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 31 October 2007

Case Number: T 1107/04 - 3.5.01

Application Number: 99961596.6

Publication Number: 1125206

IPC: G06F 12/14

Language of the proceedings: EN

Title of invention:
Secure memory management unit which uses multiple cryptographic algorithms

Applicant:
NXP B.V.

Opponent:
-

Headword:
Secure memory management / NXP

Relevant legal provisions:
EPC Art. 56

Keyword:
"Inventive step (no, obvious compromise)"

Decisions cited:
-

Catchword:
Cf. point 6 of the Reasons.

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 1107/04 - 3.5.01

D E C I S I O N
of the Technical Board of Appeal 3.5.01
of 31 October 2007

Appellant: NXP B.V.
High Tech Campus 60
NL-5656 AG Eindhoven (NL)

Representative: Pennings, Johannes
NXP Semiconductors
Intellectual Property Department
High Tech Campus 60
NL-5656 AG Eindhoven (NL)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 2 March 2004 refusing European application No. 99961596.6 pursuant to Article 97(1) EPC.**

Composition of the Board:

Chairman: S. Steinbrener
Members: K. Bumes
G. Weiss

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division to refuse European patent application No. 99961596.6 for lack of inventive step over

D10: US-A-5 081 675.

The appellant requests that the decision under appeal be set aside. He pursues the application on the basis of the claim set (claims 1 to 8) refused by the examining division. Claim 1 reads:

"1. A method by which an integrated circuit accesses second encrypted information stored in a second external memory (146), the second external memory (146) being external to the integrated circuit, the method comprising the step of using a second algorithm (94) to decrypt a first portion of the second encrypted information, the first portion of the second encrypted information including instructions for execution by a processor, the integrated circuit further accessing first encrypted information stored in a first external memory (46), the first external memory (46) being external to the integrated circuit, and the method comprising the following additional steps:

(a) when accessing a first portion of the first encrypted information, the first portion of the first encrypted information including data used during execution by the processor, then the following substep is performed:

(a.1) using a first algorithm (93) to decrypt the first portion of the first encrypted information;

the method additionally comprising the following step:

(b) when returning the first portion of the first

encrypted information to the first external memory (46), performing the following substep:

(b.1) using the first algorithm (93) to encrypt the first portion of the first encrypted information;

characterized in that the first algorithm (93) is less secure than the second algorithm (94)."

II. In an annex to summons, the Board asked what options the skilled person has, on the basis of common general knowledge, to protect more information than in D10 without adding excessive delay. Data security and processing speed were commonly known to be interrelated by the amount of information to be encrypted and by the complexity of the cryptographic algorithm used. Encrypting additional information by a less secure algorithm (as compared to the encryption already used in the system of D10) might be a compromise envisaged by the skilled person.

III. In response to the summons, the appellant has requested a decision according to the state of the file. He has informed the Board that he refrains from oral proceedings (initially requested on an auxiliary basis).

Reasons for the decision

1. *The invention*

The application as filed, and published as

A2: WO-A2-00/26791,

describes a method for managing memories in a secure manner, the method using a cryptographic algorithm to access (and decrypt) encrypted executable instructions stored in a memory, and using a less secure cryptographic algorithm to access encrypted data stored in another memory. Unlike instruction code, data is variable and therefore said to be less vulnerable to attacks. Consequently, sufficient data protection can be achieved by a less secure algorithm which may be less complicated and less time-consuming (A2, paragraph bridging pages 3 and 4; page 7, lines 13 to 16).

2. *Article 123(2) EPC - Admissibility of amendment*

Claim 1 as amended sets out from original claim 1 and has been generalised by replacing a structural term with a functional term: While the original version of the claim specifies that "the second algorithm is different than the first algorithm" (see A2, page 15, lines 13/14), the amended version requires the first algorithm to be "less secure" than the second algorithm.

The original description presents the use of a cryptographic algorithm with different keys as providing different levels of security (see A2, page 6, lines 16 to 27, and page 7, lines 11 to 16). The Board is therefore satisfied that the amendment does not extend beyond the content of the application as filed.

3. *Closest prior art*

3.1 According to D10: US-A-5 081 675, sensitive information (in particular executable code) can be stored (e.g. in memory RAMU-1) in a protected manner by scrambling the addresses of the memory locations containing the information (Figures 1 to 6; e.g. column 5, line 43 to column 6, line 63), and/or by scrambling the information bits themselves (Figures 7 and 8, column 19, line 62 to column 20, line 32).

Non-scrambled (i.e. unencrypted) information is stored in a second memory unit (e.g. RAMU-2, column 7, lines 3 to 14) and/or in regions of the first memory unit (column 14, lines 48 to 50; column 14, line 55 to column 15, line 32). Generally, no scrambling is assigned to subroutines, constants and variables which need to be accessed frequently (column 14, lines 55 to 66), because scrambling causes undesirable delays (column 7, lines 33 to 40; column 12, lines 41 to 45; column 19, lines 21 to 29; column 20, lines 29 to 32; column 23, claims 9 and 12).

3.2 Since the algorithms mentioned by D10 (column 6, line 4 to column 7, line 33; column 21, claim 4; column 23, claims 11, 15, 16; column 24, claim 20) use different keys "k" (column 6, lines 19 to 26 and line 64 to column 7, line 2; column 7, line 15 to column 8, line 10) but do not necessarily provide different levels of security, D10 does not anticipate the feature of using two algorithms of different security levels.

4. *Contribution to the closest prior art*

The Board concurs with the examining division (decision under appeal, point 2.1.2) and with the appellant (see two-part form of claim 1) in considering the use of algorithms of different security levels as a contribution over the system of D10.

5. *Technical effect of the contribution*

In contrast to the examining division (decision under appeal, point 2.1.3), the Board is convinced that the contribution solves a technical problem. By using algorithms of different strengths, the encryption of different types of information can be tailored to different security requirements in order to optimise the overall use of data processing resources (time, capacity, hardware, software). The technical problem may thus be formulated as how to increase data security with minimum burden on the data processing resources.

6. *Article 56 EPC - Inventive step*

6.1 The system of D10 protects at least instruction code while leaving other information (e.g. data variables) unprotected to avoid delays in data processing. The choice of encrypting or not encrypting information for storage reflects a skilled person's trade-off between security and speed. Providing security (by encrypting information) reduces performance (by introducing delays), and *vice versa*.

6.2 The critical question is what options the skilled person has to protect more information than in D10

without adding proportional delay. It is common knowledge that security and speed are interrelated by the volume of information to be encrypted and by the complexity of the cryptographic algorithm used. In general, securer algorithms entail higher complexity, with data volume and complexity translating into encryption time.

In fact, there are only three options:

(i) leave the unprotected information of D10 unprotected to avoid any delay;

(ii) fully protect the previously unprotected information of D10 and accept the resulting long delay; or

(iii) strike a balance between the degree of protection and the resulting delay.

6.3 In the Board's judgment, selecting any of these options does not involve an inventive step. The skilled person always contemplates protecting sensitive information and will protect such information once the cost (in terms of implementation and delays) is acceptable, and he will keep the cost acceptable by choosing a low-level encryption wherever that is sufficient for the type of data and suggested by the volume of data. This is a straightforward concept yielding only predictable results. It is an obvious compromise for a skilled person to accept some relatively simple protection for previously unprotected types of information in order to keep the associated delay at a minimum.

Therefore, the method of claim 1 does not involve an inventive step, contrary to the requirements of Articles 52(1) and 56 EPC.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

T. Buschek S. Steinbrener