BESCHWERDEKAMMERN
DES EUROPÄISCHEN
PATENTAMTS

BOARDS OF APPEAL OF
THE EUROPEAN PATENT
OFFICE

CHAMBRES DE RECOURS
DE L'OFFICE EUROPÉEN
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 28 July 2016

Case Number:	T 1244/13 - 3.5.06
Application Number:	02027872.7
Publication Number:	1293891
IPC:	G06F7/72, G06F9/302
Language of the proceedings:	EN

Title of invention:
Arithmetic processor accomodating different finite field size

Patent Proprietor:
Certicom Corp.

Opponent:
Müller, Christoph

Headword:

Relevant legal provisions:
EPC R. 99(2), 103(1)(a), 115(1)
EPC Art. 114(2), 4, 123(2)
RPBA Art. 11, 12(2)
EPC 1973 Art. 54, 56, 100

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Keyword:
Substantial procedural violation - (no)
Inventive step - after amendment (yes)

Decisions cited:
G 0010/91, T 0514/04

Catchword:

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Case Number: T 1244/13 - 3.5.06

DECISION
# of Technical Board of Appeal 3.5.06
of 28 July 2016

Appellant: (Opponent)	Müller, Christoph Ludwigstr. 22 79104 Freiburg im Breisgau (DE)
Representative:	Fechner, Benjamin Wendelsteinstrasse 29A 82031 Grünwald b. München (DE)
Respondent: (Patent Proprietor)	Certicom Corp. 4701 Tahoe Boulevard Tahoe A, 6th Floor Mississauga, Ontario L4W 0B5 (CA)
Representative:	Moore, Barry Hanna Moore + Curley Garryard House 25/26 Earlsfort Terrace Dublin 2, D02 PX51 (IE)
Decision under appeal:	**Interlocutory decision of the Opposition Division of the European Patent Office posted on 5 April 2013 concerning maintenance of the European Patent No. 1293891 in amended form.**

Composition of the Board:

Chairman	W. Sekretaruk
Members:	M. Müller
	G. Zucka

Summary of Facts and Submissions

I. The appeal lies against the interlocutory decision of the opposition division, with reasons dated 5 April 2013, that, account being taken of the amendments made by the patent proprietor during the opposition proceedings, European patent No. EP-B-1 293 981 and the invention to which it relates met the requirements of the EPC. In the decision, the following documents were relied on:

D3: DE 36 31 992 A2, and
D4: US 5 602 767.

Reference was also made to

D5: H. Sedlak, "The RSA Cryptography Processor", Advances in Cryptology - EUROCRYPT '87, Workshop on the Theory and Application of Cryptographic Techniques, April 1987, pages 95-105.

II. The opponent appealed this decision on 23 May 2013 and paid the appeal fee on the same day. A statement of grounds of appeal was filed on 15 August 2013. The appellant (opponent) requested that the decision be set aside and that the patent be revoked because it was insufficiently disclosed (Articles 83 and 100(b) EPC 1973) and lacked novelty or inventive step (Articles 54, 56 and 100(a) EPC 1973), and that the appeal fee be reimbursed (Rule 103(1)(a) EPC).

With the statement of grounds of appeal, the appellant also submitted four new documents D6 to D9. D6 is an excerpt from a handbook on algebra. Otherwise, these documents need not be identified in this decision.

III. The respondent (proprietor) replied to the grounds of appeal in a letter dated 20 January 2014, in which it requested that the appeal be dismissed, and that the request for reimbursement of the appeal fee be rejected. It argued that documents D6 to D9 should not be admitted into the appeal proceedings, *inter alia* because documents D7 to D9 had not been available to the public at the relevant date. It took the view that the objection of insufficiency of disclosure relied on a new and late-filed fact that should not be admitted into the proceedings and, because it related to claim 1 and previously only claims 2 and 4 had been objected to under insufficiency of disclosure, constituted a fresh ground for opposition (following T 514/04). As it did not agree to its introduction, it could not be considered (following G 10/91). Finally, the following document was filed:

HL8: A. Menezes *et al.*: "Handbook of Applied Cryptography"; CRC Press; 1997; pages 595-596.

With its response, the respondent also filed sets of claims according to auxiliary requests 1 to 7 and requested maintenance of the patent on this basis or on the basis of "a combination of any of auxiliary requests 1 to 7".

IV. With letter dated 10 August 2014, the appellant responded *inter alia* by submitting further documents, including

D11: U. Hamann et al.: "Krypto-Chipkarten - individuelle Sicherheit für jedermann"; Card-Forum; July 1995; pages 31-35, which, being pre-published and having the same content as D9, was intended to replace D9 in the appellant's argument. Moreover, the appellant claimed a public prior use of the cryptoprocessor SLE 44C200 and requested the board to indicate whether this objection was pertinent for the decision and, if so, whether it lacked credibility (see letter of 10 August 2014, point 2.7.3).

V. In an annex to a summons to oral proceedings, the board informed the parties of its preliminary opinion. In particular:

The board tended to consider that no substantial procedural violation had occurred in the opposition proceedings.

It took the view that D6 and D11 should be admitted, respectively, as written evidence of common knowledge in the art and as highly relevant for inventive step, and that the admission of D7 and D8 could be left open. With regard to the alleged public prior use, the board opined that all features of the cryptoprocessors 44CP2 and 44C200 on which the appellant wanted to rely were also known from D11 and it therefore doubted that the alleged public prior use could further the appellant's case.

The board expressed doubts whether the appellant's submissions, even if admitted, would establish an insufficiency of disclosure of claim 1.

The board also discussed how claim 1 had to be construed and said it tended to agree with the appellant that the claimed invention lacked inventive step over D3 and D11.

VI. In response to the summons, the respondent submitted a new, additional 8th auxiliary request with a letter dated 30 May 2016, and the appellant submitted further observations with a letter dated 6 June 2016.

VII. Oral proceedings were held on 28 June 2016. During these proceedings, towards the end of the hearing, the respondent replaced all pending requests with a single one based on auxiliary request 6. At this point, the board decided not to announce a decision. Instead, the chairman closed the debate and indicated that the board would continue the proceedings either by issuing a decision or by sending a further communication.

VIII. With letter of 14 July 2016, the board informed the parties about its decision to reopen the debate. Although it appeared that the claims on file showed an inventive step over the prior-art documents on file, the opponent had not had sufficient time to consider the latest amendments. It was proposed to hold the oral proceedings on the same day as that of another, related case between the same parties and before this board in the same composition. The parties accepted this proposal although it was made with less than two months' notice (Rule 115(1) EPC).

IX. In response to this communication, with letter dated 26 July 2016, the appellant filed a new document regarding inventive step of the then main request:

D12: W. Drescher *et al.*, "VLSI Architectures for Multiplication in GF(2^m) for Application Tailored digital Signal Processors", IEEE Workshop on VLSI Digital Signal Processing, 1996.

X. Second oral proceedings were held on 28 July 2016. During these oral proceedings, the appellant proprietor filed an amended set of claims 1-4 and requested that the patent be maintained on the basis of these claims and the description and the drawings as granted.

XI. Claim 1 reads as follows:

"An arithmetic processor (1) for performing cryptographic operations comprising:

a) an arithmetic logic unit (ALU) containing arithmetic circuitry configured to perform field operations in an underlying F_2^n field;

b) a register file (2) comprising a group of general purpose registers each having a plurality of cells, said general purpose registers being sized to contain representations of one or more operands by storing a bit vector of an operand in each of said plurality of cells,
said register file (2) being connected to said ALU (4) via data input buses (6) to provide said bit vectors to said ALU (4) for performing operations on said one or more operands and being connected to said ALU (4) via a data output bus (14) for writing results of computations performed in said ALU (4) to said register file (2); and

c) a controller (8) connected to said ALU (4) and said register file (2), said controller (8) comprising instructions for:

obtaining a field size control signal (12) indicative of said underlying F_2^n field for said one or more operands;
providing to said ALU (4) a control (13) indicative of the appropriate field size to be used as indicated by said field size control signal (12);
and
coordinating data access between said register file (2) and said ALU (4) to instruct said ALU (4) to operate sequentially on said bit vectors and write results of computations performed in said ALU (4) to said register file (2);

wherein said arithmetic circuitry comprises special purpose registers (16) each having a fixed control bit (26), a plurality of sub-ALUs (18) connected to said special purpose registers (16) by one or more bit input data buses (28) and a sequencer (20) connected to said special purpose registers via control bit inputs (24) providing said control bits (26) to said sequencer (20), said sequencer (20) comprising instructions for:

sequencing said ALU (4) through steps in computational operations by controlling data input via the input buses (6) from and to the register file (2) to the sub-ALUs (18) or special purpose registers (16),
monitoring said control bits (26), and
implementing a counter in its own control registers (22) to control the number of iterations according to the size of the field being used and thereby allow said arithmetic processor (1) to be used for different field sizes without redesigning processor hardware,

wherein said arithmetic circuitry comprises shared finite field and integer arithmetic circuitry and said controller (8) receives a mode selection control (10) for selecting between either F_2^n finite field computations or integer computations."

XII. At the end of the oral proceedings, the chairman announced the decision of the board.

Reasons for the Decision

Alleged substantial procedural violations
Article 11 RPBA and Rule 103(1)(a) EPC

1. The appellant argued that the opposition division had violated its right to be heard, as was evident from several circumstances.

1.1 The opposition division was prejudiced against the opponent's case to the point of partiality (see grounds of appeal, II.1).

1.2 Contrary to the usual practice at the EPO, the oral proceedings before the opposition division had started with the discussion of novelty rather than added subject-matter and sufficiency of disclosure (see grounds, II.2).

1.3 The opposition division, when disregarding an objection by the opponent under Article 83 EPC as a new fact, did not have the necessary discretion. In particular, such discretion could not be derived from Article 114(2) EPC (see letter of 18 August 2014, II.1.3, 2.2, 3 to 3.3).

1.4 The opposition division, when limiting the discussion of novelty to feature (a), left unclear which of the other features, if any, it considered also to be new.

This made it impossible for the opponent to address the opposition division's assessment of inventive step in a meaningful way (see grounds of appeal, II.3.2, 3.2.1.1, 3.2.1.2, 3.2.2).

1.5 The minutes of the oral proceedings were incomplete, and thus in conflict with Rule 124(1) EPC, because a handout referred to as F2 was not attached to them. This handout had been distributed during the oral proceedings and should have been included in the minutes as an accurate summary of the opponent's submission (see grounds of appeal, II.4).

2. The board agrees with the respondent that the appellant's allegations are without merit.

2.1 The appellant provides no reasoning establishing that the opposition division was biased (see respondent's letter of 20 January 2014, B.I).

2.2 The chairman of the opposition division is not constrained by the EPC in determining the order of issues to be discussed during oral proceedings (nor, for that matter, are the examining division, legal division or boards of appeal). The jurisprudence of the boards of appeal or the Guidelines for examination likewise do not prescribe a mandatory order (*ibid.*, B.II).

2.3 The appellant (opponent) had raised the new objection that the pseudocode on page 9 of the application as originally filed was deficient, with the alleged consequence that the subject-matter of claim 1 was insufficiently disclosed, in the oral proceedings before the opposition division. Earlier, entirely different objections had been raised, and only against dependent claims 2 and 4. The board agrees with the opposition division that the opponent's new submissions constitute new facts within the meaning of Article 114(2) EPC and that, therefore, the opposition division did have discretion not to admit it (*ibid.*, B.III.1.c). Moreover, it would appear from the minutes (point 3.6) that the opposition division listened to the opponent's new objections with regard to Article 83 EPC but found them, at least *prima facie*, to be without merit (*ibid.*, B.III.1.b).

The board notes in passing that the decision not to admit the new objection is only reported in the minutes whereas it should have been included in the reasons for the decision. This omission, however, is, in the board's judgement, not a substantial one because the minutes leave no doubt as to what was decided and for what reason.

2.4 The right to be heard does not imply the parties' right to know the division's opinion on every individual point before the decision. The board notes that the opposition division had given in its summons its preliminary view as to which features of claim 1 were novel, so the opponent had sufficient opportunity at the oral proceedings to present its comments (see minutes, sections 1.1, 1.3, 2.1, 2.2 and 2.6; and respondent's letter of 20 January 2014, B.III.2).

2.5 The completeness of the minutes is immaterial on appeal. Had the appellant considered an addition to the minutes to be required, it should have requested the opposition division to make it (*ibid.*, B.IV).

3. In summary, the board cannot recognise any fundamental procedural deficiency in the first-instance proceedings which could have required a direct remittal under

Article 11 RPBA. Moreover, in the absence of any substantial procedural violation, reimbursement of the appeal fee is not equitable, Rule 103(1)(a) EPC.

The invention

4. The invention is based on the observation that whereas traditional RSA cryptography mainly requires modular arithmetic operations such as modular exponentiation, in the transition to more secure elliptic curve cryptography that requires the full complement of modular and finite field operations there is a need for arithmetic processors that support both kinds of operations (see the patent, paragraphs 2 to 4). The patent acknowledges that such processors are known in prior art, but aims at improving them (paragraphs 5 and 6).

The arithmetic processor of the invention is depicted in figure 1 and comprises *inter alia* an arithmetic logic unit ALU (4 in figures 1 and 2) which further comprises a plurality of sub-ALUs (18 in figure 2). The ALU is configured to perform field operations in an underlying F_2^n field (see e.g. paragraphs 19, 25 and 27, of the patent). The ALU is further configured to carry out integer arithmetic operations (see paragraph 33 *et seq.* of the patent). Both are supported by shared finite field and integer arithmetic circuitry (see e.g. paragraphs 33, 37 and 39 of the patent, as well as figure 8).

The prior art

5. D3 discloses a cryptographic processor equipped to perform encryption and decryption according to RSA (see abstract). It provides hardware support for exponentiation, multiplication and addition/subtraction (see

page 6, lines 39-49) over the residue class ring Z/ZN, N being the product of two primes (see e.g. page 5, lines 15-18). The processor uses an exponentiation algorithm based on the iterated and interleaved execution of multiplication and modulo operations (see page 6, lines 39-43), both using look-ahead algorithms (see page 6, lines 30-34 and 55-65). The algorithm is referred to as MultMod (see page 10, lines 30-31, page 12, line 39 *et seq.*, and figure 4 and 5).

5.1 The number "N", also referred to as the "key length", is variable up to 660 bits (see page 7, lines 10-12, and page 18, lines 47-50). N determines the maximal size of operands, which can comprise at most "L(N)" bits. Accordingly, the pertinent registers in D3 have length L(N) (see page 16, line 25-57).

5.2 The processor circuitry is based on a processing component called an elementary cell ("Elementarzelle", see page 16, lines 25-27, and figure 7). Such an elementary cell comprises *inter alia* registers 12, 14 and 16 and 18, as well as a bit adder 22 and a full adder 24, operating on a register Z holding an intermediate result (hence Z for "Zwischenergebnis") of the MultMod algorithm (see page 16, lines 52-57, page 17, lines 3-8 and 34-41). The elementary cells are hierarchically grouped in blocks coupled with a MultMod controller unit (see page 17, lines 28-33, and figures 8-10 and 12).

5.3 D3 also discloses that, for security reasons, all cryptographic algorithms should as far as possible be contained on a single chip (see page 5, lines 63-68).

6. The content of D5, authored by the inventor of D3, is a scientific publication, the content of which substantially overlaps with that of D3. In particular, D5 discusses in detail the "MultMod" algorithm used in the cryptographic processor. D5 also discloses further "Features of the RSA Cryptography Processor", in particular the generation of hash functions which uses *inter alia* an XOR function (see page 104, esp. the enumeration on the middle of the page).

7. Document D11 is concerned with asymmetric cryptography, in particular RSA, on chipcards and discusses the chip SLE 44C200, which is referred to as a combination of chipcard security controller and arithmetic coprocessors (see paragraph bridging pages 1 and 2). The chip supports modular arithmetic for operands of up to 540 bits length, in particular addition, subtraction, modular reduction, XOR and shift operations (see page 33, left column, paragraph 2). It is stated that, using these operations, all known public key methods can be implemented, including elliptic curves (*loc. cit.*). The performance of the processor is illustrated in a table suggesting that, in fact, various cryptographic algorithms had been implemented on it, including RSA, DSA and elliptic curves (see page 34, figure 4). D11 also suggests various potential hardware and software extensions of the chip to support additional functionality or to better support new public-key methods such as elliptic curve cryptography (see paragraph bridging pages 34 and 35), without however disclosing any details as to how this was or should be done.

8. D12 relates to hardware support for finite field arithmetic as used in cryptography and discloses in particular that the "hardware of a typical standard

binary arithmetic multiplier" can be combined "with a $GF(2^m)$ multiplier" (see abstract). It is observed that the hardware of a $GF(2^m)$ multiplier and that of integer multiplication have such a similar physical structure that they can be integrated to save circuitry and thus chip space (see section 4, paragraphs 1 and 2). Both multiplications are based on the logical XOR function, although in $GF(2^m)$ - but not in integer arithmetic - results are taken modulo 2, see section 2), and in integer arithmetic - but not in $GF(2^m)$ - carries are used (see also section 4.1.1, esp. the paragraph just below figure 8).

9. No further prior art will be referred to in this decision. In particular, the mathematical facts required for the decision will be stated without reference, because they were not *per se* questioned in the proceedings. D7 to D9 will not be referred to, so their public availability and their admission into the proceedings need not be decided on. The alleged public prior use addressed in the summons to oral proceedings was not further argued by the appellant and hence will not be considered.

Operations over a finite field

10. The patent as granted and as maintained in opposition related to feature (a) of then claim 1 referring to an arithmetic unit "configured to perform field operations in an underlying field".

10.1 The opposition division found that the closest piece of prior art, D3, did not disclose this feature and also placed central importance on this feature in its assessment of inventive step (see the decision, reasons 14.2 and 15.4). The opposition division considered that an "arithmetic unit" as claimed, which was "configured to perform field operations", must have "a very specific hardware layout which executes [...] all finite field operations in the underlying finite field [...] for all elements of the underlying field". In contrast, D3 disclosed the mathematical operations needed for RSA, which was based on a residue class ring, and which used modulo operations with a modulus N = p*q. Not every ring being a field, the ring opera tions of D3 thus did not constitute field operations as claimed (see the decision, reasons 14.2 and 14.2.

10.2 The appellant challenged this finding, arguing that then feature(a), properly construed, was disclosed in D3. Claim 1 required an arithmetic unit configured to carry out only finite field operations without explaining which ones. The skilled person, knowing that mathematical structures of fields were defined by the two operations addition and multiplication, would thus understand "field operations" to mean just these two, addition and multiplication. Rings and fields were not different for these two operations.

Moreover, rings were different from fields in that division, the inverse of multiplication, was not defined for all elements of a ring but for all elements of a field. However, for those elements for which division *was* defined, it was exactly the same operation and would be implemented in both cases by the extended Euclidean algorithm. As a consequence, the processor of D3, when performing ring operations, would, in effect, also be performing field operations. Whether the processor of D3 operated on elements of a ring or on elements of a field would depend on the value used as the modulus. The choice of the modulus did not, however, affect the *configuration* of the arithmetic unit.

10.3 In the annex to its first summons, the board addressed this as a central issue and expressed its preliminary agreement with the appellant.

10.4 For the present claims, however, this issue need not be decided. Present claim 1 is limited to the F_2^n operations. The elements of F_2^n are binary polynomials, i.e. polynomials whose coefficients are either 0 or 1, which can be represented as n-bit strings. For binary polynomials, addition is simply bit-by-bit XOR. This means *inter alia* that no carries are needed.

10.5 The modular arithmetic in F_2^n and that used in RSA modulo N = p*q are significantly different. Hence, the appellant's argument that the hardware of D3 must be considered, as an incidental mathematical fact, as being configured to perform the pertinent finite field operations, fails at least for the particular finite field F_2^n. This was common ground between the parties.

Article 100(c) EPC 1973

11. The appellant did not provide reasons for the ground of opposition under Article 100(c) EPC 1973, either in its statement of grounds of appeal or during the appeal proceedings.

11.1 The board notes that the grounds of appeal contain a generic reference to the written and oral submissions in the proceedings before the opposition division (see page 2, lines 1-2). Such a reference to submissions made *before the decision* was delivered are normally insufficient to establish why the appellant considers individual reasons *in the decision* to be wrong. Therefore, it cannot replace the statement required by Rule 99(2) EPC indicating the reasons for setting aside the decision impugned, or the extent to which it is to be amended. By the same token, a reason substantiated only by such a reference does not meet the requirements of Article 12(2) RPBA and therefore need not be taken into account by the board.

11.2 The board takes the view that the appellant is no longer pursuing this line of argument. This was expressed as the board's preliminary opinion in the annex to the summons and it was not challenged by the appellant.

11.3 Beyond that, the board is satisfied that amended claim 1 does not extend beyond the content of the application as filed. Claim 1 is based on claims 1 and 2 of auxiliary requests 5 and 6 filed by the respondent with letter of 20 January 2014, the finite field F_2^n is mentioned throughout the application as originally filed, the shared circuitry is discussed in the application in the section on integer arithmetic (see page 14, last three lines *et seq.*), the fundamental principle being disclosed, for multiplication, in figure 8.

Article 100(b) EPC 1973

12. In its opposition, the ground of opposition under Article 100(b) EPC 1973, namely that the invention was not disclosed in a manner sufficiently clear and complete for it to be carried out by a person skilled in the art, was invoked only for claims 2 and 4 and only with regard to the term "mode selection control"

and the shared circuitry according to claim 2, and the "filling" of special purpose registers according to claim 4. The opposition division dismissed these objections (see the decision, reasons 18, esp. 18.1.3 and 18.2.3).

12.1 In its statement of grounds of appeal, these objections were not expressly repeated. Therefore, the board need not take them into account, for the reasons just given with regard to Article 100(c) EPC 1973.

12.2 Rather, the appellant argued that the invention according to claim 1 was insufficiently disclosed because the skilled person was unable to implement the multiplication operations disclosed in the patent. Neither, that is, the multiplication in F_2^n nor that in integer arithmetic (see e.g. the patent on page 4, paragraph 19, and on page 6, paragraph 34; and the grounds of appeal, point V, and esp. points 1.1 and 1.2).

12.3 The board agrees with the respondent that, with regard to claim 1 of the patent against which no objection under Article 100(b) EPC 1973 was raised in the opposition proceedings, this constitutes a new ground for opposition which under G 10/91 the board cannot admit because the respondent (proprietor) does not consent to it. In this, the board concurs with T 514/04 as cited by the respondent. However, with regard to claims 2 and 4 of the patent as granted, against which the ground for opposition pursuant to Article 100(b) EPC 1973 *was* raised, the new objection only constitutes a new fact against which the respondent does not have a veto power under G 10/91.

12.4 The algorithm given for multiplication of polynomials $a=(a_0,...,a_{n-1})$ and $b=(b_0,...,b_{n-1})$ in F_2^n contains two obvious errors: it contains a duplicate of the statement "for j from n-1 to 0 do" and, in its inner loop statement, it multiplies only bits of a and b with the same index i: "$c_j=c_{j-1}+b_ia_i+c_{n-1}m_j$". The algorithm for modular integer multiplication contained a similar index error in the line "$M_{j+1}=(b_j(a_j)+m_j+c_j)/2$".

12.5 It was common ground between the parties that the multiplication algorithm in F_2^n did not work as specified, whereas the duplication was unproblematic. In the minutes of the oral proceedings, the opposition division stated (point 3.6) that the "skilled person knows how to implement a (field) multiplication" and thus "would recognize the index error in [the] pseudo code as obvious, similar to the indexes when multiplying integers as shown on page 6". Since the objection had not been admitted as a new fact, this statement was made as an *obiter dictum*.

12.6 In its statement of grounds of appeal, the appellant argued that the skilled person might have recognised the errors but would not have been able to correct them on the basis of the description. The proprietor responded that the skilled person would have been able to correct the errors based on his common knowledge as to "how a multiplication of bit vectors is carried out". In this regard, reference was made to HL8.

12.7 In its letter of 10 August 2014, the appellant doubts the relevance of HL8 and argues that the erroneous algorithm did not work, even if the index error was corrected as proposed by the respondent.

12.8 The board follows the appellant's view that the respondent has failed to establish that the correction of the erroneous pseudo-code was obvious. However the board agrees with what it understands to be the opposition division's position, namely that the person skilled in the art of cryptographic and arithmetic processors must be assumed to know, from his common knowledge, how to multiply two polynomials in F_2^n and two integers in Z. The board expressed this preliminary opinion in its summons to oral proceedings, without making reference to a document establishing such common knowledge, and it was not challenged by the appellant.

12.9 The board thus has no reason to deviate from its preliminary opinion and finds that the cited errors in the pseudo-code do not mean that the invention was insufficiently disclosed.

Articles 54, 56 and 100(a) EPC 1973

13. Throughout the opposition proceedings, D3 was considered to constitute the closest piece of prior art and it was uncontroversial in appeal, too, that inventive step should be assessed starting from D3.

14. In its comparison between the claimed invention and D3, the appellant established a number of correspondences between both. Not all of them, however, convinced the board.

15. The appellant argued that the input marked L(N) to adder component 58 of the controller depicted in figure 12 corresponds to the claimed field size control signal which is used to implement the claimed counter "to control the number of iterations according to the size of the field being used and thereby allow said

arithmetic processor (1) to be used for different field sizes without redesigning processor hardware".

15.1 Since the processor of D3 does not operate over an F_2^n field but over rings, D3 cannot actually disclose a field size control signal. So the appellant's argument in this regard is that D3 discloses a control signal indicating the size of the underlying mathematical structure and enables the processor to be used for different such structures of different size.

15.2 The box L(N) in figure 12 is not specifically discussed in D3.

The variable L(N) occurs several times in D3 as defining the size of the registers (see page 16, lines 33-57). This size corresponding to the largest possible operands corresponds to the size of the underlying mathematical structure. However, in the context of page 16, L(N) is a constant rather than a "control signal", let alone one controlling the number of iterations of a computational operation.

In the context of figure 12 it is not clear from D3 whether the box containing L(N) denotes a register and thus might be considered as producing an internal "signal". Moreover, what is referred to as L(N) in figure 12 appears to correspond to L(M) as referred to in figure 3(b) and the number of bits of the multiplicator which remain to be processed (see page 17, lines 25-26). While figure 3(b) discloses a counter m which determines the number of iterations in an individual calculation, the initial value of the counter L(M) is the size of an individual operand rather than the size of the underlying mathematical structure.

The board accepts that the structure of the underlying mathematical structure determines the maximum (and possibly the typical) operand size and that, hence, L(N) and L(M) are related to each other. However, the board considers that they must not be confused with each other.

15.3 The board therefore comes to the conclusion that D3 does not disclose a control signal for the size of the mathematical structure which controls the number of iterations in a computational operation.

16. The appellant further argued that D3 disclosed fixed control bits as claimed. It referred to figure 12 which showed that the controller operated on the highest-valued bits of the values in registers 12 (M) and 24 (Z) (see No. 38, 50 and 52 in that figure).

16.1 The highest-valued bits are, however, not necessarily in fixed positions in the registers. With reference to figure 15, the appellant further argued that the pertinent register values were left-adjusted.

16.2 This figure does not, however, disclose left adjustment of values within a register. It discloses the relative adjustment of the values of registers C, Z, N with the aid of a 20-bit buffer (see page 14, lines 64 *et seq.*) The highest order bits of the values in registers C, Z and N may end up outside the registers and, moreover, in different positions in the buffer (see e.g. the last three triplets of columns in figure 15).

16.3 The appellant has also made reference to the fact that the controller component 52 receives an input marked as "Digit sign Reg.-Z." and argued that the sign bit is normally the highest bit of the binary representation of a value (see statement of grounds, point 3.1.2).

16.4 Even if, however, this were the case (which was disputed by the respondent, see its letter of 20 January 2014, pages 20-21, point F.I.2 e) (2) and (3)) it was not necessarily at a fixed position in the register (see also the respondent's letter, same section, point (4)).

16.5 The board therefore concludes that D3 does not disclose the claimed fixed control bits in the special-purpose registers.

17. In summary, the board finds that the subject-matter of claim 1 differs from D3 at least in the following features:

(a) The claimed arithmetic unit is configured to perform the field operations in an underlying F_2^n field (see point 9 *et seq.* above).

(b) The arithmetic processor obtains a control signal indicative of the size of the underlying mathematical structure and uses it to control the number of iterations in a computational operation (see point 15 *et seq.* above).

(c) The special purpose registers each have a fixed control bit which is monitored by the sequencer (see point 16 *et seq.* above).

(d) The arithmetic circuitry comprises shared finite field and integer arithmetic circuitry and the controller receives a mode selection control form selecting between F_2^n finite field computations or integer computations.

17.1 These differences solve the primary problem of adapting the processor of D3 so as to be able to also carry out elliptic curve cryptography.

17.2 The board considers this to be a plausible problem which the skilled person aware of D3 would have posed himself in view of D3, in view of the rise of ECC as an alternative to RSA in general but also in view of the suggestions in D11 in particular (page 33, left column, paragraph 2, figure 4, paragraph bridging pages 34 and 35). Notably, however, while D11 claims that ECC has been or could be implemented on the cryptoprocessor SLE 44C200 developed for RSA, it lacks any details as to how this was done.

18. The skilled person would realise that the processor of D3 was not only equipped for carrying out the arithmetic operations necessary for RSA but was also optimised for this purpose by means of the MultMod algorithm. Accordingly, a large part of the controller depicted in figure 12 was designed to implement this algorithm. Specific reference was made to the registers for M and Z (figure 12, no. 12 and 24), their highest value bits and the sign bit of Z, and to comparator block 38, all of which explained as part of the MultiMod algorithm (see esp. page 13, lines 37-38, and page 17, lines 9-41).

18.1 The respondent argued, and the appellant agreed, that these optimisations would not carry over to F_2^n.

18.2 The appellant did not argue that or how the skilled person would have modified the MultMod algorithm presented in D3 for ECC, nor, consequently, that or how the skilled person would have modified the controller according to figure 12 to ECC.

18.3 The board agrees with the respondent that, starting from the controller of figure 12, the skilled person would have to drop essential parts of the circuitry before even being able to adapt it to ECC; in particular comparator 38. The board takes the view that it would not have been obvious for the skilled person to undertake this as a solution to the above problem.

18.4 During the oral proceedings, both parties agreed that the skilled person setting out to solve the given problem would not start from the controller of figure 12.

19. Rather, the appellant argued that the skilled person would attempt to adapt the algorithm depicted in figure 3(b) with a view to using hardware features from D3 when implementing an algorithm for ECC (such as the elementary cell of figure 7).

19.1 In doing this, the skilled person would have to adapt the mathematical operations in the algorithm to work for F_2^n, *inter alia* by replacing addition and subtraction with XOR and the test for Z>N with a comparison of degrees of two polynomials, as a matter of his common knowledge of the required mathematics, then introduce a field size control signal as claimed to increase flexibility, further consider left adjustment of register value as an obvious choice and a matter of common knowledge, and also refer to D12 as providing a solution for the shared circuitry for finite field and integer arithmetic. The appellant conceded that this required the skilled person to perform quite a number of steps but argued that each of these was obvious.

19.2 The board doubts that the skilled person would actually have started the development of an arithmetic processor for ECC based on a processor developed and optimised for RSA, and moreover whether he would have considered modifying an algorithm for RSA in such a document for ECC rather than looking it up in a handbook.

19.3 As regards the shared circuitry feature, the board accepts the appellant's submission that, in general, sharing of circuitry is an interest of the skilled person with a desire to save chip space, and that D12 discloses the general lines of how sharing between $F_2{}^n$ and integer multiplication can be practised.

19.4 However, the appellant did not provide any particular motivation why the skilled person would consider left adjusted register values in this context, and the board does not consider that use of the highest-value bits in the MultMod algorithm of D3 (see also figure 12) provides such motivation. The appellant also did not provide any specific motivation for the skilled person, starting from D3, to provide the field size control signal.

19.5 The board thus considers that the skilled person *could* have been able to arrive at the claimed invention in the manner outlined by the appellant but is not convinced that the skilled person *would* have performed the many necessary steps without exercising an inventive step.

19.6 That is, the board finds that the appellant has not established that the claimed invention would have been obvious for the skilled person based on D3 and thus concludes that the subject-matter of claim 1 shows the required inventive step.

20. When, during the oral proceedings, the board indicated that this was its conclusion, and on specific request by the board, the appellant did not present an inventive-step argument starting from any other prior-art document.

Summary

21. The board concludes that none of the grounds for opposition under Article 100(a) to (c) EPC 1973 nor, pursuant to Article 102(3) EPC 1973, any other requirement of the EPC prejudices the maintenance of the patent in amended form.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.
2. The case is remitted to the opposition division with the order to maintain the patent on the basis of the following documents: claims 1-4 as filed on 28 July 2016, and the description and drawings as granted.

The Registrar: The Chairman:

Beschwerdekammern des Europäischen Patentamts
Boards of Appeal of the European Patent Office
Chambres de recours de l'Office européen des brevets

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated