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) [ ] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 16 February 2011

Case Number: T 1211/09 - 3.5.06

Application Number: 04017172.0

Publication Number: 1560110

IPC: G06F 7/72

Language of the proceedings: EN

Title of invention:
Multiple-word multiplication-accumulation circuit and Montgomery modular multiplication-accumulation circuit

Applicant:
Fujitsu Semiconductor Limited

Opponent:
-

Headword:
Montgomery modular MAC circuit/FUJITSU

Relevant legal provisions:
EPC Art. 123(2)

Relevant legal provisions (EPC 1973):
-

Keyword:
"Amendments - added subject matter (yes, main and 1st, 2nd and 3rd auxiliary requests)"

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 1211/09 **-** 3.5.06

D E C I S I O N
of the Technical Board of Appeal 3.5.06
of 16 February 2011

Appellant: Fujitsu Semiconductor Limited
2-10-23 Shin-Yokohama
Kohoku-ku, Yokohama-shi
Kanagawa 222-0033 (JP)

Representative: Seeger - Seeger - Lindner
Partnerschaft Patentanwälte
Paosostraße 95
D-81249 München (DE)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 9 February 2009 refusing European patent application No. 04017172.0 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman: D. H. Rees
Members: A. Teale
C. Heath

Summary of Facts and Submissions

I. The appeal is against the decision by the examining division, posted on 9 February 2009, to refuse European patent application 04017172.0 on the basis that claim 1 according to the then main and auxiliary requests set out a result to be achieved, but not the features that were necessary to achieve the result, and was thus unclear, Article 84 EPC 1973.

II. Claim 1 as originally filed read as follows:

"A multiple-word multiplication-accumulation (MAC) circuit that performs MAC operation on given input values each supplied as multiple-word data, comprising: a memory providing storage for a plurality of multiple-word data; a MAC operator having multiplicand and multiplier input ports with different bit widths to calculate a sum of products of the multiple-word data read out of said memory; and a plurality of registers to supply the multiple-word data to said MAC operator, wherein the amount of the data supplied in each clock cycle is adjusted such that total amount of data consumed and produced by said MAC operator in one clock cycle will be equal to or smaller than maximum amount of data that said memory can transfer in one clock cycle".

The claims as originally filed also comprised a further independent apparatus claim 4.

III. In a notice of appeal received on 7 April 2009 the appellant requested that the decision be set aside and

a patent granted, the appeal fee being paid the same day.

IV. With a statement of grounds of appeal received on 19 May 2009 the appellant filed a replacement set of amended claims.

V. With a letter received on 27 July 2009 the appellant filed another replacement set of amended claims.

VI. In a letter received on 24 June 2010 the appellant made an auxiliary request for oral proceedings.

VII. In an annex to a summons to oral proceedings the board gave its preliminary opinion on the appeal, stating *inter alia* that it understood that the appellant was seeking grant of a patent based on the following description and figures.

Description:
pages 1 to 7 and 9 to 47 as originally filed, received by the EPO on 24 July 2004, and page 8 as filed with the letter dated 19 December 2008, received on the same day.

Figures:
sheets 1 to 11 as originally filed, received by the EPO on 24 July 2004.

The board questioned *inter alia* whether the subject-matter of claim 1 satisfied Article 123(2) EPC regarding added subject-matter. The board also stated that any amendments should be submitted at the latest one month before the date of the oral proceedings.

VIII. With a letter received on 17 January 2011 the appellant filed four sets of amended claims according to a main and first, second and third auxiliary requests. The appellant requested grant of a patent on the basis of the description and figures as set out in the annex to the summons to oral proceedings and the claims according to one of the main or first, second or third auxiliary requests.

IX. Oral proceedings before the board were held on 16 February 2011 at which the appellant requested that the decision under appeal be set aside and that a patent be granted according to the main request, or any of the auxiliary requests 1 to 3, all filed with the letter of 17 January 2011.

X. At the end of the oral proceedings the board announced its decision.

XI. Claim 1 according to the main request reads as follows:

"A multiple-word multiplication-accumulation (MAC) circuit that performs MAC operation on given input values each supplied as multiple-word data, comprising: a memory (11) providing storage for a plurality of multiple-word data; a MAC operator (12) having multiplicand (a) and multiplier input (b) ports with different bit widths, getting MAC operator inputs (a, b, c, d) to calculate a sum of products (axb+c+d) of the multiple-word data (a, b, c) read out of said memory (11) and output data (d) of said MAC operator (12) which in addition produces an output value (e); and a plurality of registers (13, 14, 15, 16, 17) to

supply the multiple-word data (a, b, c) from said memory (11) and output data (d) from said MAC operator (12) itself, to said MAC operator (12) and to buffer and transfer said output value (e) from said MAC operator (12) to said memory (11), wherein said MAC operator (12) being adapted such that the amount of the data supplied in each clock cycle is adjusted such that the total amount of data in form of the multiplier input (b) and other input (c) than the multiplicand input (a) from said memory (11) consumed and produced as output value (e) by said MAC operator (12) in one clock cycle will be equal to or smaller than maximum amount of data that said memory (11) can transfer in one clock cycle."

The claims according to the main request also comprise an independent method claim 7.

XII. Claim 1 according to the first auxiliary request reads as follows:

"A multiple-word multiplication-accumulation (MAC) circuit that performs MAC operation on given input values each supplied as multiple-word data, comprising: a single-port memory (11) providing storage for a plurality of multiple-word data, the single-port having a first bit width; a MAC operator (12) having multiplicand and multiplier input ports to calculate a sum of products of the multiple-word data read out of said single-port memory (11), the multiplicand input having a second bit width, the multiplier having a third bit width which is different from said second bit width, the second bit width being larger than the third bit width; characterized by a plurality of registers

(13, 14, 15) each for storing a part of the multiple-word data stored in said single-port memory (11) as an input value to be supplied to said MAC operator (12), the plurality of registers (13, 14, 15) including a first register (13), a second register (14) and a third register (15), the second register (14) having more bits than the third register (15), an input of the first register (13) having the first bit width, and the output of the first register (13) having the second bit width, an input of the second register (14) having the first bit width, an output of the second register (14) having the third bit width, an input of the third register (15) having the first bit width, an output of the third register (15) having the third bit width; a fourth register (16) for storing an output value to be used in next MAC operation; and a fifth register (17) for writing an output of said MAC operator to the single-port memory when an amount of the output of said MAC operator reaches the first bit width, an input of the fifth register (17) having the third bit width, and an output of the fifth register (17) having the first bit width."

XIII. Claim 1 according to the second auxiliary request adds the following to claim 1 of the first auxiliary request:

"wherein a sum in bit width of an output of the second register (14), an output of the third register (15), and an input of the fifth register (17) is equal or less than the first bit width, and wherein the outputs of the second register and third register arrive at the MAC operator simultaneously."

XIV. Claim 1 according to the third auxiliary request further adds:

"and wherein said MAC operator (12) being adapted such that the amount of the data supplied in each clock cycle is adjusted such that total amount of data consumed (b+c) and produced (e) by said MAC operator (12) in one clock cycle will be equal to or smaller than maximum amount of data that said single-port memory (11) can transfer in one clock cycle."

Reasons for the Decision

1. *Admissibility of the appeal*

In view of the facts set out at points I to IV above, the appeal is admissible.

2. *Procedural issues*

2.1 *The appellant's submission received on 27 July 2009*

This submission was received after expiry of the time limit for filing the grounds of appeal and thus constitutes an amendment to the appellant's case, Article 13(1) RPBA (OJ EPO 2007, 536). Under the circumstances, taking into account in particular the complexity of the new subject-matter submitted, the state of the proceedings and the need for procedural economy, the board decided to exercise its discretion to admit these amendments.

2.2 *The appellant's submission received on 17 January 2011*

This submission, concerning a further amendment to the appellant's case, Article 13(1) RPBA, arrived one day after the final date (16 January 2011) set by the board for submitting any amendments to the application prior to the oral proceedings. However under the circumstances, taking into account in particular the complexity of the new subject-matter submitted, the state of the proceedings and the need for procedural economy, the board likewise decided to admit this amendment.

3. *The context of the invention*

3.1 The invention relates to a multiplication-accumulation (MAC) circuit suitable for execution of modular multiplication and accumulation according to the Montgomery algorithm used, for instance, in cryptography. The circuit carries out a sum of products calculation of the form

$$(d,e)=(a \times b) + c + d$$

where "d" and "e" represent the upper bits and lower bits, respectively, of the result obtained at each iteration, "d" being fed back as an input for use in the next iteration, thus carrying out accumulation. The input values "a", "b" and "c" are parts of multiple-word variables read from a memory. The description refers to "a" as the "multiplicand" and to "b" as the "multiplier"; see page 11, lines 18 to 22. The calculation is implemented as an algorithm having a nested double loop structure; see page 4, line 14, to

page 5, line 18, of the description. In the outer loop a new value of "a" is read from memory, whilst in the inner loop (lines 1.4 to 1.10 of the algorithm) the value of "a" remains the same and only the values of "b" and "c" change.

3.2 The invention concerns a MAC circuit comprising a MAC operator, which carries out the above calculations, associated registers for the input and output variables and a memory. The amount of data consumed and produced by the MAC operator in one clock cycle has been a matter of debate in these appeal proceedings. The application describes embodiments using single-ported memory, meaning that "a", "b", "c" and "e" values must all pass via the same port to and from the memory; specifically in, for example, figures 1, 2, 6 and 7 and the description from page 11, line 5, to page 24, line 5, and from page 31, line 3, to page 36, line 5. Other embodiments (see, for example, figure 9 and the description, page 39, line 7, to page 41, line 18) concern multi-port memories, meaning that "a", "b", "c" and "e" values may pass via different ports to and from the memory. The debate has focused on the embodiments in figures 1, 2, 6 and 7 comprising a single-port memory.

3.3 In the case of the embodiment shown in figure 1, each of the input values "a", "b" and "c" is read from a memory 11 and stored in a separate register (13, 14 and 15, respectively) before being fed to the MAC operator 12, which performs the calculation itself. As to the outputs of the MAC operator, output "d" is stored in register 16 before being fed back as an input to the MAC operator, and output "e" is stored in register 17

before being written to memory. The memory offers a data transfer speed of one word (1W) per clock cycle; see page 11, lines 14 to 17. The lengths of "a", "b", "c" and "e" as fed to or received from the MAC operator are 3W, W/3, W/3 and W/3, respectively. In the inner loop, W/3 "b" bits and W/3 "c" bits are read in by the MAC operator and W/3 "e" bits are written by the MAC operator in every clock cycle. This means that the inner loop runs at a data transfer speed of W/3 + W/3 + W/3 = 1W per cycle. As the memory allows a data transfer speed of 1W per clock cycle, it follows that the inner loop runs at the same data transfer speed as the memory. The skilled person would however realize that the outer loop would also require data transfers to take place, namely to transfer new "a" values to register 13. When this occurs the MAC operator will have to wait for the memory to catch up, meaning that overall the total amount of data consumed and produced by the MAC operator in one clock cycle will be greater than the maximum amount of data that the memory can transfer in one clock cycle. The board notes that on this analysis this purported "embodiment" does not satisfy the independent claims as originally filed, nor does it achieve the goal of the invention as stated repeatedly in the application (see page 13, lines 7 to 13, page 35, line 25, to page 36, line 5, and page 45, line 25, to page 46, line 4) that "the amount of data to be supplied in each clock cycle is adjusted such that [the] total amount of data consumed and produced by [the] MAC operator in one clock cycle will be equal to or smaller than [the] maximum amount of data that the memory can transfer in one clock cycle." (Emphasis added by the board.) There is, however, no disclosure in the application that what is achieved, balancing the

inner loop alone and the memory speed, should be taken as the actual or even an alternative goal of the invention.

3.4 Another embodiment, shown in figure 2 and explained in the timing diagrams shown in figures 6 and 7, does however satisfy the independent claims as originally filed. It concerns two MAC operators connected in series. The structure of the circuit differs from that of the figure 1 in that result values "E" are not written to memory but instead are fed to an input of the second MAC operator 121. For the purposes of this decision only the operation of the first MAC operator 111 need be considered. Each of the input values "A", "B" and "C" is read from a memory and stored in a separate register (112, 113 and 114, respectively) before being fed to the first MAC operator 111. As to the outputs of the first MAC operator, output "D" is stored in register 115 before being fed back as an input, and output "E" is stored in register 124 before being fed to the second MAC operator 121. A word (W) is defined as being 32 bits (see page 26, line 9), while the memory access width is 64 bits i.e. 2W (see page 18, line 26, to page 19, line 2). The description also states (at page 35, line 26, to page 36, line 1), as pointed out by the appellant, that the MAC operator produces three 64-bit memory reads and one 64-bit memory write within a four-clock period. Thus the board agrees with the appellant that the memory shown in figure 2 offers a data transfer speed of 64 bits, i.e. 2W per clock cycle. In this case in the inner loop 16 "B" bits (i.e. W/2) and 16 "C" bits (i.e. W/2) are read in by the MAC operator and 16 "E" bits (i.e. W/2) are written by the MAC operator in each clock cycle. Thus

the inner loop runs at 16 + 16 + 16 = 48 bits (i.e. 1.5W) per clock cycle. As the memory allows a data transfer speed of 64 bits (i.e. 2W) per clock cycle, the inner loop runs below the transfer speed provided by the memory. The skilled person would understand that the remaining memory access capacity of 16 bits (i.e. 0.5W) per clock cycle would be occupied by fetching "A" from the memory in the outer loop.

3.5 According to both independent claims as originally filed and the description (see page 13, lines 7 to 13, page 35, line 25, to page 36, line 5, and page 45, line 25, to page 46, line 4), the total amount of data supplied in each clock cycle is adjusted such that total amount of data consumed and produced by the MAC operator in one clock cycle is equal to or smaller than the maximum amount of data that the memory can transfer in one clock cycle. Put another way, the MAC operator never has to wait for the memory. The skilled person would have understood the total amount of data consumed and produced by the MAC operator in one clock cycle to include both the inner and outer loops of the algorithm and thus to include the reading of variables "a", "b" and "c" (or "A", "B" and "C") from memory, as well as the writing of the result "e" (or "E") to memory. As is stated in the description, and has been relied upon by the appellant, in the embodiment shown in figure 2 the MAC operator produces three 64-bit memory reads (i.e. "A", "B" and "C") and one 64-bit memory write (i.e. the result "E") within a four-clock period. In other words, in the application as originally filed the references to the total amount of data consumed and produced by the MAC operator in one clock cycle included not only the inner loop but also the outer loop of the

calculation algorithm. This embodiment satisfies the associated condition.

4. *Added subject-matter, Article 123(2) EPC*

4.1 *Main request*

4.1.1 Claim 1 according to the main request essentially sets out a multiple-word multiplication-accumulation (MAC) circuit comprising a memory, a MAC operator having multiplicand and multiplier ports with different bit widths and a plurality of registers for storing the data from memory, output data to be fed back to the MAC operator and output data to be written to memory. The last paragraph of claim 1 sets out the following limitation "wherein said MAC operator (12) being adapted such that the amount of the data supplied in each clock cycle is adjusted such that the total amount of data in form of the multiplier input (b) and other input (c) than the multiplicand input (a) from said memory (11) consumed and produced as output value (e) by said MAC operator (12) in one clock cycle will be equal to or smaller than maximum amount of data that said memory (11) can transfer in one clock cycle."

4.1.2 Bearing in mind that reference signs shall not be construed as limiting the claim, Rule 29(7) EPC 1973, the board understands the "multiplier input (b)", in the light of the description and figures, to refer to input "b" to the MAC operator 12 in figure 1 or input "B" to the MAC operator 111 in figure 2. Likewise the board understands the expression "other input (c) than the multiplicand input (a)", in the light of the description and figures, to refer to input "c" to the

MAC operator 12 in figure 1 or input "C" to the MAC operator 111 in figure 2. In view of the reference earlier in the claim to the MAC operator producing an "output value" as well as "output data", said "output data" forming an input to the MAC operator, the board understands the expression "output value (e)" to refer to input "e" to buffer 17 in figure 1 or input "E" to register 124 in figure 2.

4.1.3 Interpreted in this manner, the limitation in the last paragraph of claim 1 states that the amount of data supplied to the MAC operator at the "b" and "c" (or "B" and "C") inputs plus the amount of data produced by the MAC operator at the "e" (or "E") output in each clock cycle is less than or equal to the maximum amount of data that the memory can transfer in one cycle (W in figure 1 and 2W or 64 bits in figure 2). In other words, the total data transfer due to the inner loop of the calculation algorithm is less than or equal to the maximum amount of data that the memory can transfer in one cycle. This feature is not directly and derivable from the application as originally filed which repeatedly stated a condition which required that the total data transfer due to the inner and outer loops is less than or equal to the maximum amount of data that the memory can transfer in one cycle. In particular, it is not directly and unambigously derivable from the application as originally filed that the data transfer rate due to the inner loop can be any value less than the maximum amount of data that the memory can transfer in one cycle.

4.1.4 The appellant has argued that the restriction to the inner loop only was originally disclosed in figures 1,

6 and 7 and the description (see page 8, lines 11 to 24, page 13, line 7, to page 16, line 12, and page 35, line 25, to page 36, line 5 (corresponding to paragraphs [0012], [0025] to [0031] and [0078] as published)). In the oral proceedings the appellant also filed a sheet entitled "Information and instructions" (which is annexed to the minutes) which also referred to page 35, line 25, to page 36, line 5, of the description as originally filed. The board does not accept these arguments. The first cited passage summarises the invention and does not mention any restriction of the data transfer rate to the inner loop. The second cited passage discusses the operation of registers 13 to 17 which store input and output data for the MAC operator 12. It does show an "embodiment" in which the inner loop transfer rate requirement is equal to the memory transfer rate. However, as stated above, the skilled person studying the application in the light of such statements as the summary of the invention would understand that the total data transfer due to the inner and outer loops is intended to be less than or equal to the maximum amount of data that the memory can transfer in one cycle and that this "embodiment" does not satisfy that requirement (see 3.3 above). It cannot therefore be on its own the basis for a new, generalised form of technical teaching that embraces this "embodiment", that of figure 2, and everything in between. The third cited passage concerns the embodiment shown in figure 2 and explained in the timing diagrams in figures 6 and 7. As explained above (see point 3.4), the skilled person studying this embodiment would understand that in this case the total data transfer due to the inner and outer loops is

indeed less than or equal to the maximum amount of data that the memory can transfer in one cycle.

4.1.5 The appellant has also argued that, as the value of "a" does not change in the inner loop, there is no need to allow time to load "a" values. The board is not convinced by this argument as the inner loop runs inside the outer loop (steps 1.1 to 1.3 and 1.11 to 1.12; see the description, page 4, line 14, to page 5, line 18). In the outer loop "a" values are loaded from memory to register 13 (figure 1) or register 112 (figure 2) and this will require data transfer time. If no new "a" values are loaded then the inner loop will eventually stop.

4.1.6 Hence the board finds that the amendments to claim 1 do not satisfy Article 123(2) EPC regarding added subject-matter.

4.2 *First auxiliary request*

4.2.1 Claim 1 is the same as that according to the request (received with the letter dated 27 July 2009) considered by the board in the annex to the summons to oral proceedings. There the board took the view that the deletion of the expression from claim 1 "wherein the amount of the data to be supplied in each clock cycle is adjusted such that total amount of data consumed and produced by said MAC operator (12) in one clock cycle will be equal to or smaller than maximum amount of data that the memory (11) can transfer in one clock cycle", in other words the "result to be achieved" according to the appealed decision, seemed to add subject-matter, Article 123(2) EPC, since this

result was set out in both original independent claims and was mentioned repeatedly in the description and it was questionable whether the features added to the claim, in particular the register input and output bit widths, were sufficient to limit the claim to circuits achieving the above result.

4.2.2 The appellant's subsequent submission (received 17 January 2011) did not contain any substantive response to this objection, and in the oral proceedings the appellant's representative stated that he had nothing to add regarding this request.

4.2.3 The appellant has not persuaded the board to deviate from its preliminary opinion on this request. Considering claim 1 in the light of figure 1, the bit width of the multiplier "b" (referred to as the "third bit width") is the same as the bit width of "c" (buffer 15) and "e" (input to buffer 17), the "third bit width" only being limited by the feature in claim 1 that it is less than the "second bit width", i.e. that of multiplicand "a". Hence claim 1 has been amended to now cover the case of e.g. the "third bit width" being W/2 instead of W/3 as shown in figure 1. In the case of W/2, the inner loop alone would result in a data transfer of 1.5 W per clock cycle (two reads per cycle of W/2 and one write of W/2) which would be greater than the maximum amount of data that the memory can transfer in one clock cycle (1 W). In such a case the memory would have to wait for the MAC operator, a situation excluded in the application as originally filed. Thus claim 1 has been amended to cover registers and MAC operators with bit widths which do not fulfil the limitation consistently set out in the application as originally

filed and are not directly and unambiguously derivable from the application as originally filed.

4.2.4 Hence the board finds that the amendments to claim 1 do not satisfy Article 123(2) EPC regarding added subject-matter.

4.3 *The second and third auxiliary requests*

Claim 1 according to both requests contains the feature "wherein a sum in bit width of an output of the second register (14), an output of the third register (15), and an input of the fifth register (17) is equal or less than the first bit width". Since the first bit width is defined in claim 1 of both requests as being that of the memory, this feature has the effect that the data transfer in the inner loop per clock cycle is equal to or less than the maximum amount of data that the memory can transfer in one clock cycle. Hence this feature is another way of formulating the same limitation as that discussed above in connection with the main request and found to contain added subject-matter. The remaining features of claim 1 of both requests do not affect the board's assessment of the above feature. Hence claim 1 according to these requests has been amended contrary to Article 123(2) EPC for essentially the same reasons as given above in connection with the main request.

5. *Conclusion*

None of the appellant's main or first, second or third auxiliary requests is allowable, Article 123(2) EPC.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

B. Atienza Vivancos D. H. Rees