert eines Primärschlüsselattributs (PK) des
25 Datensatzes gespeichert wird.
14. Verfahren nach dem vorhergehenden Anspruch, wobei vor dem entschlüsseln der verschlüsselten Fremdschlüsselattribute (FK) geprüft wird, ob für den Wert des Primärschlüsselattributs (PK) des Datensatzes bereits ein
30 Mapping-Datensatz (MDS) in der Mapping-Relation (TM) gespeichert ist.

15. Verfahren nach einem der beiden vorhergehenden Ansprüche, wobei in dem Mapping-Datensatz (MDS) zusätzlich gespeichert werden:
- eine erste Spaltenkennung (SK1), die eine Information darüber umfasst, welchem Fremdschlüsselattribut (FK) des Datensatzes der in dem Mapping-Datensatz (MDS) gespeicherte Wert des Fremdschlüsselattributs zugeordnet ist, und
 - vorzugsweise zusätzlich:
 - eine erste Relationskennung (RK1), die eine Information darüber umfasst, welcher ersten Relation (T1) von mehreren ersten Relationen der Mapping-Datensatz (MDS) zugeordnet ist, und/oder
 - eine zweite Relationskennung (RK2), die eine Information darüber umfasst, welche zweite Relation (T2) von mehreren zweiten Relationen von dem Wert des Fremdschlüsselattributs des Mapping-Datensatzes (MDS) referenziert wird, und/oder
 - eine zweite Spaltenkennung (SK2), die eine Information darüber umfasst, welcher Schlüssel (K) von dem Wert des Fremdschlüsselattributs des Mapping-Datensatzes (MDS) in der zweiten Relation (T2) referenziert wird.
16. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Mapping-Relationen (TM) in einer gesicherten und versiegelten Infrastruktur gespeichert werden und/oder die Werte der verschlüsselten Fremdschlüsselattribute (FK) in einer gesicherten und versiegelten Infrastruktur entschlüsselt werden, wobei die hierfür notwendigen kryptographischen Schlüssel ausschließlich in der gesicherten und versiegelten Infrastruktur gespeichert sind.
17. Verfahren nach dem vorhergehenden Anspruch, wobei eine Anwendung zum Zugriff auf die Daten der Mapping-Relationen (TM) in der gesicherten und versiegelten Infrastruktur ausgeführt wird.

18. System zum Sichern von Werten von Fremdschlüsselattributen eines Datensatzes (DS), der in einer ersten Relation (T1) einer Datenbank speicherbar ist, vor einem unberechtigten Zugriff, wobei ein Wert eines Fremdschlüsselattributs (FK) des Datensatzes auf einen Schlüssel (K) der ersten Relation (T1) oder einer zweiten Relation (T2) verweist, wobei das System einen flüchtigen Datenspeicher (CUA) und einen nichtflüchtigen Datenspeicher (PM) umfasst, und wobei das System angepasst ist
- 5
- den Wert des Fremdschlüsselattributs (FK) in einer Mapping-Relation (TM), die in dem flüchtigen Datenspeicher (CUA) gespeichert ist, zu speichern, und
 - 10 - die Werte der Attribute (F), die keine Fremdschlüsselattribute sind, des Datensatzes in der ersten Relation (T1), die in dem nichtflüchtigen Datenspeicher (PM) gespeichert ist, zu speichern.
- 15 19. System nach Anspruch 18, wobei der flüchtige Speicher (CUA) und der nichtflüchtige Speicher (PM) jeweils von einem Serversystem bereitgestellt werden, die physikalisch voneinander getrennt sind.
20. System nach einem der beiden vorhergehenden Ansprüche, wobei das System weiter angepasst ist, das Verfahren nach einem der Ansprüche 2 bis 16 auszuführen.
- 20
21. Computerprogrammprodukt, das in den internen Speicher eines Rechnersystems geladen werden kann und das Programmabschnitte umfasst, mit denen die Schritte der Verfahrens gemäß einem der Ansprüche 1 bis 17 ausgeführt werden, wenn das Computerprogrammprodukt auf dem Rechnersystem zu Ausführung gebracht wird.
- 25

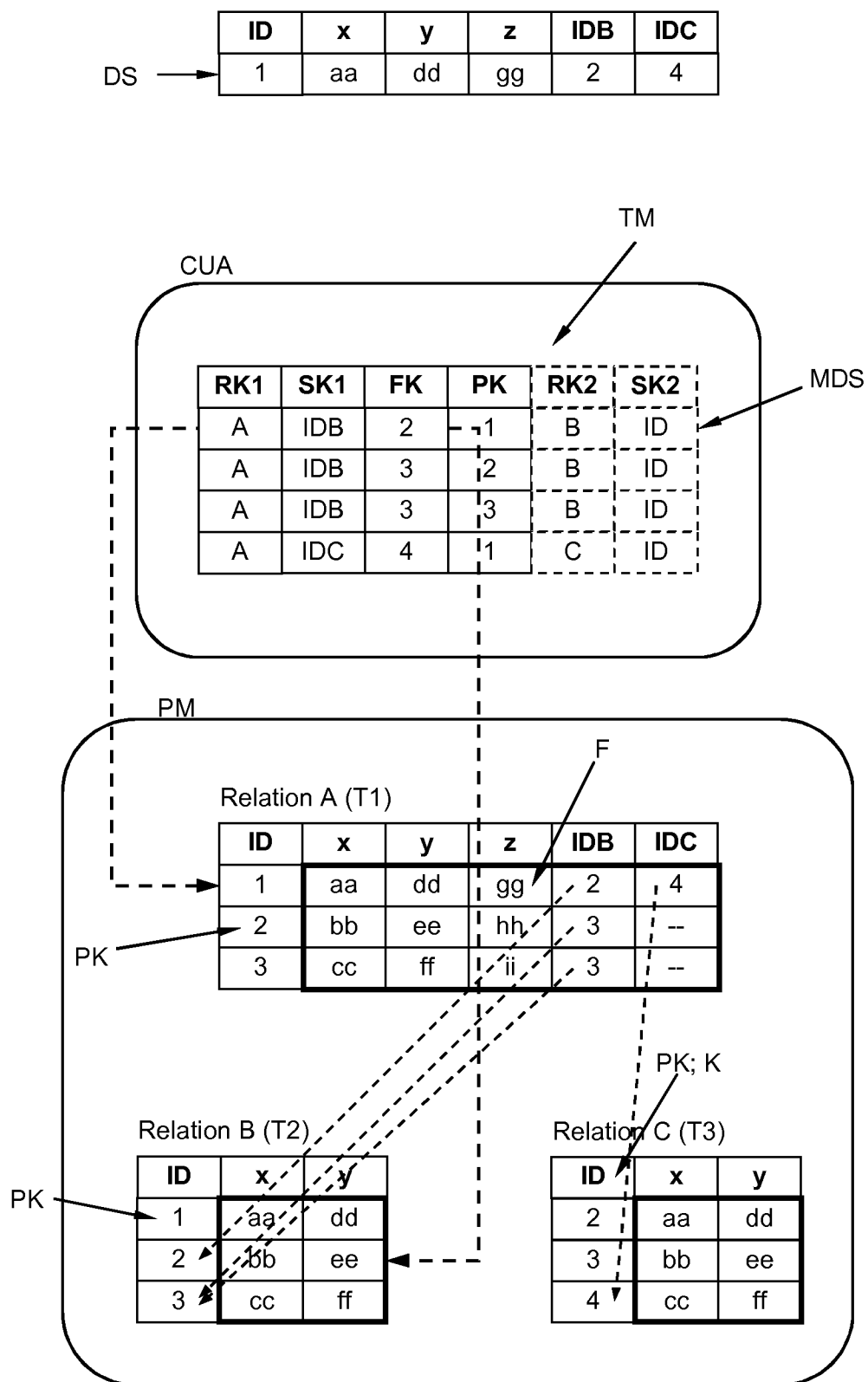


Fig. 1

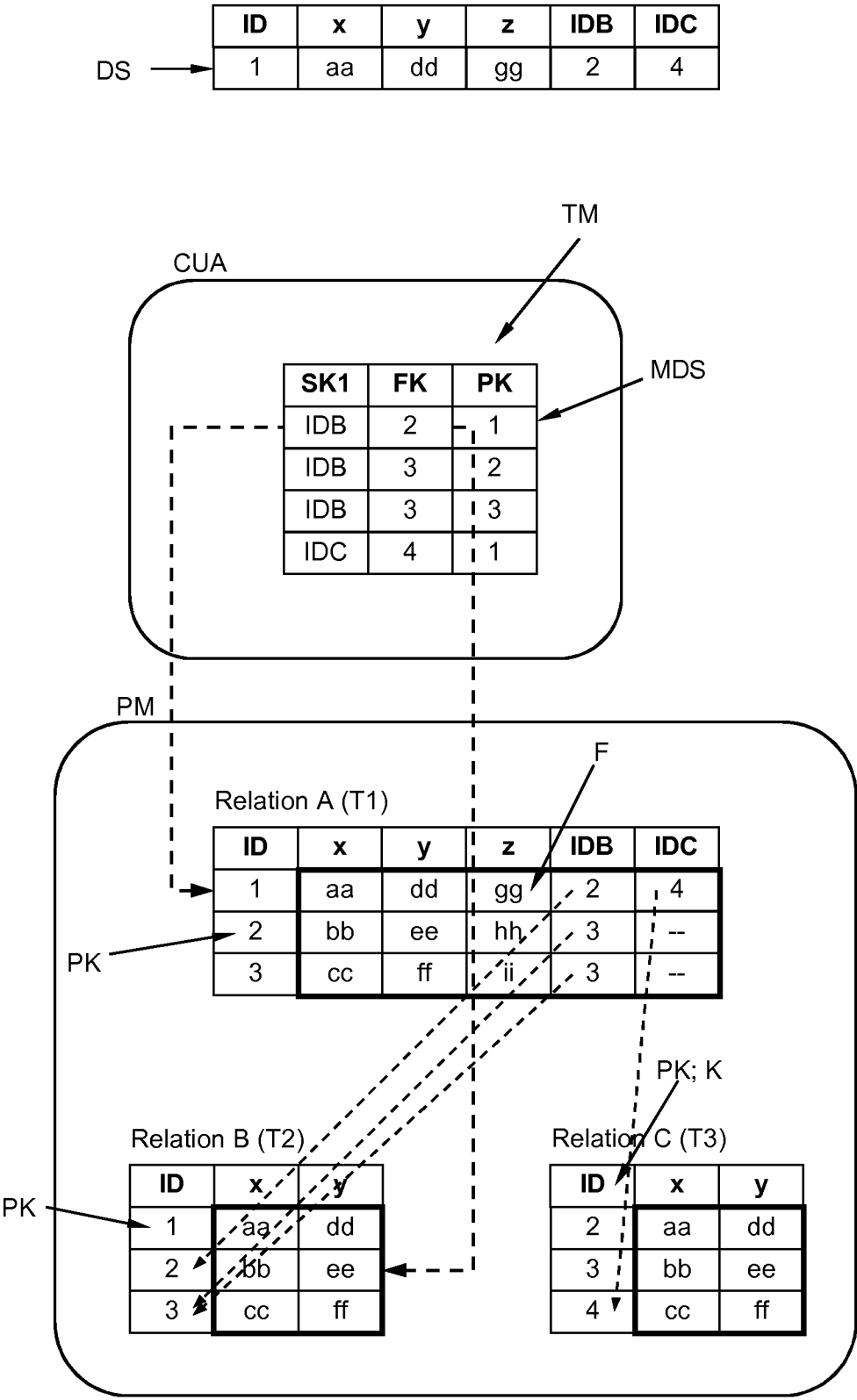


Fig. 2

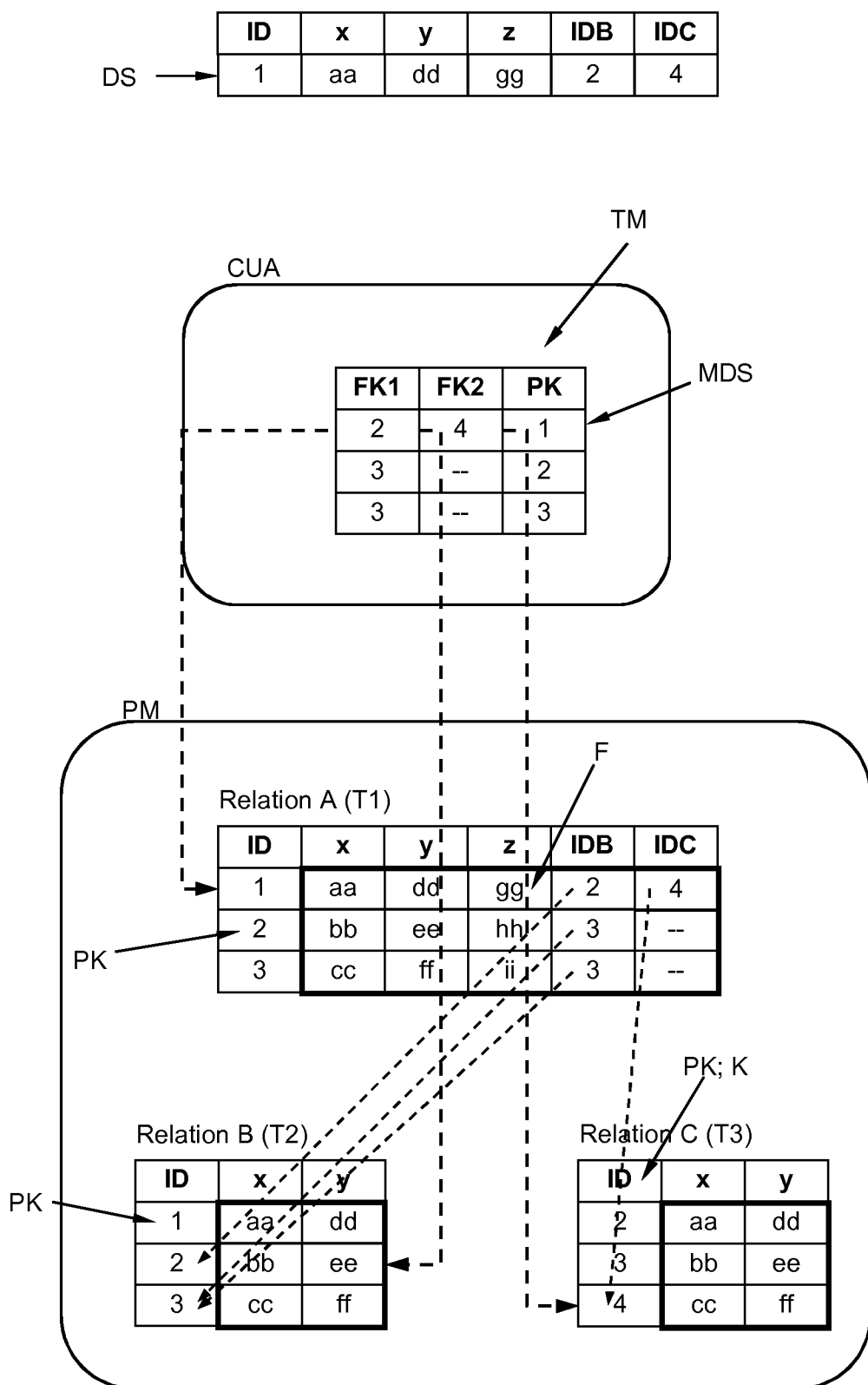


Fig. 3

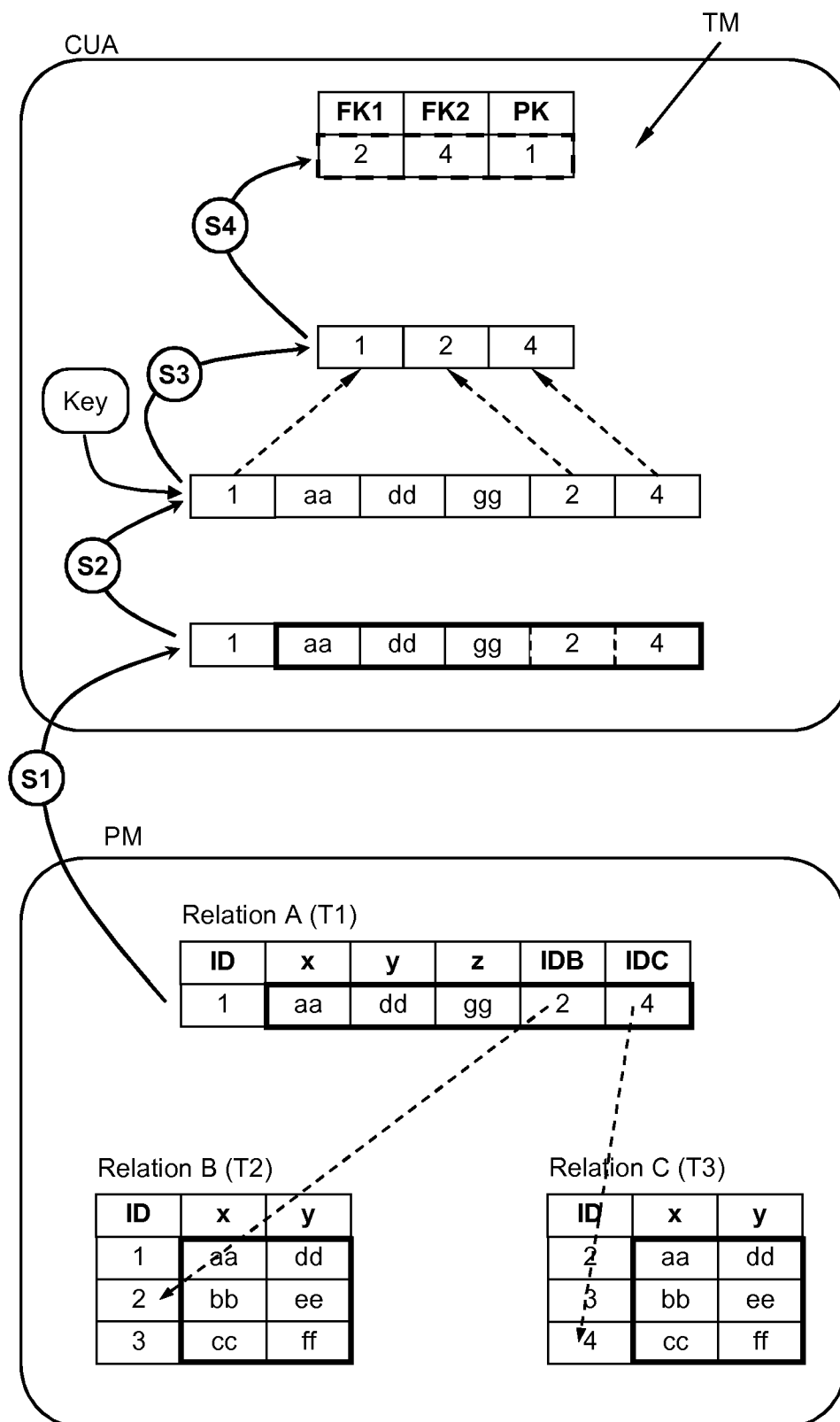


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2015/052959

A. CLASSIFICATION OF SUBJECT MATTER
 INV. G06F21/62
 ADD.

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)
 G06F

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 practicable, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	LUC BOUGANIM ET AL: "Chip-Secured Data Access: Confidential Data on Untrusted Servers", PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON VERY LARGEDATA BASES, XX, XX, 1 January 2002 (2002-01-01), pages 1-12, XP002427422, paragraph [04.2]; figure 3	1-21
A	DE 199 25 910 A1 (SIEMENS AG [DE]) 22 February 2001 (2001-02-22) abstract	1-21
A	DE 10 2006 012311 A1 (DEUTSCHE TELEKOM AG [DE]) 20 September 2007 (2007-09-20) abstract	1-21



Further documents are listed in the continuation of Box C.



See patent family 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 application or patent 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

14 April 2015

Date of mailing of the international search report

22/04/2015

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040,
 Fax: (+31-70) 340-3016

Authorized officer

Mezödi, Stephan

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2015/052959

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19925910 A1	22-02-2001	DE 19925910 A1	22-02-2001
		JP 2001034538 A	09-02-2001
		US 6789195 B1	07-09-2004

DE 102006012311 A1	20-09-2007	DE 102006012311 A1	20-09-2007
		EP 2013811 A1	14-01-2009
		US 2009265788 A1	22-10-2009
		WO 2007110035 A1	04-10-2007

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F21/62
ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F

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

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	LUC BOUGANIM ET AL: "Chip-Secured Data Access: Confidential Data on Untrusted Servers", PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON VERY LARGEDATA BASES, XX, XX, 1. Januar 2002 (2002-01-01), Seiten 1-12, XP002427422, Absatz [04.2]; Abbildung 3 -----	1-21
A	DE 199 25 910 A1 (SIEMENS AG [DE]) 22. Februar 2001 (2001-02-22) Zusammenfassung -----	1-21
A	DE 10 2006 012311 A1 (DEUTSCHE TELEKOM AG [DE]) 20. September 2007 (2007-09-20) Zusammenfassung -----	1-21



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



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" frühere Anmeldung oder Patent, die bzw. 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 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

14. April 2015

Absendedatum des internationalen Recherchenberichts

22/04/2015

Name und Postanschrift der Internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Mezödi, Stephan

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2015/052959

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 19925910 A1	22-02-2001	DE 19925910 A1	22-02-2001
		JP 2001034538 A	09-02-2001
		US 6789195 B1	07-09-2004

DE 102006012311 A1	20-09-2007	DE 102006012311 A1	20-09-2007
		EP 2013811 A1	14-01-2009
		US 2009265788 A1	22-10-2009
		WO 2007110035 A1	04-10-2007
