BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS

Internal distribution code:
(A) [ ] Publication in OJ
(B) [ ] To Chairmen and Members
(C) [X] To Chairmen
(D) [ ] No distribution

Datasheet for the decision of 13 July 2007

Case Number: T 0377/03 - 3.5.01

Application Number: 98302286.4

Publication Number: 0874307

IPC: G06F 7/72

Language of the proceedings: EN

Title of invention:
Accelerated finite field operations on an elliptic curve

Applicant:
Certicom Corp.

Opponent:
-

Headword:
Elliptic curve cryptosystem/CERTICOM

Relevant legal provisions:
EPC Art. 84, 111(1), 123(2)

Keyword:
"Clarity (yes - after amendment)"
"Added subject-matter (no - after amendment)"
"Remittal (yes)"

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 0377/03 - 3.5.01

D E C I S I O N
of the Technical Board of Appeal 3.5.01
of 13 July 2007

Appellant: Certicom Corp.
200 Matheson Boulevard West,
Suite 103
Mississauga,
Ontario L5R 3L7 (CA)

Representative: Beresford, Keith Denis Lewis et al.
BERESFORD & Co.
16 High Holborn
London WC1V 6BX (GB)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 31 July 2002 refusing European application No. 98302286.4 pursuant to Article 97(1) EPC.**

Composition of the Board:

Chairman: S. Steinbrener
Members: R. R. K. Zimmermann
G. Weiss

Summary of Facts and Submissions

I. European patent application EP-A-0 874 307 (application number 98 302 286.4) relates to an elliptic curve encryption system.

II. The examining division refused the application at the end of oral proceedings; the only reason given in the decision in writing dated 31 July 2002 was that then claim 1 did not meet the requirements of Article 123(2) EPC.

III. The applicant (appellant) lodged an appeal against this decision, filing the notice of appeal and paying the appeal fee on 27 September 2002. A written statement setting out the grounds of appeal was filed on 29 November 2002.

IV. Following communications in writing, the appeal was finally set down for oral proceedings on 13 July 2007.

In the oral proceedings, the appellant filed an amended set of claims, claim 1 reading as follows:

"A method of operating an encryption/decryption unit (16) to determine a k-fold multiple kP of a point P on an elliptic curve defined over a finite field using points having x and y coordinates, the method steps performed by the encryption/decryption unit comprising; a) performing successive double and add operations on a pair of points that differ by P to obtain values of the x coordinates of a pair of points, one of which corresponds to kP, and the other of which corresponds to a point [k-1]P or [k+1]P that differs by P from kP;

said method characterised by the steps of:
b) substituting the x coordinate, x', of the one point kP into the elliptic curve to determine possible values, y', of the y coordinate of the point kP on the curve;
c) changing at least one of the possible points having coordinates x', y' representing the one point kP by either adding or subtracting P to said possible point to obtain a changed point having coordinates x", y";
d) comparing the changed point and said other point [k-1]P or [k+1]P to determine if said points correspond; and
e) determining as the y coordinate of the one point kP the possible value of y coordinate that provides a changed point that has coordinates that correspond to the other point."

V. According to the appellant's only request, the decision under appeal should be set aside and a patent be granted on the basis of claims 1 to 15 submitted at the oral proceedings.

VI. The matter was discussed with the appellant. Before the oral proceedings were closed, the decision was announced orally by the Chairman.

Reasons for the Decision

1. The appeal is admissible and allowable on the basis of the request filed at the oral proceedings on 13 July 2007.

2. The Board is satisfied that the request meets the claim requirements of the EPC. In compliance with the requirements of Article 84 EPC, the claim wording is clear and concise so that the scope of protection can be determined and the claimed invention can be examined for patentability.

3. Neither are there any objections under Article 123 (2) EPC.

The subject matter of the amended claims can be derived unambiguously and directly from the application, figures 2 , 3, and 4, and the corresponding parts of the description, in particular page 7, lines 5-7, page 8, lines 15-46, and page 11, lines 30-33 (all references relate to the A-publication).

The generalisations made in the claims do not broaden the invention beyond the technical teaching disclosed in the application as filed, and are thus admissible.

In particular, claim 1 defines a "double and add" algorithm in general terms, namely "performing successive double and add operations on a pair of points that differ by P", without indicating the arithmetic details given in original claim 1. The explicit limitation to such a specific algorithm is not necessary: Double-and-add methods on pair of points are already part of the prior art ("Montgomery method", see the application, page 4, lines 47-51); in such methods, the term "double and add" defines an iterative algorithm which is controlled by the bit values of the multiplication factor k in binary representation. The

present wording is sufficiently complete to define the essential features of this algorithm.

It is also not necessary to restrict claim 1 by specifying the finite field. The basis 2^m, although particularly convenient for digital processing, is not essential to the present invention (see application, page 2, lines 3 and 4) since other types of finite fields could be used as well without any substantial modification of the technical teaching disclosed in the application.

Claim 1 encompasses the alternative methods for computing the x- and y-coordinates of kP disclosed at page 8, lines 15 to 46. There are no objections to bring these methods together under a common definition.

It is noted that figure 4 displays some obvious writing errors for which there is no doubt how to correct them: the first step in figure 4 should read as " $\bar{x}$[(k-1)P];x′[kP]" as at page 8, line 37 f., and step 58 as "y of -kP" as at page 8, line 43 of the application. In the light of such corrections, the method of figure 4 for determining the y-coordinate is clearly consistent with the Montgomery method of figure 3 for computing kP. As generally explained at page 7, lines 1-7, adding a pair of points P_1, P_2 requires the x-coordinates of the points (only), but also the x-coordinate of P_1-P_2. The x-coordinates of (k-1)P and kP required in the method of figure 4 are the x-coordinates of P_1-P and P_1, respectively, provided in the last iteration (i=M) of figure 3.

In summary, the present claims meet the requirements of Article 123(2) EPC.

4. Since the examining division refused the application only for added subject matter, without addressing any substantive issues of patentability, the Board considers it necessary to remit the case to the examining division to continue the substantive examination on the basis of present claims 1 to 15.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the examining division for further prosecution.

The Registrar: The Chairman:

T. Buschek S. Steinbrener