(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
16. Oktober 2003 (16.10.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2003/085879 A3

(51) Internationale Patentklassifikation[7]: G06F 7/72

(21) Internationales Aktenzeichen: PCT/EP2003/003601

(22) Internationales Anmeldedatum:
7. April 2003 (07.04.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102 15 164.4 5. April 2002 (05.04.2002) DE

(71) Anmelder und
(72) Erfinder: **MIHAILESCU, Preda** [CH/CH]; Seestrasse 78, CH-8700 Erlenbach (CH).

(74) Anwalt: **LUCHT, Silvia**; Werderring 15, 79098 Freiburg (DE).

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

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

Veröffentlicht:
— *mit internationalem Recherchenbericht*
— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

(88) Veröffentlichungsdatum des internationalen Recherchenberichts: 28. Oktober 2004

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

(54) Title: CRYPTOGRAPHIC METHOD

(54) Bezeichnung: KRYPTOGRAFISCHES VERFAHREN FUR OFFENTLICHE SCHLUSSEL

(57) Abstract: The invention relates to a cryptographic method for the machine encryption of data and the machine decryption of the encrypted data or for encoding data. According to the invention, Galois fields that are adapted to the processor are used whose field characteristic p is adapted to the machine word length B, whereby $2^{B}/^{2-2}<p<2^{B}$.

(57) Zusammenfassung: Es wird ein kryptografisches Verfahren zur maschinellen Verschlüsselung von Daten und zur maschinellen Entschlüsselung der verschlüsselten Daten oder zur Datencodierung vorgeschlagen, bei dem Prozessor angepasste Galoiskörper verwendet werden, deren Körpercharakteristik p der Maschinenwortlänge B angepasst ist, wobei $2^{B}/^{2-2} < p < 2^{B}$.

WO 2003/085879 A3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 03/03601

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/72

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 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 practical, search terms used)
EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BAILEY D V ET AL: "Optimal extension fields for fast arithmetic in public-key algorithms" ADVANCES IN CRYPTOLOGY. CRYPTO '98. 18TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. SANTA BARBARA, AUG. 23 - 27, 1998. PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE ; VOL. 1462, BERLIN : SPRINGER, DE, 23 August 1998 (1998-08-23), pages 472-485, XP002165681 ISBN: 3-540-64892-5 Paragraph 2 ----- -/--	1

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

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 July 2004	29/07/2004

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

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 03/03601

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Y. FUTA ET AL.: "Efficient construction of elliptic curves over optimal extension-field" TRANSACTIONS OF THE INFORMATION PROCESSING SOCIETY OF JAPAN, vol. 41, no. 8, August 2000 (2000-08), pages 2092-2101, XP008032150 JAPAN ISSN: 0387-5806 page 2094, right-hand column; table 1	1
X	P. MIH?ILESCU: "Medium Galois Fields, their Bases and Arithmetic"'Online! February 2000 (2000-02), XP002286072 Retrieved from the Internet: URL:http://web.archive.org/web/20010820191512/http://grouper.ieee.org/groups/1363/P1363a/contributions/Medium.pdf> 'retrieved on 2004-06-24! page 3	1
L	-& INTERNET ARTICLE, 'Online! XP002286073 Retrieved from the Internet: URL:http://web.archive.org/web/*/http://http://grouper.ieee.org/groups/1363/P1363a/NumThAlgs.html> 'retrieved on 2004-06-24! the whole document Zeigt dass das Dokument http://grouper.ieee.org/groups/1363/P1363a/NumThAlgs.html am 20. August 2001 verfügbar war.	1
L	-& ANONYMOUS: "IEEE P1363a: Additional number-theoretic algorithms" INTERNET ARTICLE, 'Online! XP002286074 Retrieved from the Internet: URL:http://web.archive.org/web/20010820191512/http://grouper.ieee.org/groups/1363/P1363a/NumThAlgs.html> 'retrieved on 2004-06-24! paragraph '0006! Bestimmt die Publikationsdatum von http://web.archive.org/web/20010820191512/http://grouper.ieee.org/groups/1363/P1363a/contributions/Medium.pdf als Februar 2000	1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP 03/03601

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 2-6
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

See Annex PCT/ISA/210

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

Continuation of Box I.2

Claims No.: 2-6

It is not clear from the application to what extent the methods as per claims 2-6 would differ technically from the prior art because these claims mention no method steps (PCT Rule 6.3(a)), the methods explained in the description include many alternatives and no clear technical effect is obtained (PCT Rule 5.1(iii)). Moreover, the method as per claim 5 is not supported by the description (PCT Article 6).

The applicant is advised that claims or parts of claims relating to inventions in respect of which no international search report has been established cannot normally be the subject of an international preliminary examination (PCT Rule 66.1(e)). In its capacity as International Preliminary Examining Authority the EPO generally will not carry out a preliminary examination for subjects that have not been searched. This also applies to cases where the claims were amended after receipt of the international search report (PCT Article 19) or where the applicant submits new claims in the course of the procedure under PCT Chapter II. After entry into the regional phase before the EPO, however, an additional search can be carried out in the course of the examination (cf. EPO Guidelines, C-VI, 8.5) if the defects that led to the declaration under PCT Article 17(2) have been remedied.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 03/03601

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F7/72

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 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, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	BAILEY D V ET AL: "Optimal extension fields for fast arithmetic in public-key algorithms" ADVANCES IN CRYPTOLOGY. CRYPTO '98. 18TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. SANTA BARBARA, AUG. 23 - 27, 1998. PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE ; VOL. 1462, BERLIN : SPRINGER, DE, 23. August 1998 (1998-08-23), Seiten 472-485, XP002165681 ISBN: 3-540-64892-5 Paragraph 2 ----- -/--	1

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

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
13. Juli 2004	24 08. 2004

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

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 03/03601

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	Y. FUTA ET AL.: "Efficient construction of elliptic curves over optimal extension-field" TRANSACTIONS OF THE INFORMATION PROCESSING SOCIETY OF JAPAN, Bd. 41, Nr. 8, August 2000 (2000-08), Seiten 2092-2101, XP008032150 JAPAN ISSN: 0387-5806 Seite 2094, rechte Spalte; Tabelle 1 ---	1
X	P. MIH?ILESCU: "Medium Galois Fields, their Bases and Arithmetic"[Online] Februar 2000 (2000-02), XP002286072 Gefunden im Internet: URL:http://web.archive.org/web/20010820191512/http://grouper.ieee.org/groups/1363/P1363a/contributions/Medium.pdf> [gefunden am 2004-06-24] Seite 3	1
L	-& INTERNET ARTICLE, [Online] XP002286073 Gefunden im Internet: URL:http://web.archive.org/web/*/http://http://grouper.ieee.org/groups/1363/P1363a/NumThAlgs.html> [gefunden am 2004-06-24] das ganze Dokument Zeigt dass das Dokument http://grouper.ieee.org/groups/1363/P1363a/NumThAlgs.html am 20. August 2001 verfügbar war.	1
L	-& ANONYMOUS: "IEEE P1363a: Additional number-theoretic algorithms" INTERNET ARTICLE, [Online] XP002286074 Gefunden im Internet: URL:http://web.archive.org/web/20010820191512/http://grouper.ieee.org/groups/1363/P1363a/NumThAlgs.html> [gefunden am 2004-06-24] Absatz [0006] Bestimmt die Publikationsdatum von http://web.archive.org/web/20010820191512/http://grouper.ieee.org/groups/1363/P1363a/contributions/Medium.pdf als Februar 2000 ---	1

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 03/03601

Feld I Bemerkungen zu den Ansprüchen, die sich als nicht recherchierbar erwiesen haben (Fortsetzung von Punkt 2 auf Blatt 1)

Gemäß Artikel 17(2)a) wurde aus folgenden Gründen für bestimmte Ansprüche kein Recherchenbericht erstellt:

1. ☐ Ansprüche Nr.
weil sie sich auf Gegenstände beziehen, zu deren Recherche die Behörde nicht verpflichtet ist, nämlich

2. ☒ Ansprüche Nr. 2-6
weil sie sich auf Teile der internationalen Anmeldung beziehen, die den vorgeschriebenen Anforderungen so wenig entsprechen, daß eine sinnvolle internationale Recherche nicht durchgeführt werden kann, nämlich
siehe BEIBLATT PCT/ISA/210

3. ☐ Ansprüche Nr.
weil es sich dabei um abhängige Ansprüche handelt, die nicht entsprechend Satz 2 und 3 der Regel 6.4 a) abgefaßt sind.

Feld II Bemerkungen bei mangelnder Einheitlichkeit der Erfindung (Fortsetzung von Punkt 3 auf Blatt 1)

Die internationale Recherchenbehörde hat festgestellt, daß diese internationale Anmeldung mehrere Erfindungen enthält:

1. ☐ Da der Anmelder alle erforderlichen zusätzlichen Recherchengebühren rechtzeitig entrichtet hat, erstreckt sich dieser internationale Recherchenbericht auf alle recherchierbaren Ansprüche.

2. ☐ Da für alle recherchierbaren Ansprüche die Recherche ohne einen Arbeitsaufwand durchgeführt werden konnte, der eine zusätzliche Recherchengebühr gerechtfertigt hätte, hat die Behörde nicht zur Zahlung einer solchen Gebühr aufgefordert.

3. ☐ Da der Anmelder nur einige der erforderlichen zusätzlichen Recherchengebühren rechtzeitig entrichtet hat, erstreckt sich dieser internationale Recherchenbericht nur auf die Ansprüche, für die Gebühren entrichtet worden sind, nämlich auf die Ansprüche Nr.

4. ☐ Der Anmelder hat die erforderlichen zusätzlichen Recherchengebühren nicht rechtzeitig entrichtet. Der internationale Recherchenbericht beschränkt sich daher auf die in den Ansprüchen zuerst erwähnte Erfindung; diese ist in folgenden Ansprüchen erfaßt:

Bemerkungen hinsichtlich eines Widerspruchs

☐ Die zusätzlichen Gebühren wurden vom Anmelder unter Widerspruch gezahlt.

☐ Die Zahlung zusätzlicher Recherchengebühren erfolgte ohne Widerspruch.

WEITERE ANGABEN PCT/ISA/ 210

Fortsetzung von Feld I.2

Ansprüche Nr.: 2-6

Aus der Anmeldung geht nicht deutlich hervor in wiefern die Verfahren von Ansprüchen 2-6 sich technisch vom Stand der Technik unterscheiden könnten, weil in diesen Ansprüchen kein einziger Schritt genannt wird (Regel 6.3(a) PCT), weil die in der Beschreibung ausgearbeitete Verfahren viele Alternativen haben und weil kein deutlicher technischer Effekt vorliegt (Regel 5.1(iii) PCT). Das Verfahren von Anspruch 5 wird weiterhin nicht von der Beschreibung gestützt (Artikel 6 PCT).

Der Anmelder wird darauf hingewiesen, dass Patentansprüche auf Erfindungen, für die kein internationaler Recherchenbericht erstellt wurde, normalerweise nicht Gegenstand einer internationalen vorläufigen Prüfung sein können (Regel 66.1(e) PCT).In seiner Eigenschaft als mit, der internationalen vorläufigen Prüfung beauftragte Behörde wird das EPA also in der Regel keine vorläufige Prüfung für Gegenstände durchführen, zu denen keine Recherche vorliegt.Dies gilt auch für den Fall, dass die Patentansprüche nach Erhalt des internationalen Recherchenberichtes geändert wurden (Art. 19 PCT), oder für den Fall, dass der Anmelder im Zuge des Verfahrens gemäss Kapitel II PCT neue Patentanprüche vorlegt.Nach Eintritt in die regionale Phase vor dem EPA kann jedoch im Zuge der Prüfung eine weitere Recherche durchgeführt werden (Vgl. EPA-Richtlinien C-VI, 8.5), sollten die Mängel behoben sein, die zu der Erklärung gemäss Art. 17 (2) PCT geführt haben.