This document includes some recent decisions of the EPO in 2015 with regards to software related inventions and shows relevant extracts from the respective decisions.

T0039/11 (Data access control/NTT DOCOMO) of 17.10.2014

European Case Law Identifier: ECLI:EP:BA:2014:T003911.20141017

COMMUNICATION DEVICE

Keywords: Inventive step - (no)

Application number: 03723394.7
IPC class: G06F 12/14, G06F 9/44, H04B 7/26, H04M 1/00, H04M 1/725
Applicant name: NTT DoCoMo, Inc.
Cited decisions: T 0641/00

Board: 3.5.01

http://www.epo.org/law-practice/case-law-appeals/pdf/t110039eu1.pdf

1. The invention

1.1 The invention concerns the protection of sensitive data, such as the user's address book and telephone numbers, stored in a mobile phone. It would be a security risk if this information were freely accessible to downloaded Java applications (apps) that could try to steal data.

1.2 The invention seeks to overcome this by providing the phone data in an encapsulated object. In this way, downloaded apps may not access the data directly, but may only interact with encapsulated data via the public methods provided in the object. The invention uses two types of encapsulated object: "perfect encapsulated objects" and "imperfect encapsulated objects". The type of encapsulation depends on the type of data to be encapsulated. For example, the address book is particularly sensitive, and, therefore, is provided in a "perfect encapsulated object".

Claim 1 of the main request reads:

"A communication device comprising:

a receiving means for receiving a program in byte code;

a specifying means adapted to specify data to be used from among data stored in the communication device when a program received by said receiving means is executed;

a first generation means for generating, when the received program is to be executed, a perfect encapsulated object having a method which is for processing encapsulated data from an outside object, the object having the encapsulated data specified by said specifying means, and which is adapted to deny access to said encapsulated data by said executed program received by said receiving means, wherein the generation means is for generating a perfect encapsulated object or an imperfect encapsulated object depending on a type designation information associated with the specified data, said perfect encapsulated object not having a method for authorizing access to encapsulated data by an executed program;

an access control means for restricting accessible resources, and prohibiting access to data specified by said specifying means from among data stored in the communication device."

2.9 .. the distinguishing features of the invention are directed to providing more or less access to encapsulated data, depending on the type of data. This is essentially the Examining Division's reasoning in the decision under appeal.

2.10 **In the Board's view, the aim of protecting sensitive information is not technical**, and may legitimately appear in the formulation of the technical problem (T 641/00 - "Two identities/Comvik", OJ EPO 2003, 352). Therefore, the Board considers that the **problem solved by the invention is controlling access to data stored in the communication device, in the light of the non-technical requirement of protecting sensitive data**.

2.11 The skilled person, who is a Java programmer, would inevitably have had to consider how to define her objects/classes, including which forms of access to give to encapsulated data, i. e. which accessor methods to provide, depending on the desired functionality and degree of protection. If "get"-access to a particular type of data is not desired for security reasons, the Board's opinion is that it would be self-evident to exclude methods such as getByte().

2.12 The appellant argued that the purpose of using encapsulation in object-oriented programming was different from that achieved by the invention. According to the appellant, the motivation behind encapsulation was normally to protect code from accidental corruption, and not to protect data from malicious code. In other words, it was not known to use encapsulation for data security purposes.

2.13 In the Board's view, however, the access control in claim 1 is not limited to any particular purpose or intention. Indeed, the difference between malicious code and unintentionally erroneous code lies entirely in the mind of the programmer writing the code. The Board considers that the general idea behind encapsulation is to protect the object's data components from access by unauthorized code defined outside the class, and that the skilled person would have considered it as a means to protect sensitive data stored in the mobile phone.

2.14 Thus, in the Board's judgement, the subject-matter of claim 1 does not involve an inventive step (Article 56 EPC 1973) in view of a communication device comprising the standard Java environment.

T 0896/13 () of 22.6.2015

European Case Law Identifier: ECLI:EP:BA:2015:T089613.20150622

Verpackungsmaschine mit wenigstens einer Anmeldungsvorrichtung und Datenträger

Schlagwörter: Erfinderische Tätigkeit - (ja)

Anmeldenummer: 09005462.8
IPC-Klasse: B65B 57/00, G07C 9/00, G06F 21/00
Name des Anmelders: Multivac Sepp Haggenmüller GmbH & Co. KG

Kammer: 3.2.07

http://www.epo.org/law-practice/case-law-appeals/pdf/t130896du1.pdf

Anspruch 1 lautet wie folgt:

"Verpackungsmaschine (1) mit wenigstens einer Anmeldungsvorrichtung (13, 16), insbesondere Einloggvorrichtung, zur Anmeldung und Überprüfung der personenbezogenen Zugriffsberechtigung, wobei wenigstens eine der Anmeldungsvorrichtungen (13, 16) umfasst:

eine Leseeinheit zum Empfang drahtlos und/oder berührungslos übermittelter Informationen von drahtlos bzw. berührungslos auslesbaren, tragbaren Datenträgern (12, 18), die jeweils eine RFID-Transpondereinheit (20) umfassen,

wobei die Leseeinheit erst zum Empfang von Informationen bereit ist, wenn zuvor in einem Anmeldeprogramm eine Eingabe vorgenommen wurde, wobei die Verpackungsmaschine (1) eine Kontrolleinheit (25) umfasst, die dazu ausgebildet ist, bei der Anmeldung anhand der drahtlos und/oder berührungslos übermittelten Informationen unterschiedliche Zugriffsrechte zu erteilen,

wobei ferner eine Sendeeinheit zur Aussendung elektromagnetischer Wellen vorhanden ist und die Lese- und/oder Sendeeinheit als RFID-Station zur Informationsübertragung mit den RFID- Transpondereinheiten (20) ausgebildet ist,

wobei die wenigstens eine Anmeldungsvorrichtung ferner eine alternative Eingabevorrichtung zur verdrahteten Eingabe von Informationen umfasst."

D6 ist die einzige sich im Verfahren befindende Entgegenhaltung, die eine Verpackungsmaschine betrifft und somit eine gattungsgemäße Vorrichtung beschreibt.

Somit ist D6 gegenüber D4 ein besser geeigneter Ausgangspunkt zur Beurteilung der erfinderischen Tätigkeit.

Die Kammer kommt im vorliegendem Fall zu diesem Schluss, weil es sich im Anspruch 1 um eine Verpackungsmaschine handelt und nicht, im allgemeinen, um eine Anmeldungsvorrichtung "für eine Verpackungsmaschine", d.h. eine solche, die nur für diesen Zweck geeignet zu sein braucht.

Es kann durchaus sein, dass ein Fachmann aus dem Gebiet solcher Anmeldungsvorrichtungen wie D4 sich nach anderen Anwendungsgebieten als dem der allgemeinen Rechner-Arbeitsplätzen herumschaut.

Warum der Fachmann dabei ausgerechnet auf Verpackungsmaschinen stoßen würde, hat die angefochtene Entscheidung jedoch nicht erläutert. Gleiches gilt im übrigen für die Dokumente D1 bis D3 und D5.

1.3 Als Unterschied der Maschine nach Anspruch 1 gegenüber die im D6 beschriebene Verpackungsmaschine gilt, dass die Anmeldungsvorrichtung zur Überprüfung der personenbezogenen Zugriffsberechtigung geeignet ist und die folgenden zusätzlichen Merkmale umfasst:

- eine Leseeinheit zum Empfang drahtlos und/oder berührungslos übermittelter Informationen von drahtlos bzw. berührungslos auslesbaren, tragbaren Daten-trägern, die jeweils eine RFID-Transpondereinheit umfassen, wobei die Leseeinheit erst zum Empfang von Informationen bereit ist, wenn zuvor in einem Anmeldeprogramm eine Eingabe vorgenommen wurde, wobei die Verpackungsmaschine eine Kontrolleinheit umfasst, die dazu ausgebildet ist, bei der Anmeldung anhand der drahtlos und/oder berührungslos übermittelten Informationen unterschiedliche Zugriffsrechte zu erteilen, wobei ferner eine Sendeeinheit zur Aussendung elektromagnetischer Wellen vorhanden ist und die Lese- und/oder Sendeeinheit als RFID-Station zur Informationsübertragung mit den RFID Transpondereinheiten ausgebildet ist.

1.4 Wirkung-zu lösende Aufgabe

Diese Merkmale bewirken, dass unberechtigte Personen diese Vorrichtung nicht bedienen können, und dass eine passwortlose Anmeldung stattfinden kann.

Die zu lösende **Aufgabe** ist somit, die aus D6 bekannte **Verpackungsmaschine mit erhöhter Sicherheit auszustatten**, wobei eine Anmeldung mit möglichst wenig Zeit- bzw. Arbeitsaufwand verbunden ist

Ein Fachmann aus der Verpackungstechnik, wobei solche Maschinen üblicherweise mit mindestens einem Rechner-Arbeitsplatz versehen sind, wird sich zur Lösung der obigen Aufgabe schon mit dem allgemeinen Gebiet der Rechner-Arbeitsplätzen beschäftigen, und dabei auf die Dokumente D2 bis D5 stoßen.

Die Kammer ist der Auffassung, dass der Fachmann die Vorteile dieser Lehren (insbesondere der Lehren der D2, D4 und D5) erkennen und sie ohne praktische Schwierigkeiten auf die bekannte und rechnergesteuerte Verpackungsmaschine übertragen wird.

1.5.2 D2 (Seite 3, Zeilen 14-19) und D4 (Spalte 2, Zeilen 42-43) offenbaren, dass die Leseeinheit kontinuierlich oder zyklisch zum Empfang von Informationen bereit ist.

Die Leseeinheit der in der D5 beschriebenen Vorrichtungen ist immer bereit, Informationen zu empfangen (siehe Seite 175, Absatz 3 der D5), wobei die Zugangsperre nur desaktiviert ist, nachdem das Signal empfangen und in einem Anmeldeprogramm eine Eingabe vorgenommen wurde.

Der **Fachmann würde, bei einer direkten Anwendung einer dieser Lehren, ohne Ausübung einer erfinderischen Tätigkeit, nicht zum Gegenstand des Anspruchs 1 gelangen können**, weil keiner dieser Schriften lehrt, dass die Leseeinheit erst zum Empfang von Informationen bereit sein sollte, wenn zuvor in einem Anmeldeprogramm eine Eingabe vorgenommen wurde.

1.5.3 Die Prüfungsabteilung war der Auffassung, dass diese Merkmale sich aus der Anwendung des allgemeinen Fachwissens zwingend ergeben, weil es selbstverständlich sei, dass die Leseeinheit nur erst angeschaltet und zum Empfang von Informationen bereit sein solle, wenn zuvor in einem Anmeldeprogramm eine Eingabe vorgenommen würde, weil dadurch Stromkosten gespart würden.

Die Kammer teilt diese Auffassung nicht.

Grund dafür ist, dass alle zitierten Dokumente zeigen, dass es eher üblich ist, die Leseeinheit ständig bereit zu halten, weil diese Konfiguration Vorteile in der Anmeldung ermöglicht (z. B. eine berührungslose Anmeldung wird möglich).

Dazu kommt, dass die Energieeinsparung, die durch das Ausschalten einer solchen Leseeinheit ermöglicht wird, ein **Bruchteil davon ist, was für eine Verpackungsmaschine normalerweise an Energie benötigt ist, so dass der Fachmann diese Möglichkeit der Energieeinsparung nicht wirklich in Betracht ziehen würde**.

Aus diesen Gründen kommt die Kammer zu dem Schluss, dass der Gegenstand des Anspruchs 1 auf einer erfinderischen Tätigkeit beruht.

T 0718/10 (Format description/HARMAN BECKER) of 25.2.2015

European Case Law Identifier: ECLI:EP:BA:2015:T071810.20150225

Format description for a navigation database

Keywords: Inventive step - (yes)

Application number: 06014255.1
IPC class: G01C 21/26, G06F 17/30
Applicant name: Harman Becker Automotive Systems GmbH
Cited decisions: T 0929/94, T 0190/03

Board: 3.5.07

http://www.epo.org/law-practice/case-law-appeals/pdf/t100718eu1.pdf

The invention

2.1 The invention relates to databases for navigation systems. According to the background section of the application, known databases employ customised proprietary binary (or text) data formats that minimise storage requirements and optimise data access in view of a particular application. This approach has the problem that such data formats are difficult to adapt to future unforeseen requirements and format extensions. In particular, it is difficult to adapt a navigation database to a modified more recent format in such a way that it can still be read by older software releases. The object of the invention is therefore to provide a method for managing a navigation database in an efficient and reliable manner that allows for further extensions without any loss of compatibility.

2.2 The solution proposed by the present application is to associate with the database a "format description" describing the structure of the database records and to provide the navigation software with a "parser" for interpreting the data stored in the data file in accordance with the format description. In this way, if the format of the database is changed by extending the data records with new data fields, an existing version of the navigation software is still able to use the new database.

Claim 1 of the main request reads as follows:

"Method for organizing and managing data in a navigation database (1) of a navigation system comprising at least one data file (2), comprising

storing data in the at least one data file (2);

implementing at least one format description for the at least one data file (2) of the navigation database (1), wherein the format description declares types of records consisting of different data types and declares a sequence of elements of the records;

implementing a parser (4) for interpreting data stored in the at least one data file (2) and for parsing the data to a navigation software, wherein the parser is controlled by the at least one format description."

Claim 10 of the main request reads as follows:

"Navigation database (1) for a navigation system comprising at least one data file (2) and a format description for the at least one data file (2) configured to control a parser (4) that is configured to interpret data stored in the at least one data file (2) and to parse the data to a navigation software, wherein the format description declares types of records consisting of different data types and declares a sequence of elements of the records."

Inventive step - Article 56 EPC

5.1 In its decision, the Examining Division essentially argued with respect to claim 1 of the then main request that interpreting stored data for application software in accordance with a format description was generic functionality that could be found in a variety of well-known computer technologies and was implemented in "[a]ny program that interprets, maps, or parses data to an application according to some associated metadata". Examples of such technologies were "HTML, XML, PostScript, LaTeX, and Hashing Tables". The further limitation to navigation databases was obvious.

5.2 While the Board accepts that processing XML data typically involves parsing an XML data file on the basis of metadata embedded in the file, this metadata cannot be regarded as a "format description" that declares types of records. As explained on page 2, fourth paragraph, of the original description of the present application, in an XML file data entities are stored in association with identification tags. Each tag describes only its corresponding data entities; the tags do not give a general description of all data entities stored in the file.

5.3 The other examples given by the Examining Division are even less convincing. HTML, PostScript and LaTeX are document formats that include document processing instructions. These formats are not suitable for storing generic data entities, and documents in these formats do not include a "format description" within the meaning of the claim. In addition, it is not clear to the Board how "Hashing Tables" would relate to the invention, and the contested decision does not explain this further.

5.4 The Board is hence not convinced by the inventive step reasoning set forth in the decision under appeal. It will therefore perform its own assessment, starting with selecting the closest prior art.

5.5 As discussed in the background section of the present application, the starting point for the present invention was a commonplace vehicle navigation system. Such a vehicle navigation system comprises a (navigation) database storing lists of entries representing inter alia cities, streets and points of interest, typically in a customised proprietary data format in order to minimise storage requirements and optimise data access.

5.6 The European search report cited documents D1 and D2. Document D1 relates to the generation of route maps. It is not concerned with database formats for such route maps. Document D2 relates to the transformation of XML documents using stylesheets. Neither of

these documents is closer to the invention than the aforementioned commonplace vehicle navigation system, which is hence taken to be the closest prior art.

5.7 The subject-matter of claim 1 differs from this closest prior art essentially in that the navigation software accesses the data stored in the navigation database using a parser that parses the data on the basis of a format description. According to the claim, this format description "declares types of records consisting of different data types and declares a sequence of elements of the records".

The **effect of these features** is that **the data format of the data stored in the navigation database is decoupled from the navigation software in the sense that a particular version of the navigation software continues to be functional even if the data format of the navigation database is changed**, e.g. if new data fields are added. This ability to work with future data formats is known in the art as "upward compatibility".

Starting from a known navigation system as described in the background section of the application, the **objective technical problem to be solved may therefore be regarded as that of ensuring compatibility of the system with future versions of the system's navigation database**. Neither document D1 nor document D2 addresses this problem.

5.8 In its communication accompanying the summons to oral proceedings, the Board cited document D3. Section 2 of this document discusses the "SDF Self-Describing File Format". An SDF file consists of a descriptive header followed by a series of data records. The header describes the format of data records and specifies mnemonic names for data-record types and data-record fields. According to section 2.2, SDF files offer several advantages, one of them being the potential of upward-compatible extension, meaning that new fields or record types can be added in a way that allows old programs to accept the new data files without even needing to be recompiled.

5.9 At the oral proceedings, the appellant did not call into question that document D3 implicitly disclosed a "parser" for parsing the data contained in an SDF file on the basis of its descriptive header. **The appellant contested, however, that the skilled person would consider document D3** when looking for a solution to the problem posed.

5.10 As explained in its abstract, document **D3 focuses on the use of SDF files for the purpose of building tools for gathering and visualising parallel program performance data**. The field of program performance analysis is **clearly remote from the field of navigation databases.**

In the Board's view, the skilled person faced with the stated problem would not confine himself to navigation databases but would look for a solution in the more general field of database technology. It could further be argued that the skilled person would recognise that the teaching of sections 2 and 2.2 of document D3 is not limited to the processing of performance data, but is more generally applicable. **However, document D3, while dealing with data sets comprising large numbers of data records, is not concerned with accessing individual records in a database.** Instead, the SDF files of document D3 are processed as a whole, and the SDF format is primarily intended to allow information exchange between different application programs (see abstract and page 259, lines 6 to 16). **SDF files are therefore not comparable to databases of navigation systems.**

Hence, the Board concurs with the appellant and judges that **the skilled person, faced with the problem posed, would not consider document D3**.

5.11 It follows that the subject-matter of claim 1 and that of corresponding claim 10 of the main request involves an inventive step over the available prior art. By virtue of their dependency on claim 1, the same applies to the subject-matter of claims 2 to 9. The main request hence meets the requirements of Articles 52(1) and 56 EPC.

T 1003/09 (Virtual index changes/GOOGLE) of 29.4.2015

European Case Law Identifier: ECLI:EP:BA:2015:T100309.20150429

A database system for viewing effects of changes to a[n] index for a query optimization plan

Inventive step - (yes)

Application number: 00960157.6
IPC class: G06F 17/30
Applicant name: Google Inc.
Cited decisions: T 0910/03

Board: 3.5.07

http://www.epo.org/law-practice/case-law-appeals/pdf/t091003eu1.pdf

As explained in the background section of the description (application as published, page 1, third paragraph), in most databases, "data is externally structured into tables. Each table generally includes a series of fields which define columns of the table. Each row of the table comprises a single record".

A program referred to as a "Database Management System" ("DBMS") identifies and retrieves certain information objects in response to "queries" from a user.

To facilitate information retrieval from a database, information objects are "indexed", that is they are characterised by assigning descriptors to identify their content.

According to the description, the process of building an index for a large table generally consumes great amounts of time and resources as it requires the DBMS to scan the table, retrieve the data from every row and column and to add the data to the index, which is often in the form of a B-tree structure.

The gist of the present invention consists essentially in creating a "virtual table" by copying the original table, excluding any of the original data. By excluding data when copying the

original table to define the "virtual table", the associated index, i.e. the "virtual index" may be easily and quickly modified or created, if it does not exist. By replacing in the query references to the original table with references to the "virtual table", changes to the original indexing design can be quickly tested and a new optimisation plan determined (cf. page 5, line 10 to page 6, line 14).

Claim 1 of the main request considered in the decision under appeal related to a "computer implemented-method for viewing changes to an original optimization plan for a query to a database".

Claim 1 specified the following features and steps:

(a) the database has an original table with data stored therein;

(b) the query includes a reference to the original table;

(c) defining a virtual table that is a copy of the original table but which excludes data stored in the rows of the original table,

(i) wherein defining a virtual table includes copying the original table statistics to the virtual table;

(d) defining a virtual index, the virtual index being an index associated with the virtual table;

(e) replacing, in the query, the reference to the original table with a reference to the virtual table;

(f) determining a new optimization plan for the query;

(g) replacing, in the new optimization plan, a reference to the virtual table with a reference to the original table; and

(h) displaying the new optimization plan.

9.1 In particular, the Examining Division noted that the method known from the closest prior-art document D1 essentially achieved the same purpose as the present invention, in the sense that both supported a "what-if" analysis for query optimisation plans with respect to index changes. However, document D1 implemented this analysis as part of the DBMS software, using modifications of built-in SQL commands such as "CREATE INDEX", whereas the application proposed an alternative implementation on top of the DBMS, thus without requiring access to the DBMS source code.

9.2 In the Examining Division's view, third-party tool developers usually had no access to the DBMS source code, but often wanted to provide known tools for a particular DBMS software. Thus, the question to be considered was whether the implementation of a known tool on top of a DBMS by a third-party vendor involved an inventive step.

9.3 The Examining Division came to the conclusion that the implementation according to the claimed method was straightforward, as it merely involved copying table and index

information for hypothetically changing the index topography, and using the existing tools for obtaining the query optimisation plan. In other words, the Examining Division considered that the claimed method was the result of routine software development.

9.5 In summary, the Examining Division considered that a developer wishing to provide a third-party tool for adding a known functionality to a DBMS, faced a one-way situation leading directly to the claimed solution.

11.5 In summary, the method known from document D1 inter alia comprises the following steps:

(a) the database has an original table with data stored therein;

(b) the query includes a reference to the original table;

(c) defining a hypothetical index;

(d) determining a new optimization plan for the query;

(e) displaying the new optimization plan.

12. Claim 1 of the appellant's main request in particular differs from the arrangement known from document D1 in that it comprises the following steps:

- defining a virtual table that is a copy of the original table but which excludes data stored in the rows of the original table, wherein defining a virtual table includes copying the original table statistics to the virtual table;

- replacing, in the query, the reference to the original table with a reference to the virtual table;

- replacing, in the new optimization plan, a reference to the virtual table with a reference to the original table.

12.2 In summary, both document D1 and the present invention seek to provide a tool for analysing the impact of an index design on the operation of a database. D1 solves the problem at the level of the DBMS, whilst the invention proposes a solution on top of the DBMS.

13.4 None of the available prior art teaches copying a table without data to create a virtual table while keeping the statistics of the original table.

It may be, as held by the Examining Division, that there is only one solution to the problem of providing the functionality of the method according to document D1 without modifying the DBMS software. **However, this does not imply that this solution is a straightforward application of the teaching of D1 or that it would be obvious to the skilled person**.

In fact, in the Board's opinion, **the alleged uniqueness of a solution to a known problem does not provide sufficient proof for a lack of inventive step.** What matters is whether it would have been obvious to a skilled person to actually arrive at the solution.

13.5 According to the Examining Division, the skilled person was aware that the optimizer needed the metadata of the database under the "what-if" scenario, i.e. the metadata of the tables, indexes, statistics that would be present if the indexes were changed as foreseen by the "what-if" scenario. From this, the Examining Division concluded that the straightforward way was to create a new "virtual" table having the same schema as the original table with the changed set of virtual indexes and to provide the optimiser with the table statistics and index statistics. Since the concept of a "virtual table", as a copy of the original table which excludes data stored in the original table but includes the original table statistics, is not disclosed in any of the available prior art, the Board considers that a pointer to the invention is missing which would bridge the gap between the prior art and the present invention.

14. In summary the Board comes to the conclusion that the subject-matter of claim 1 according to the appellant's main request involves an inventive step.

T 0756/09 (Fluid flow simulation/MOLDFLOW) of 18.3.2015

European Case Law Identifier: ECLI:EP:BA:2015:T075609.20150318

Method for modelling three-dimensional objects and simulation of fluid flow

Application number:	98905149.5
IPC class:	G06F 17/13, G06F 17/50, B29C 33/00, B29C 45/02, B29C 45/76, G06T 17/20
Applicant name:	Moldflow Pty. Ltd.
Opponent name:	Dassault Systèmes SA
Cited decisions:	G 0002/94, G 0004/95, T 0334/94

Board: 3.5.07

http://www.epo.org/law-practice/case-law-appeals/pdf/t090756eu1.pdf

Claim 1 according to the respondent's request relates to a computer-implemented method for producing simulations of fluid flow within a three dimensional object. The claimed method comprises the following features itemised by the Board:

(a) specifying first and second generally opposed surfaces of said object,

(b) matching each element of the said first surface with an element of said second surface between which a reasonable thickness may be defined,

(i) wherein matched elements of said first surface constitute a first set of matched elements and

(ii) matched elements of said second surface constitute a second set of matched elements,

(c) specifying a fluid injection point,

(d) performing a flow analysis using each set of said matched elements, and

(e) synchronizing flow fronts resulting from said flow analysis along said first and second surfaces,

(f) whereby the resulting flow fronts along said first and second surfaces are synchronized.

Inventive step

11. As pointed out in the description of the published application the "flow of melt in an injection mold is determined by the familiar conservation laws of fluid mechanics. Solution of the equations in their full generality presents several practical problems. Owing to the characteristically thin walls of molded components, however, it is possible to make some reasonable assumptions that lead to a simplification of the governing equations. These simplified equations describe what is called Hele-Shaw flow and may be readily solved in complex geometries using an appropriate numerical technique such as the finite element and/or finite difference method".

11.1 As pointed out in the paragraph bridging pages 2 and 3, flow analysis using the Hele-Shaw approximation "requires the use of a surface model, representing the midplane of the real component, which is then meshed with triangular or quadrilateral elements to which suitable thicknesses are ascribed. The preparation of such a mesh can take a considerable amount of time, and requires substantial user input ...".

… The high number of elements makes the problem intractable for any but the fastest super computers. ... Thus, although three dimensional simulation provides a solution that avoids the requirement of a midplane model, it is not as yet a practical solution".

12. Thus, an **object of the invention** is to **provide a method for the simulation of flow in a three dimensional object that can produce simulations substantially automatically, without requiring the solution of the governing equations in their full generality**.

12.1 According to the … application as published, the method of the present invention utilises only the outer surfaces defining the three dimensional object to create a computational domain. These surfaces correspond to the representations of the domain in which flow is to be simulated and would comprise for example meshed representations of the top and bottom surfaces of a part. Thus, "the invention could be said to utilize an outer skin mesh rather than a midplane mesh. Elements of the two surfaces are matched, based on the ability to identify a thickness between such elements. An analysis, substantially along conventional lines (by means, for example, of the Hele-Shaw equations), is then performed of the flow in each of these domains in which flow is to be simulated, but linked to ensure fidelity with the physical reality being modelled".

12.2 In other words, the **gist of the present invention consists essentially in replacing the midplane representation of an object, conventionally used when the Hele-Shaw approximation is applied, with a mesh representation of the top and bottom surfaces of a part, whereby the two simulated flows are linked to reflect the physical reality of a flow in a cavity delimited by the part's top and bottom surfaces**.

15.1 …, document D2 specifies that the lead-lag shown in figure 4 represents a physical reality, which corresponds to the results provided by the simulation, and not an imperfect simulation of the physical reality which required some corrective measure. In fact, **adding a flow front synchronising step to the flow simulation method described in D2 would be contrary to the teaching of this document**, as it would not lead to a result compatible with the representation of the physical flow fronts of epoxy melt injected into the two cavities delimited in the mould by the leadframe.

15.2 Furthermore, the Board agrees with the respondent that in the particular case considered in document D2 the two surfaces are not the outer surfaces of an object that should be modelled for the purpose of injection moulding. The surfaces referred to in document D2 appear indeed to represent a plane on either side of the leadframe which divides the mould into two cavities with separate flows of the injected melt. For lack of evidence to the contrary, it seems reasonable to assume, as argued by the respondent, that the simulation referred to in document D2 uses the midplane representation or at the most the three-dimensional simulation acknowledged as prior art in the contested patent.

15.3 Hence, the Board considers that it would not have been obvious to a person skilled in the art starting from the teaching of document D2 to arrive at a method falling within the terms of claim 1 of the respondent's request (Article 56 EPC).

T 1211/10 (Two-channel authentication/ERICSSON) of 16.4.2015

European Case Law Identifier: ECLI:EP:BA:2015:T121110.20150416

METHOD AND APPARATUS FOR AUTHORIZING INTERNET TRANSACTIONS USING THE PUBLIC LAND MOBILE NETWORK (PLMN)

Application number: 02788365.1
IPC class: G06F 1/00
Applicant name: Ericsson Inc.
Cited decisions: T 0641/00, T 0154/04, G 0003/08

Board: 3.5.06

http://www.epo.org/law-practice/case-law-appeals/pdf/t101211eu1.pdf

2. The context of the invention

2.1 The application relates to a two-channel authentication and transaction authorisation method for e-commerce transactions.

2.2 The user conducts an online shopping transaction at a merchant's website using a PC with an Internet connection; see 101 and step 1 in figure 1 and page 10, lines 16 to 20. The user fills a notional "shopping cart" and proceeds to the "check out" point where he/she is requested to enter the number of the mobile phone (103 in figure 1) which he/she intends to use for the authentication and authorisation process (page 10, lines 18 to 23; 203 in figure 2A; page 15, lines 10 to 11). Figure 4 shows an example PC screen on which the user enters his/her mobile phone number.

2.3 The user then receives on his/her mobile phone a WAP push message, sent through the mobile phone operator's PLMN, comprising a hyperlink to a WML contract at the WAP server (see page 11, lines 1 to 4 and 9 to 14; 205 in figure 2A; page 15, lines 12 to 19). Figure 5 shows the screen of the mobile phone displaying the message received at the mobile phone.

2.4 When the user follows the hyperlink, a WML contract representative of the transaction initiated at the PC is displayed on the mobile phone as a WMLScript signText string (see page 11, lines 13 to 19; 206 in figure 2A and 207 in figure 2B; page 15, line 20, to page 16, line 3). The WML contract is shown in figure 6. If the user accepts the terms of the contract, he/she digitally signs it by means of the signText routine with his/her private key securely stored on the mobile phone and transmits it back to the merchant (see page 11, line 19, to page 12, line 2; 208 in figure 2B; page 16, lines 20 to 21).

2.5 The signed contract is forwarded by the merchant to an operator or an "acquirer" or "issuer" for signature verification and archiving of the signed payment contract (see page 12, lines 7 to 10; 210 and 211 in figure 2B, 212 in figure 2C; page 16, line 22, to page 17, line 11). Once the signed contract is verified, the user receives, both on the PC and on the mobile phone (see figure 9), a confirmation that the transaction has been authorised (see page 12, lines 10 to 15; 216 in figure 2C; page 17, lines 18 to 21).

Claim 1 according to the main request reads as follows:

"A method of authorizing a transaction in which transaction information indicative for the transaction is presented from a server to a user at an Internet access device (PC) in a first information set in a first format suitable for presentation on the Internet access device (PC), the method comprising steps performed by the server or a further server:

- creating a second information set in a second format suitable for presentation at a mobile terminal (PTD), wherein the second information set is representative of the first information set;

- linking the first information set and the second information set;

- sending the second information set to a public land mobile network (PLMN) for presentation to the user at the mobile terminal (PTD);

- receiving authentication information from the mobile terminal (PTD) through the PLMN; and

- requesting a verification of the received authentication information before authorizing the transaction."

5. Article 52(2)(c) EPC (methods for doing business, etc.)

5.1 Although the examples given in the description relate principally to commercial applications, in particular to online shopping, the board considers the invention not to fall under the exclusions listed in Article 52(2)(c) EPC. In particular, **the board does not accept the reasoning in the appealed decision that the problem to be solved by the computing devices used in the invention is "not a technical problem but a business one**"; see point 1.5 of the reasons. **The board considers that, contrary to the finding in the decision, the aim of the invention is token-based authentication by means of a mobile phone, which is a technical problem**. **The particular application context in which this problem is solved, i.e. online shopping, does not detract from the technical nature of this problem**.

5.2 The board also does not agree with the statement in the decision that the dependent claims of the then main request "do not introduce any further limiting features not falling under the exclusions of Article 52(2)(c) EPC"; see point 2 of the reasons. In the board's view, the features set out in these claims, which relate to WAP push messages, HTML and WML formatting, digital signatures using a WAP signText script and public key infrastructure (PKI) information are, in the context of this case, **not related solely to business activities**.

5.3 Consequently the board considers document D3 to be a more appropriate starting point for the assessment of inventive step than the "commonly known technical apparatus [such as] the Internet access device (common PC), a mobile terminal (mobile phone), public mobile network ([GSM]) and the Internet" relied on in the decision; see point 1.11 of the reasons.

… In a public key infrastructure the validity of a key is typically ensured by a separate certification authority. If the validation of a digital signature relies on the signer's public key issued earlier, then no interaction with the certification authority is required at this point. Such an interaction may be needed, however, in order to establish that the key certificate has not been revoked. Thus "sending a request for verification" to a "separate [...] authority server" is already obvious over standard PKI architecture. To the extent that "verification of the received authentication information" involves steps not commonly performed by the certification authority, the board first notes that adding a further party to the verification process need not improve the security of the process. Indeed, it may introduce an additional security risk. Adding a further party to the verification process may, however, relieve the merchant server of some of its computational burden, which is obvious since outsourcing computational tasks to other servers is standard practice in the relevant art.

8.7 Therefore the board concludes that the subject-matter of claim 1 according to the twelfth auxiliary request does not involve an inventive step, contrary to Article 56 EPC 1973.

11.1 As the subject-matter of claim 1 of the twelfth auxiliary request is considered not to involve an inventive step, and since claim 1 of the main, first to third, sixth and ninth auxiliary requests is even broader than claim 1 of twelfth auxiliary request, their subject-matter is also considered not to involve an inventive step, contrary to Article 56 EPC 1973.

T 1925/11 (Modular reduction hardware/INSIDE SECURE) of 25.3.2015

European Case Law Identifier: ECLI:EP:BA:2015:T192511.20150325

RANDOMIZED MODULAR POLYNOMIAL REDUCTION METHOD AND HARDWARE THEREFOR

Keywords: Inventive step - after amendment (yes)

Application number: 06749987.1
IPC class: G06F 7/72
Applicant name: Inside Secure

Board: 3.5.06

http://www.epo.org/law-practice/case-law-appeals/pdf/t111925eu1.pdf

The invention

1. The application relates to cryptographic methods based on modular arithmetic in finite fields. Such methods, the AES/Rijndael cipher being mentioned as one example (p. 1, lines 20-26), rely on polynomial reduction by a specified modulus.

1.1 Since this reduction operation is one of the most expensive operations in cryptography, a number of dedicated fast methods have been developed, one of which by Barrett. The application presents the necessary formulae for Barrett's algorithm adapted to modular reduction of polynomials in a binary finite field (see p. 8, lines 29-34, and p. 9, esp. lines 18 and 28).

1.2 The application mentions in general terms that "[m]athematical computations performed by cryptographic systems may be susceptible to power analysis and timing attacks" (p. 1, lines 26-28). Elsewhere, reference is made to "crypt[]analytic attacks that rely upon consistency in power usage to determine the modulus" (p. 11, lines 6-8).

1.3 The invention sets out to make Barrett's algorithm "more secure against crypt[]analysis attacks, while still providing fast and accurate results". To achieve this effect, the application proposes to "[inject] a random polynomial error E(x) [...] into the computed polynomial quotient to obtain a randomized quotient" (p. 10, lines 4-7).

1.4 The description discloses the mathematical steps to be performed in a "polynomial reduction operation", and then that "[f]or a modulus of high degree (multi-word) the operation can be performed with word shifts rather than bit shifts" (p. 9, lines 20-32). To this end, the formulae used are reformulated in terms of the "word size w", more precisely in terms of divisions by x**((2k+w)) and x**((k-w)) (see p. 9, lines 32-34). This is said to "simplif[y] handling of the polynomial quantities on computational hardware" (see p. 9, line 35 - p. 10, line 3).

1.5 The description further explains that the multi-word modular reduction is to be carried out on computational hardware which locates the operands within the RAM by means of a pointer and an indication of the operand length in terms of number of words (see p. 4, lines 7-25, esp. lines 20-25).

2. In the board's opinion it is evident for the skilled reader that "the operation" mentioned on page 9, line 31, refers to the polynomial reduction operation as a whole and, in particular, to the calculation of q(x) and u(x). Furthermore, in the board's view, the statement that the operation "can be performed with word shifts rather than bit shifts" (emphasis by the board) must be read as stating that bit shifts are replaced by word shifts throughout the operation.

The prior art

3. D1 discloses a variant of Barrett's method generalized to polynomial reduction in a binary finite field which is substantially equivalent to the one presented in the application (see D1, abstract, lines 6-7, and in particular p. 204, equation (1)) except for the exponents in the central formula (loc. cit.) which define the number of bit shifts to be performed. The central formula is based on bit shifts defined in terms of p, the degree of the modulus N(x), and "some value of beta to be defined later" (see sec. 2, the para. just above equation (1)). In the sequel of the paper, it is noted that the calculation can be simplified for "beta >= alpha" and, in particular, for "beta = alpha", where alpha=deg(U)-deg(N) is the difference between the degrees of the polynomial to be reduced and of the modulus (see sec. 1, 1st para. and the sentences just below equations (4) and (7)).

Inventive step

6. D1 is not concerned with cryptanalytic side channel attacks and thus has no occasion to disclose anything about protection against such attacks. D1 also does not mention the choice of beta in view of the chosen hardware platform nor the exploitation of word shifts in the implementation of the algorithm.

7. The claimed invention therefore differs from D1 by

(a) the generation of a randomized polynomial quotient q'(x) based on a random polynomial error value E(x), and

(b) the calculation of the polynomial reduction operation by performing word shifts.

7.1 These features address different problems. Difference (a) is meant **to increase security against crypt[]analysis attacks**" while difference (b) is argued to **allow for a more efficient implementation on hardware with multi-word operands and instructions**.

7.2 The preamble of claim 1 refers to a "cryptographic method comprising a modular polynomial reduction operation". The body of claim 1 does not state, however, where specifically in the cryptographic method the modular polynomial reduction is to be performed and what its parameters mean in that context.

7.3 For that reason, the board has its doubts - as indicated in the summons (point 6.3) - whether difference (a) in the claimed modular polynomial reduction operation could be said to

increase cryptographic security as long as the claims did not specify that the masked operation indeed relate to a "secret" of the cryptographic method which might be the target of a cryptanalytic attack (see summons, point 6.3).

7.4 As regards difference (b), the board is satisfied that, as explained in the description, commonly known cryptographic methods rely on modular polynomial reduction operations, and that, therefore, such methods may profit from a different, possibly more efficient, implementation of modular polynomial reduction - independent of whether they "relate to a secret" or not.

7.5 Further with regard to difference (b), the board considers that **the use of word shifts rather than bit shifts may be more efficient under certain circumstances,** in particular for certain sizes of the modulus and the polynomial to be reduced, **but doubts that this can be said for all such values**. An **increase of efficiency can hence not be attributed to the claimed method over its entire breadth**, and the description provides no basis for the skilled person to determine the pertinent circumstances.

7.6 The board is, **however, satisfied that the claimed implementation of the operation by word shifts, i.e. difference (b), enables a different implementation of the known algorithm exploiting a particular multi-word operand addressing scheme.** In this regard the board notes specifically that for an operand given in terms of a pointer and a length in number of words (see description, p. 4, lines 20-25), a right shift by, say, one word can be implemented by a mere decrement of the operand length.

8. As mentioned above, D1 does not disclose or suggest the selection of the exponent beta in terms of the word size w of the given computer hardware in view of implementing the algorithm in terms of word shifts. Nor do documents D2-D4 which rather relate to the security aspect of the present invention (by way of "masking", "brouillage" or "Verfremdung", resp.). Since, moreover, the board does not consider this modification of the known modular polynomial reduction operation to be obvious from common knowledge alone, the board comes to the conclusion that claim 1 shows the required inventive step over D1 in view of D2-D4, Article 56 EPC 1973. The same applies to claim 5 by virtue of its explicit reference to method claim 1.

9. As a consequence, the inventive merit of difference (a) vis-à-vis D1 and, in particular, the questions of whether it contributes to increased cryptographic security and the technical character of the claimed method can be left open.