Internal distribution code:

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

Datasheet for the decision of 3 July 2023

Case Number: T 0099/21 - 3.5.06

Application Number: 13731599.0

Publication Number: 2883186

IPC: G06F21/79, G06F21/62

Language of the proceedings: EN

Title of invention:
METHOD AND DEVICES FOR SELECTIVE RAM SCRAMBLING

Applicant:
Qualcomm Incorporated

Headword:
Selective RAM Scrambling/QUALCOMM

Relevant legal provisions:
EPC Art. 56, 84, 111(1), 112(1)(a)
RPBA 2020 Art. 11, 13(2)

Keyword:
Inventive step - (no)
Referral to the Enlarged Board of Appeal - (no)
Remittal - (no)
Amendment after summons - exceptional circumstances (no)
Claims - interpretation of ambiguous terms

Decisions cited:

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Case Number: T 0099/21 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 3 July 2023

Appellant: (Applicant)	Qualcomm Incorporated 5775 Morehouse Drive San Diego, CA 92121 (US)
Representative:	Bardehle Pagenberg Partnerschaft mbB Patentanwälte Rechtsanwälte Prinzregentenplatz 7 81675 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 25 September 2020 refusing European patent application No. 13731599.0 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	M. Müller
Members:	T. Alecu
	K. Kerber-Zubrzycka

Summary of Facts and Submissions

I. The appeal is against the decision of the Examining Division to refuse the application.

II. With the statement of grounds of appeal the Appellant requested that the decision of the Examining Division be set aside and that a patent be granted on the basis of a sole request, based on the auxiliary request 2 underlying the appealed decision, with a (minor) clarifying amendment.

III. That auxiliary request had been refused for lack of clarity, and for lack of inventive step starting from D1: US 2003/200451 A1.

IV. In a communication accompanying a summons to oral proceedings, the Board provided its provisional opinion in which it generally agreed with the conclusions of the decision under appeal.

V. With the letter of 14 March 2023, the Appellant filed a new auxiliary request. It also requested on an auxiliary basis that the case be remitted to the Examining Division for further prosecution on the basis of either the main or the auxiliary request together *"with [...] the ratio decidendi regarding the clarity issues"*.

VI. Oral proceedings were held as a videoconference on 3 July 2023. During the oral proceedings the Appellant filed an amended description, a new (second) auxiliary request and a request to refer a question to the Enlarged Board.

VII. The requests of the Appellant are therefore as follows:

1) to grant a patent on the basis of the set of claims filed with the grounds of appeal of January 26, 2021 (main request);

2) alternatively to remit the case to the Examining Division with the main request and the ratio decidendi regarding the clarity issues;

3) further alternatively to grant a patent on the basis of the set of claims according to the auxiliary request submitted with the letter filed on 14 March 2023;

4) further alternatively to remit the case to the Examining Division with the auxiliary request and the ratio decidendi regarding the clarity issues;

5) further alternatively to grant a patent on the basis of auxiliary request II submitted in oral proceedings before the Board;

6) further alternatively to remit the case to the Examining Division with the auxiliary request II and the ratio decidendi regarding the clarity issues;

7) to refer the following question to the Enlarged Board of Appeal:

"*If the specification is adapted in accordance with the new stricter appliance of the Guidelines, is it then still allowable to interpret a claim according to explicitly non claimed subject-matter?*".

VIII. Claim 1 of the main request defines:

A method for selective memory scrambling within a computing device (100) to efficiently protect data from pattern matching attacks, the method comprising:
adding tagging information to a data bus transaction (114), wherein the data bus transaction is an information transaction conducted over the data bus and wherein the tagging information identifies a content of the data bus transaction (114), wherein the tagging information added to the data is a content protection, CP, bit, which indicates whether the data bus transaction (114) includes protected content;
determining whether the data bus transaction (114) includes protected content based on the tagging information;
storing the data in a secure domain (124) of a memory (120) with applying a scrambling routine to the data in response to determining that the data includes protected content; and
storing the data in an unsecure domain (122) of the memory (120) without applying the scrambling routine to the data in response to determining that the data does not include protected content.

IX. Claim 1 of the auxiliary request defines:

A method for selective memory scrambling within a computing device (100) to efficiently protect data from pattern matching attacks, the method comprising:
adding tagging information to a data bus transaction (114), wherein the data bus transaction is an information transaction conducted over the data bus and wherein the tagging information identifies a content of the data bus transaction (114), wherein the tagging information added to the data is a content protection, CP, bit, which indicates whether the data bus

transaction (114) includes content that is to be protected;
determining whether the data bus transaction (114) includes protected content based on the tagging information;
storing the data in a secure domain (124) of a memory (120) with applying a scrambling routine to the data in response to determining that the data includes protected content, wherein the secure domain (124) is a domain of the memory (120) in which stored data is scrambled; and
storing the data in an unsecure domain (122) of the memory (120) without applying the scrambling routine to the data in response to determining that the data does not include protected content, wherein the unsecure domain (122) is a domain of the memory (120) in which stored data is not scrambled.

X. Claim 1 of the auxiliary request II differs from that of the first auxiliary request by specifying the entities performing the different steps as follows:

... the method comprising:
adding, by a bus controller (128), tagging information...
determining, by a memory controller (110), whether...
storing, by the memory controller (110), the data in a secure domain...
storing, by the memory controller (110), the data in an unsecure domain...

Reasons for the Decision

The application

1. The application relates to a method for selective scrambling/encryption of RAM data. It is explained (paragraph 2) that RAM scrambling uses less complex encryption methods for performance reasons. This reduced complexity, according to the application, could permit pattern matching attacks, i.e. attackers repeatedly writing known data into memory so as to be able to reverse engineer the encryption (n.b. since scrambling is effectively encryption and the described complexity difference is mostly a matter of degree, the Board will use this latter term throughout).

1.1 The application proposes to encrypt only the data that needs to be encrypted. This is said to neutralize pattern matching attacks (paragraph 25), presumably because data sent by the attackers is no longer encrypted, so there is no data available for use in the reverse engineering process (see end of paragraph 35).

2. The indication as to which data is to be encrypted is provided by adding tagging information for transactions over the communication bus; the tagging information may relate, according to the application, to the source or the content of the data (paragraphs 8 and 22). According to this information the memory controller encrypts the data, or not, when writing it, and decrypts it, or not, when reading it (paragraph 27). Three main embodiments are presented.

2.1 In the first one (that of figure 2), the tagging information contains the virtual machine identifier

(VMID) of the machine initiating the transaction. Data is encrypted or not depending on the VMID.

2.2 In the second one (depicted in figure 3), the tagging information contains the destination memory address. Data is encrypted if the destination address is in a secure domain, and not encrypted if it is in an unsecure domain.

2.3 In the third one (depicted in figure 4), the tagging information is a content protection (CP) bit. Paragraph 54 describing that embodiment states:
"The method 400 is similar to the methods described above, except that a computing device employing the method 400 may cause data within data bus transaction to be scrambled by setting a CP bit value instead of indicating a protected VMID or destination memory address. In an aspect, the computing device may include dedicated pins or connections on the bus to enable protection indicators for various components, such as processors, modems, etc. For example, a modem component may include a dedicated pin that enables data bus transactions from the modem to include a protected CP bit. In another aspect, components having dedicated pins may be configured to selectively set CP bit values for memory scrambling. For example, a component with a dedicated pin for setting protected CP bit values may transmit data bus transaction such that a memory controller may not scramble the transaction data.".

Clarity and claim construction

3. The Examining Division was of the opinion (decision point 5) that the
"*terms 'tagging information', 'protected content', 'secure domain', and 'unsecure domain' are vague and*

unclear, leaving a skilled person in doubt as to the meaning of the technical features to which they refer".

4. The Board agrees in part. It is unclear whether "*protected content*" means anything more than content that is to be protected, i.e. whether there is any content property that makes it "*protected content*". Likewise, it is unclear if the terms "*secure domain*" and "*unsecure domain*" mean anything more than that the data is stored therein in encrypted, respectively unencrypted form, for instance whether the domains are pre-defined and secured also by other security measures.

4.1 The Board takes the view that the intention is for "*protected content*" to mean only "*content that is to be protected*" and for "*secure domain*" and "*unsecure domain*" to define no more than domains in which data is stored in encrypted or unencrypted form, respectively.

5. This analysis was provided in the Board's communication accompanying the summons to oral proceedings (point 5.1), which also appears to correspond with the Appellant's submissions in its grounds of appeal (at point 2).

5.1 The Appellant agreed with the proposed claim interpretation in its letter of 14 March 2023 (B.I.2).

6. The Board concludes that claim 1 of the main request lacks clarity (Article 84 EPC).

6.1 Given, however, that the Appellant was willing to file clarifying amendments, which were indeed also filed as part of the auxiliary requests, the Board proceeds to

discuss inventive step of the main request on the basis of this interpretation.

7. Also the term "*tagging information*" was considered by the Examining Division to lack clarity.

7.1 In the claim, this term is first stated to "*[identify] a content of the data bus transaction*".

7.2 It is then characterised as a single bit which indicates whether the content is to be protected ("*wherein the tagging information added to the data is a content protection, CP, bit*"). The Board therefore considers the claim to define this term clearly as one bit indicating whether content needs to be protected.

7.3 As a single bit, however, it cannot *identify* the content (e.g. its type) beyond the fact that it needs to be protected or not.

8. The Appellant argued that the claim should be interpreted as specifying that the content protection bit is set based on the data content (see for instance letter of 14 March 2023, B.I.3). It referred to paragraph 3 of the application, stating:
"*determining whether the data to be stored in a memory includes protected content may include adding tagging information to data transmitted over a bus of the computing device identifying a source or content of the data, and determining the source or content of the transaction based on the tagging information*".
In the Appellant's view, "*these two alternatives – (1) source / (2) content – are equally described throughout the application documents*". The claims, however, related exclusively to the second alternative, where

the tagging information identified the content of the data, such as DRM (Digital Rights Management) content.

8.1 This was clear to the skilled person also from the name of the tagging information, i.e. content protection bit. The bit was set based on the content of the data rather than its source. The Appellant referred also to paragraph 29, which would make clear that the nature of data was identified for selective encryption. That paragraph states:
"using data tables for classifying data is provided as a non-limiting example of how the computing device processor or bus controllers may classify, identify, or reference data for purposes of selective RAM scrambling. For example, to identify the nature of data within a data bus transaction, the computing device, via the hypervisor, may determine the nature of a data bus transaction based on operating system calls or computing device elements used to transmit the data bus transaction to a memory."

8.2 Moreover, in paragraph 54, which contains a detailed discussion on the matter, setting the CP bit based on the nature of the data is presented expressly distinguished from setting it based on a VMID (see quotation above in 2.3). The correct claim interpretation therefore required that the CP bit was taken to be set based on its content rather than on the source ID.

8.3 Furthermore, in the adapted description, all embodiments other than the one of figure 4, paragraphs 54 and 55, were either removed or declared not to be part of the claimed matter. There was therefore no more room for an interpretation deviating from the embodiment disclosed in paragraphs 54 and 55.

9. The Board disagrees. The Appellant is correct to say that the application teaches that the tagging information can be defined based on the nature of the data, e.g. type of content.

9.1 However, the claim does not define that. The step of adding tagging information does not define how it is carried out. The name "Content Protection bit" does not indicate, let alone imply, that the content is analysed (or identified) in order to set that bit, but only that the content needs to be protected (see above points 4 and 5).

9.2 In the Board's view, the claim subsumes the alternative that the Content Protection bit is based on the hardware source. This is also consistent with the paragraphs cited by the Appellant. In paragraph 29, the nature of data transactions may be determined based on "*computing device elements*". Likewise paragraph 54 describes "*dedicated pins or connections on the bus to enable protection indicators for various components, such as processors, modems, etc.*". This is distinct from using a virtual source ID (VMID), as the Appellant submitted, but it does not exclude a setting based on the hardware source alone.

Request for remittal on the basis of the main request or of the auxiliary request "with the ratio decidendi on clarity"

10. The Appellant requests that the Board's decision be limited to its opinion on clarity but that a further discussion on inventive step is left to further prosecution by the Examining division.

10.1 The Examining Division decided, based on an interpretation corresponding to the Board's as explained above

(see the decision, points 3.2 to 3.2.1), that the main request lacked inventive step in view of D1. Since the auxiliary request is amended to clarify the claim language in conformance with that interpretation, the reasons for the decision apply to the first auxiliary request as well.

10.2 According to Article 11 RPBA 2020, the Board shall remit a case only if "*special reasons present themselves for doing so*". The Board sees no such special reasons, nor has the Appellant presented any.

10.3 According to Article 111(1) EPC, the Board shall examine the allowability of the appeal, i.e. whether, in view of the appellant's submissions, the decision under appeal must be set aside or amended. Normally, this implies an examination whether the reasons in the decision under appeal are correct or have been overcome by amendment. In the present case, the reasons concerning the question of inventive step still apply. Therefore, remitting the case without assessment of inventive step, as the Appellant effectively asked, would defeat the purpose of the present appeal proceedings.

10.4 The request for remittal is therefore rejected.

Inventive step

11. Document D1 (see abstract; figures 4 and 5; paragraphs 39 to 41) teaches a method of providing different levels of access to memory for different functional masters (e.g. a processor, paragraph 26). The bus controller transmits the read/write request together with the master ID to an access control function, which uses an access table to determine whether the requesting master has access to the requested memory address,

and if yes, whether the data should be encrypted/ decrypted (by an encryption engine) or left in clear.

12. The Examining Division was of the opinion (point 6.1 and 3.1 of the decision) that claim 1 differed from the teachings of D1 by "*unclear terms*", i.e "*secure*", "*unsecure*" domain, and "*protected content*", and by the definition of the tagging information as being "*a content protection bit*", which "*does not change the claimed subject-matter in any technically clear way*".

13. The Appellant argued in its statement of grounds of appeal (end of page 9) that in the application "*the addition of a content protection bit, which identifies the content, to the data allows to change the storage location and moreover also the way the data is stored (unscrambled in the unsecure domain vs. scrambled in the secure domain)*". In contrast (page 12 of the statement of grounds of appeal) "*it is clear to the person skilled in the art that document D1 describes a storage mechanism, which is based on the source of the data and not the content of the data (which is indicated by the content protection bit) as claimed*".

13.1 In its letter of reply, and in its submission during the oral proceedings, the Appellant further insisted that the claim differed from D1 in that the tagging information was based on data content (see discussion on claim construction above), unlike in D1, where it was based on the source ID.

13.2 It also submitted during the oral proceedings that in the application the tagging information was set at the sending side (based on content). This was also different from D1.

14. The Board does not find this argumentation convincing.

14.1 As already explained above, the Board does not read the claim to require that the Content Protection bit is based on content; it can also be based on the source, as in D1.

14.2 D1 also stores data in encrypted or unencrypted from, so in secure/unsecure domains as claimed, depending inter alia on the source ID.

14.3 The Board notes that D1 does not explicitly specify a content protection *bit*. However, the access control function of D1, which is part of the bus controller, provides an indication to the encryption engine whether the transmitted data must be encrypted or decrypted, although this is not explicitly specified. The Board regards as at least obvious, if not implicit, to provide such an indication by setting a bit value, which bit is then effectively a *"Content Protection bit*".

14.4 The Board further remarks that the claim does not specify where, or by which entity, the tagging information is added.

15. The Board therefore confirms the Examining Division's conclusion that the subject matter of claim 1 of the main request does not involve an inventive step in view of D1 (Article 56 EPC).

16. This applies to the claim 1 of the auxiliary request as well, which is in substance not different from that of the main request. The Appellant did not argue otherwise.

Auxiliary request II

17. This auxiliary request was filed during the oral proceedings, and its admittance is governed by Article 13(2) RPBA 2020. The Appellant justified its filing by the fact that it was only at the oral proceedings that the position of the Board had become clear, in particular the fact that the claim did not define which entity executed which steps. The amendments clarified that, and this should provide support for the Appellant's claim interpretation that the tagging information is based on the data content.

18. On the one hand, the Board notes that the Board's interpretation only confirmed the one in the decision of the Examining Division. This certainly does not constitute or indicate any exceptional circumstances.

19. On the other hand, the Board does not see, at least not prima facie, how the amendments could establish a different interpretation. The new claim defines that the tagging information is added by the bus controller (which is also the case in D1), but says nothing about how the content protection bit is determined.

20. Thus the Board does not admit this request (Article 13(2) RPBA 2020).

Request for referral to the Enlarged Board of Appeal (Article 112(1)(a) EPC)

21. The Appellant requested that the following question be referred to the Enlarged Board:
"*If the specification is adapted in accordance with the new stricter appliance of the Guidelines, is it then*

still allowable to interpret a claim according to explicitly non claimed subject-matter?".

21.1 The Appellant argued that the adapted description made clear that the only embodiment the claim could have meant to cover was that disclosed in figure 4 and paragraphs 54 and 55. This embodiment only described determination of the content protection bit based on content. The claim could therefore no longer be interpreted to cover an embodiment where the content protection bit is determined based on the source, because those were no longer claimed.

22. However, as the Board's interpretation relies on the claim wording and is consistent with paragraph 54 (see 9.1 and 9.2 above), an answer to this question is not required (see Article 112(1)a) EPC). The request for referral is therefore rejected.

Order

For these reasons it is decided that:

1. The appeal is dismissed.
2. The request to refer a question to the Enlarged Board of Appeal is rejected.

The Registrar: The Chairman:

L. Stridde Martin Müller

Decision electronically authenticated