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 E C I S I O N
of 18 June 1997

Case Number: T 0834/94 - 3.4.1

Application Number: 90300090.9

Publication Number: 0378306

IPC: H01L 23/58

Language of the proceedings: EN

Title of invention:
Secure integrated circuit chip with conductive field

Applicant:
General Instrument Corporation of Delaware

Opponent:
-

Headword:
-

Relevant legal provisions:
EPC Art. 56, 123(2)

Keyword:
"Main request: inventive step (no)"
"Auxiliary requests 1 to 3 satisfying Article 123(2) EPC"
"Remitted to first instance for further prosecution"

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 0834/94 - 3.4.1

D E C I S I O N
of the Technical Board of Appeal 3.4.1
of 18 June 1997

Appellant: General Instrument Corporation of Delaware
2200 Byberry Road
Hatboro
Pennsylvania 19040 (US)

Representative: Mackenzie, Andrew Bryan
Withers & Rogers
4 Dyer's Buildings
Holborn
London EC1N 2JT (GB)

Decision under appeal: Decision of the Examining Division of the European Patent Office posted 24 May 1994 refusing European patent application No. 90 300 090.9 pursuant to Article 97(1) EPC.

Composition of the Board:

Chairman: G. D. Paterson
Members: H. J. Reich
R. K. Schukla

Summary of Facts and Submissions

I. European patent application No. 90 300 090.9 (publication No. 0 378 306) was refused by a decision of the Examining Division in respect of Claim 1 filed on 28 September 1993.

Claim 1 filed on 28 September 1993 with letter dated 23 September 1993 reads as follows:

"1. An integrated circuit chip (10) containing a secure area (11) in which secure data is processed and/or stored, comprising a semiconductive layer (SC) containing diffusions (S, D) defining circuit element components; a first conductive layer (CN_1) coupled to the semiconductive layer to interconnect the components to thereby define circuit elements (14, 16, 17, M_1, M_2, M_n) for distributing, storing, processing and/or affecting the processing of secure data; and a second conductive layer (CN_2) overlying the circuit elements to thereby define a secure area (11) in which the circuit elements are shielded from inspection, and coupled to the circuit elements for conducting to the circuit elements a predetermined signal that is essential to an intended function of the circuit elements, whereby removal of the second conductive layer will prevent the predetermined essential signal from being provided to the circuit elements and thereby prevent the intended function, characterised by the shielded circuit elements further including

means (20) for generating clock signals and distributing said clock signals to the shielded circuit elements (14, M_1, M_2, M_n) that store and/or process secure data."

With the letter dated 23 September 1993 the appellant had filed further Claims 2 to 16 and requested on 8 March 1994 to delete Claims 14 to 16. Claims 2 to 13 are dependent on Claim 1.

II. The reason given for the refusal was that the subject-matter of Claim 1 did not satisfy the requirements of Articles 52 and 56 EPC having regard to document:

D1: EP-A-0 221 351.

The Examining Division took the following view:

The features in the pre-characterising part of **Claim 1** are disclosed in document D1. It is suggested in document D1 that "means for generating clock signals" may be provided in a non-secure region; see D1 column 7, lines 5 to 17. Thereby it is implicit that "means for distributing said clock signals" are also provided. The objective problem consists in additionally shielding the means for generating and distributing the clock signals from external inspection. Since such a need would occur on the demand of a customer using a particular layout wherein clock signals represent information that required protection, the problem in itself is not inventive. Once the problem becomes apparent, its solution is obvious for an expert, since he only needs to extend the second conductive layer (F) accordingly in the circuit disclosed in document D1.

III. The appellant lodged an appeal against this decision, and with the grounds of appeal filed on 3 October 1994, maintained Claims 1 to 13 filed on 28 September 1993 as main request and filed new Claims 1 forming the basis of auxiliary requests 1, 2 and 3, respectively.

Claim 1 of **auxiliary request 1** reads as follows:

"1. An integrated circuit chip (10) containing a secure area (11) in which secure data is processed and/or stored, comprising a semiconductive layer (SC) containing diffusions (S, D) defining circuit element components; a first conductive layer (CN_1) coupled to the semiconductive layer to interconnect the components to thereby define circuit elements (14, 16, 17, M_1 M_2, M_n) for distributing, storing, processing and/or affecting the processing of secure data; and a second conductive layer (CN_2) overlying the circuit elements to thereby define a secure area (11) in which the circuit elements are shielded from inspection, and coupled to the circuit elements for conducting to the circuit elements a predetermined signal that is essential to an intended function of the circuit elements, whereby removal of the second conductive layer will prevent the predetermined essential signal from being provided to the circuit elements and thereby prevent the intended function, characterised by the shielded circuit elements further including

means (20) for generating clock signals and distributing said clock signals to the shielded circuit elements (14, M_1, M_2, M_n) that store and/or process secure data,

a memory (M) having a plurality of memory locations, with a predetermined location being for the storage of unalterable secure data;

memory control logic circuit (38) coupled to the memory and an address bus (46) for causing data to be stored in locations of the memory indicated by address signals provided on the address bus;

a fuse element (42) having an initial state and an irreversibly altered state:

means (44) coupled to the fuse element for irreversibly altering the state of the fuse element in response to a predetermined control signal (48); and

a decoder (40) coupled to the fuse element, the memory control circuit and the address bus for monitoring the state of the fuse element and said address signals, and for preventing the memory control circuit from causing data to be stored in the predetermined memory location after the state of the fuse element has been altered irreversibly whenever the predetermined memory location is indicated by an address signal on the address bus."

IV. In a communication preparing for oral proceedings, the Board informed the appellant of its provisional view that Claim 1 of the main request did not appear to satisfy Article 56 EPC; and expressed doubts that Claims 1 of auxiliary requests 1, 2 and 3 are allowable under Article 123(2) EPC, on the basis that there is no disclosure in the original description that the circuit disclosed in Figure 8 with the corresponding description (auxiliary request 1) or the circuit disclosed in Figure 9 with the corresponding description (auxiliary requests 2 and 3) - both such circuits including a "fuse element" - shall be combined with the clock means as claimed in original claim 24. Original claim 24 is referred back via claim 23 to claim 1, but not to original claims 9, 13 or 14 (which include a "fuse element").

V. Oral proceedings were held on 18 June 1997, at the end of which the appellant requested that the decision under appeal be set aside and a patent be granted on the basis of one of the requests as set out in paragraph III above.

VI. In support of his requests the appellant argued essentially as follows:

(a) Document D1 representing the technical starting point to the present invention, teaches in column 4, lines 15 to 20 against moving clock means into the secure area of the chip. In a continuous etch step described in document D1 for removing protective second conductive layer (F) within area II, conductors L1 in area I are simultaneously destroyed (D1, column 5, lines 1 to 29). Hence, in the prior art the clock means are disabled before protective layer F is removed, so that a skilled person would not move the known clock means under the protective layer F. After removal of layer F, clock means, if provided in area II, would be accessible, and would not be disabled and thereby degrade the security of the circuit chip. The invention aims at improving the security of the circuit chip. This problem is solved by including clock means in the shielded circuit elements of the chip. When the clock means are provided within the secure area of the chip, it is impossible to manipulate them, in particular to change the clock period and to thereby influence the functioning of the circuit. A shielded clock means is nowhere disclosed in the cited documents and is not obvious to a skilled person.

(b) The provision of clock means **and** a fuse element

within secure area 11 is disclosed in the application in suit as originally filed (although such combination is not disclosed in the original claims). The description on page 5, lines 20 to 24 reads: "Within the secure area 11, the **chip 10 defines** the following circuit elements: a microprocessor 14 for processing secure data, a plurality of memories M_1, M_2, M_n for storing secure data, a secure data bus 16, a secure address bus 17, transfer logic circuits 18, and **secure clock and power control circuits** 20". The original description at page 11, line 27 to page 12, line 5 discloses: "It is critically important that secure data stored in the chip 10 during formation of a product that includes the chip not be modified after the storage of such secure data. To accomplish this purpose **chip 10 includes** a system for preventing the alteration of secure data stored in a predetermined memory location. Alternative embodiments of such prevention system are shown in Figures 8 and 9". Figures 8 and 9 clearly disclose a **fuse element and a fuse altering device** (emphasis added by the Board).

VII. At the conclusion of the oral proceedings, the decision was announced that the decision of the Examining Division is set aside and that the case is remitted to the Examining Division for further examination and prosecution on the basis of auxiliary request 1.

Reasons for the Decision

1. *Main request - Claim 1 - inventive step*

1.1 From the closest prior art disclosed in document D1 there is known in the wording of Claim 1 of the main request:

"An integrated circuit chip containing a secure area (see D1, II and III in Figure 1) in which secure data is processed and/or stored, comprising a semiconductive layer (S in Figure 1) containing diffusions defining circuit element components; a first conductive layer (L) coupled to the semiconductive layer to interconnect the components to thereby define circuit elements (D1, column 2, lines 44 to 46) for distributing, storing, processing and/or affecting the processing of the secure data (column 4, lines 27 to 35); and a second conductive layer (F in Figure 1) overlying the circuit elements to thereby define a secure area (II, III) in which the circuit elements are shielded from inspection (column 5, lines 1 to 9), and coupled (via K in Figure 1), to the circuit elements for conducting to the circuit elements a predetermined signal that is essential to an intended function of the circuit elements (column 6, lines 18 to 22), whereby removal of the second conductive layer (F) will prevent the predetermined essential signal from being provided to the circuit elements and thereby prevent the intended function (column 6, lines 43 to 47 in combination with column 5, lines 9 to 29) characterised by the ... circuit elements further including means for generating clock signals and distributing said clock signals to the shielded circuit elements that store and/or process secure data (column 7, lines 10 to 17)".

1.2 Starting from document D1, the objective problem underlying the invention as claimed in Claim 1 of the main request is - in line with the appellant's submission according to paragraph VI-(a) above - to improve the security of an integrated circuit chip. In the Board's view, such technical aim lies within the normal development of prior art, so that the definition of the objective problem does not contribute to an inventive step in the subject-matter of Claim 1.

1.3 According to the wording of the characterising part of Claim 1 the above problem is solved in that the means for generating and distributing clock signals are included in the "shielded" circuit elements.

1.4 Clock means are known to be circuit elements which are basically necessary for the functioning of the circuit on the chip; see document D1, column 4, lines 15 to 20. Furthermore, document D1 teaches that second conductive layer (F) prevents access to underlying circuit elements. Hence, a skilled person is able to derive from document D1 that by placing clock means below the second conductive layer (F) an analysis of the working of the clock means and of the overall functioning of the chip circuit can be prevented. In view of such a foreseeable advantage a skilled person has a clear technical incentive to displace the clock means from area I to secure areas II and III to improve the security of the integrated circuit chip.

1.5 The appellant's submission in paragraph VI-(a) above can be followed only to the extent that the circuitry of the clock means would become accessible with regard to its geometrical design when layer (F) is etched away. In the same way, the etching step would also provide access to the pattern of the other shielded circuit elements within the secure area. However, the skilled person learns from document D1, column 6,

lines 18 to 22 that layer (F), as in the subject-matter claimed in Claim 1, supplies a signal to the circuit elements within the secure area that is essential to their intended functioning, in particular a voltage which serves as power supply. Therefore, the skilled person can easily foresee that the removal of layer (F) removes power from all shielded circuits; see also the published description of the present application, column 6, lines 33 to 42, and column 7, lines 40 to 56. Hence, contrary to the appellant's submission in paragraph VI-(a) above, when layer (F) is etched away, the clock means are disabled as well so that an unauthorised access to the functioning of the clock means would not be possible. Moreover, one and the same technical measure cannot improve and degrade the security of the chip at the same time. The description of the present application is totally silent about any particular effect resulting from shielded clock means.

1.6 For the reasons set out above in paragraph 1.1 to 1.5, Claim 1 of the main request does not involve an inventive step and is not allowable pursuant to Articles 52(1) and 56 EPC. Claims 2 to 13 fall because of their dependence on Claim 1.

2. *Auxiliary requests 1, 2 and 3 - Article 123(2) EPC*

2.1 The original description at page 5, lines 20 to 24 clearly discloses that chip 10 incorporates within its secure area (11) clock circuits 20 for generating and distributing clock signals. On page 11, line 27 to page 12, line 5 in combination with Figures 8 or 9 and their related description, it is disclosed that **chip 10** includes within the shielded circuit elements a fuse element and means coupled to the fuse element for irreversibly altering their state. The description of the preferred embodiments as originally filed

consistently distinguishes between the protection of secure data from **inspection and reading out** of such data, on the one hand, and from **alteration and modification** of such data, on the other hand (see for example page 5, line 24 to page 6, line 3). The immediately preceding passage (already quoted in VI-(b) above) at page 5, lines 20 to 24 states that "the chip 10" (of Figure 1) defines inter alia a secure clock circuit, and the description with reference to Figure 1 (as well as Figures 2 to 6) describes how the secure circuit elements (including the clock circuit) are shielded from **inspection and reading out**.

The original description at page 11, line 27 to page 12, line 5 (already quoted at VI-(b) above) emphasises that secure data stored in "the chip 10" should not be **modified** after storage of such data, and explains that "the chip 10", which has previously been described with reference to Figure 1 as including a clock circuit, also **includes** a system for preventing the **alteration** of secure data - such a prevention system being described with reference to Figures 8 and 9 as including inter alia a fuse element. In other words, the systems of Figures 8 and 9 are described as being included in the chip 10 of Figure 1 which includes the clock circuit. This is consistent with the passage at page 5, line 24 to page 6, line 3, which states that "the chip 10 ... may contain any mixture of circuit elements wherein secure data is to be either protected against unauthorised attacks of reading out or modification of secure data ...".

In the Board's view, the original description of the preferred embodiments discloses that the chip 10 includes the clock circuit 20 within the secure area, and also includes as shielded circuit elements a fuse element and means coupled to the fuse element, as set out in the claims of the auxiliary requests.

2.2 For the above reasons Claims 1 of auxiliary requests 1, 2 and 3 are held to satisfy Article 123(2) EPC.

3. The subject-matter of Claims 1 of the appellant's auxiliary requests has not yet been examined by the Examining Division with regard to all the other requirements of the EPC. For this reason, the Board exercises its power under Article 111(1) EPC to remit the case to the first instance for further examination and prosecution on the basis of auxiliary request 1.

Order

For these reasons it is decided that:

1. The decision of the Examining Division is set aside.

2. The case is remitted to the Examining Division for further examination and prosecution on the basis of auxiliary request 1.

The Registrar: The Chairman:

M. Beer G. D. Paterson