

**Internal distribution code:**

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

**Datasheet for the decision  
of 15 November 2022**

**Case Number:** T 1626/20 - 3.5.05

**Application Number:** 15193346.2

**Publication Number:** 3021226

**IPC:** G06F12/14

**Language of the proceedings:** EN

**Title of invention:**

DATA STORAGE SYSTEM AND SECURE STORAGE DEVICE AND METHODS

**Applicant:**

Winbond Electronics Corp.

**Headword:**

Rearranged bits/WINBOND

**Relevant legal provisions:**

EPC Art. 56

RPBA 2020 Art. 12(8), 15(3), 12(4), 12(6)

**Keyword:**

Inventive step - (no)

Late-filed request - should have been submitted in first-  
instance proceedings (yes) - admitted (no)



**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 1626/20 - 3.5.05

**D E C I S I O N**  
**of Technical Board of Appeal 3.5.05**  
**of 15 November 2022**

**Appellant:** Winbond Electronics Corp.  
(Applicant) No. 8 Keya 1st Rd., Daya District,  
Central Taiwan Science Park,  
Taichung City, Taiwan. (TW)

**Representative:** Fuchs Patentanwälte Partnerschaft mbB  
Westhafenplatz 1  
60327 Frankfurt am Main (DE)

**Decision under appeal:** **Decision of the Examining Division of the  
European Patent Office posted on 17 January 2020  
refusing European patent application No.  
15193346.2 pursuant to Article 97(2) EPC.**

**Composition of the Board:**  
**Chair** A. Ritzka  
**Members:** E. Konak  
E. Mille

## **Summary of Facts and Submissions**

- I. The appeal is against the examining division's decision to refuse the application. The examining division decided that the main request and auxiliary requests 1 to 7 then on file did not meet the requirements of Article 56 and/or 123(2) EPC.
- II. The contested decision relied on the following documents for the objection under Article 56 EPC:  
  
D1: WO 2012/047200 A1  
D5: US 2013/101111 A1
- III. With the statement setting out the grounds of appeal, the appellant filed a new main request and new auxiliary requests 1 to 4. The new main request corresponds to auxiliary request 2 on which the contested decision is based. The appellant requested that the decision be set aside and that a patent be granted on the basis of one of these requests. It further requested oral proceedings as an auxiliary measure.
- IV. The board summoned the appellant to oral proceedings. In a communication pursuant to Article 15(1) RPBA 2020, it gave its preliminary opinion that the main request did not meet the requirements of Article 56 EPC and that the auxiliary requests were not admissible.
- V. The appellant did not reply in substance to the board's preliminary opinion. It merely informed the board that it would not attend the oral proceedings. The scheduled oral proceedings were thus cancelled.

VI. Claim 1 of the main request reads as follows:

A secure data storage device (120) for preventing tampering with data stored thereon, comprising:

a two-dimensional memory array (125) configured to store data, the array (125) comprising a predetermined number of data words, each data word comprising a set of bits, each data word associated with a single physical address in the memory array (125);

a key storage area (121) configured to store a key of the data storage device (120);

an address conversion unit (123) configured to convert a logical address to a corresponding physical address pointing to a location in the memory array (125), said converting based on a conversion function, a first portion of the key stored in the key storage area (121) and the logical address; and

a bit mixing unit (127) configured to mix bit values of an input data word to obtain a mixed word value, such that the mixed word value is a rearrangement of the bit values of the input data word, said mixing based on a one-to-one mapping function, a second portion of the key and the logical address of the input data word, wherein the mixed word value is stored in the physical address obtained from the logical address by the address conversion unit;

wherein said device is electrically connectable to a host to receive the logical address,

wherein the number of "0" values in the input data word is equivalent to the number of "0" values in the mixed word value, and the number of "1" values in the input data word is equivalent to the number of "1" values in the mixed word value.

Claim 1 of auxiliary request 1 reads as follows:

A secure data storage device (120) for preventing tampering with data stored thereon, comprising:

- an address interface (135) connected to a host (100) for receiving a logical address in a write command;

- a two-dimensional memory array (125) configured to store data, the two-dimensional memory array (125) comprising a predetermined number of data words, each data word comprising a set of bits, each data word associated with a single physical address in the two-dimensional memory array (125);

- a key storage area (121) configured to store a key of the data storage device (120);

- an address conversion unit (123) connected to the address interface (135) and configured to convert the logical address to a corresponding physical address pointing to a location in the memory array (125), said converting based on a conversion function, a first portion of the key stored in the key storage area (121) and the logical address;

- a mixing control unit (128) connected to the key storage area (121) and the address interface (135) and being configured to provide control parameters calculated based on a second portion of the key and the logical address in the write command; and

- a bit mixing unit (127) for receiving an input data word in the write command, connected to the mixing control unit (128) for receiving the control parameters, and configured to mix bit values of the input data word to obtain a mixed word value, such that the mixed word value is a rearrangement of the bit values of the input data word, said mixing based on a one-to-one mapping function, and the control parameters, wherein the mixed word value is stored in the corresponding physical address obtained from

converting the logical address by the address conversion unit;

wherein said device is electrically connectable to the host (100) to receive the logical address,

wherein the number of "0" values in the input data word is equivalent to the number of "0" values in the mixed word value, and the number of "1" values in the input data word is equivalent to the number of "1" values in the mixed word value.

Claim 1 of auxiliary request 2 differs from claim 1 of auxiliary request 1 as follows (with the additions underlined and the deletions ~~struck through~~):

A secure data storage device (120) for preventing tampering with data stored thereon, comprising:

an address interface (135) connected to a host (100) for receiving a logical address in a write command;

a two-dimensional memory array (125) configured to store data and have an efficient writing direction and an inefficient writing direction, the two-dimensional memory array (125) comprising a predetermined number of data words, each data word comprising a set of bits, each data word associated with a single physical address in the two-dimensional memory array (125);

a key storage area (121) configured to store a key of the data storage device (120), wherein the key comprises a first portion and a second portion;

an address conversion unit (123) connected to the address interface (135) and configured to convert the logical address to a corresponding physical address pointing to a location in the two-dimensional memory array (125), said converting based on a conversion function, at the first portion of the key stored in the key storage area (121) and the logical address;

a mixing control unit (128) connected to the key storage area (121) and the address interface (135) and being configured to provide control parameters calculated based on at the second portion of the key stored in the key storage area (121) and the logical address in the write command; and

a bit mixing unit (127) for receiving an input data word in the write command, connected to the mixing control unit (128) for receiving the control parameters, and configured to mix bit values of the input data word to obtain a mixed word value, such that the mixed word value is a rearrangement of the bit values of the input data word, said mixing based on a one-to-one mapping function, and the control parameters, wherein the mixed word value is stored in the corresponding physical address obtained from converting the logical address by the address conversion unit without requiring to write values in the inefficient writing direction;

wherein said device is electrically connectable to the host (100) to receive the logical address,

wherein the number of "0" values in the input data word is equivalent to the number of "0" values in the mixed word value, and the number of "1" values in the input data word is equivalent to the number of "1" values in the mixed word value,

wherein the two-dimensional memory array is initiated to store initial data comprising only bit values of "1" or only bit values of "0", and the secure data storage device allows writing additional data by changing a part of the bit values of the initial data in the efficient writing direction, as long as there is still a bit value which is not been changed.

Claim 1 of auxiliary request 3 differs from claim 1 of auxiliary request 2 as follows (with the additions underlined):

[...]

wherein the bit mixing unit (127) comprises a plurality of multiplexers (201-209), each multiplexer (201-209) having a predetermined number of input lines and output lines, each multiplexer (201-209) determining which input line to pass to which output line, each determination based on the control parameters, and

wherein the two-dimensional memory array is initiated to store initial data comprising only bit values of "1" or only bit values of "0", and the secure data storage device allows writing additional data by changing a part of the bit values of the initial data in the efficient writing direction, as long as there is still a bit value which is not been changed.

Claim 1 of auxiliary request 4 differs from claim 1 of auxiliary request 3 as follows (with the additions underlined):

[...]

wherein said device is electrically connectable to the host (100) including a random key generator to receive the logical address and the key,

[...]



## **Reasons for the Decision**

### 1. Procedural matters

This decision is taken in written proceedings without holding oral proceedings in accordance with Articles 12(8) and 15(3) RPBA. In reply to the summons to oral proceedings and the board's preliminary opinion, the appellant's representative stated that "neither he nor the applicant will attend the oral proceedings. As such, the oral proceedings are to be conducted without the attendance of the applicant or his representative" (see the appellant's letter dated 8 November 2022). The explicit declaration of the appellant's intention not to attend the scheduled oral proceedings is considered equivalent to a withdrawal of the request for oral proceedings, and the appellant is to be treated as relying only on its written case. In such a case, the board has discretion to cancel the oral proceedings and issue a decision in written proceedings (see Case Law of the Boards of Appeal, 10th edn., July 2022, III.C.4.3.2).

### 2. Main request

2.1 The contested decision found claim 1 of the then auxiliary request 2, which corresponds to claim 1 of the main request, to differ from D1 in that the number of "0" and "1" values in the input data word is respectively equivalent to the number of "0" and "1" values in the mixed word value. The examining division stated that this distinguishing feature of claim 1 had the effect and solved the problem of providing an alternative technique for fast data encryption. It then found the distinguishing feature not to involve an

inventive step since bit permutation was a common measure in the relevant art.

2.2 The appellant argued that there were additional distinguishing features of claim 1 over D1:

a) a key having a first portion stored in the key storage area and having a second portion

b) a bit mixing unit configured to mix bit values of an input data word to obtain a mixed word value such that the mixed word value is a rearrangement of the bit values of the input data word, this mixing based on a one-to-one mapping function, a second portion of the key and the logical address of the input data word

c) an address conversion unit configured to convert a logical address to a physical address pointing to a location in the memory array, this converting being based on a conversion function, a first portion of the key stored in the key storage area and the logical address

d) a two-dimensional memory array

2.3 Regarding feature a), the appellant argued that D1 teaches using a first key to scramble address information and then a second key to encrypt data. It argued that according to D1, [0022], the second key is a mixed key generated from data key 120 by the key mixer 124 and therefore by definition cannot be a portion of the same key as data key 120 (the first key), as required by the wording of claim 1.

This argument does not convince the board. D1 discloses various scenarios for the relationship of these two

keys. For example, D1, [0024] discloses another scenario in which the key used to scramble the "initial physical address" is a different key from the data key used for encryption. Therefore, it is not necessary in D1 that the encryption key be a mixed key generated from the first key. They can be two different keys. At the technical implementation level, it is doubtful whether using two different keys from a key storage or using two different portions of the same key would make any difference and, even if it did, the board cannot see any technical effect of this implementation detail.

2.4 Regarding feature b), the appellant argued that D1 discloses performing an XOR function or AES encryption, neither of which rearranges bit values as claimed. However, it still holds (in line with the examining division's assessment) that the technical effect of the bit rearrangement as claimed lies in providing an alternative encryption technique. The appellant contested this and argued that the real technical effects were explained in the application in, *inter alia*, paragraphs [0024] to [0027] of the description as published (which corresponds to page 6, line 23 to page 7, last line of the description as filed). This passage explains that using encryption methods such as RSA or AES changes the number of "0" bit values and "1" bit values after encryption and that, taking into consideration the characteristics of flash memory, it would be desirable to provide an encryption method which does not change the bit values of the data. Thus, this passage confirms the examining division's assessment that the distinguishing features provide an alternative encryption technique. The alternative encryption technique provided by the distinguishing features of claim 1 is a rearrangement of the bit values according to a transposition cipher, which would

have been an obvious choice for the skilled person looking for an alternative encryption technique.

- 2.5 Regarding feature c), the appellant argued that D1 scrambles an initial physical address to form a scrambled physical address and that this initial physical address is a physical address and thus cannot be considered a logical address, as also explained in D1, [0016]. These arguments are not technically convincing. To the contrary, if an "initial physical address" is scrambled, the scrambled address is no longer the physical address at which physical storage takes place and thus, by definition, is no longer a physical address but a logical address. D1's own terminology defined in paragraph [0016] for distinguishing between a "physical address" and a "virtual address" does not change this fact.
- 2.6 Regarding feature d), a memory chip normally consists of memory cells organised in the form of a matrix and is therefore a "two-dimensional [memory] array" as claimed. Therefore, this feature cannot be a distinguishing feature over D1. The feature "two-dimensional memory array" in claim 1 refers to 125 in Figure 1, which is a flash memory, one of the options for the storage device 106 in D1 (see D1, page 1, last full sentence).
- 2.7 Therefore, claim 1 of the main request does not involve an inventive step over D1 (Article 56 EPC).
3. Admittance of the auxiliary requests
- 3.1 In view of the primary object of the appeal proceedings to review the decision under appeal in a judicial manner, an appellant's appeal case must be directed to

the requests on which the decision under appeal was based (Article 12(2) RPBA). Any part of an appellant's appeal case which does not meet this requirement is to be regarded as an amendment unless the appellant demonstrates that this part was admissibly raised and maintained in the proceedings leading to the decision under appeal. Any such amendment may be admitted only at the discretion of the board. The appellant should provide reasons for submitting the amendments in the appeal proceedings (Article 12(4) RPBA).

3.2 In the current case, the contested decision is not based on auxiliary requests 1 to 4. These requests were not raised and maintained in the examination proceedings. Therefore, they are amendments within the meaning of Article 12(2) and (4) RPBA, which can only be admitted at the discretion of the board.

3.3 As reasons for submitting these amendments in the appeal proceedings, the appellant argued that the amendments were to address objections in the contested decision, were implicit in previous requests and/or did not constitute shifts toward subject-matter that had not been examined. However, these are not valid reasons for submitting amendments in the appeal proceedings. They instead indicate that the amendments should have been made in the examination proceedings (Article 12(6) RPBA).

3.4 Therefore, the board did not admit auxiliary requests 1 to 4 into the appeal proceedings.

**Order**

**For these reasons it is decided that:**

The appeal is dismissed.

The Registrar:

The Chair:



K. Götz-Wein

A. Ritzka

Decision electronically authenticated