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 25 March 2015

| | |
|---|---|
| **Case Number:** | T 1925/11 - 3.5.06 |
| **Application Number:** | 06749987.1 |
| **Publication Number:** | 1889398 |
| **IPC:** | G06F7/72 |
| **Language of the proceedings:** | EN |

**Title of invention:**
RANDOMIZED MODULAR POLYNOMIAL REDUCTION METHOD AND HARDWARE THEREFOR

**Applicant:**
Inside Secure

**Headword:**
Modular reduction hardware/INSIDE SECURE

**Relevant legal provisions:**
EPC Art. 56

**Keyword:**
Inventive step - after amendment (yes)

**Decisions cited:**

**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 1925/11 - 3.5.06**

# DECISION
# of Technical Board of Appeal 3.5.06
# of 25 March 2015

**Appellant:**
(Applicant)

Inside Secure
Rue de la Carrière de Bachasson, CS 70025
Arteparc Bachasson, Bât. A
13590 Meyreuil (FR)

**Representative:**

de Roquemaurel, Bruno
OMNIPAT
24 Place des Martyrs de la Résistance
13100 Aix en Provence (FR)

**Decision under appeal:**

**Decision of the Examining Division of the European Patent Office posted on 23 March 2011 refusing European patent application No. 06749987.1 pursuant to Article 97(2) EPC.**

**Composition of the Board:**

| | |
|---|---|
| **Chairman** | W. Sekretaruk |
| **Members:** | M. Müller |
| | G. Zucka |

## Summary of Facts and Submissions

I. The appeal lies against the decision of the examining division dated 23 March 2011, for reasons referring to the communication dated 25 October 2010, to refuse the application for lack of clarity and support, Article 84 EPC, and for lack of an inventive step, Article 56 EPC, over the documents

D1: Dhem J.-F., "Efficient Modular Reduction Algorithm in Fq[x] and its Application to 'Left to Right' Modular Multiplication in F2[x]", Proc. of CHES 2003, LNCS 2779, Springer-Verlag, pages 203-213,
D2: WO 2004/0111831 A2,
D3: US 2003/044014 A1, and
D4: US 2003/079139 A1

II. A notice of appeal was received on 1 June 2011, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 21 June 2011. The appellant requested that the decision under appeal be set aside and a patent be granted on the basis of claims according to a main or auxiliary request as filed with the grounds of appeal, apparently in combination with the application documents on file, namely drawings pages 1-2 and description pages 1-5, 8-11 as originally filed and description pages 6 and 7 as filed with letter of 8 April 2009.

III. With a summons to oral proceedings, the board informed the appellant about its preliminary opinion according to which the pending claims lacked clarity, Article 84 EPC 1973, and an inventive step, Article 56 EPC 1973 over D1-D4. In particular, the board questioned whether and to what extent the claimed subject matter could be said to be "cryptographically secure" and whether the claims established that the alleged technical effect of increased efficiency could be ascribed to the claimed subject matter due to its reliance on a "word-size" parameter w.

IV. In response to the summons, with letter dated 4 March 2015, the appellant filed amended claims 1-9 according to a main and a first auxiliary request and claims 1-5 according to a second auxiliary request and requested the grant of a patent based on one of these sets of claims. With the same letter the appellant informed the board that the appellant's representative would not attend the oral proceedings. The appellant further filed a document containing technical background on DSS (FIPS PUB 186-2), which is not relevant for the purpose of this decision, and a declaration by one of the inventors, Vincent Dupaquis, relating to how one skilled in the art would have read the description.

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

"A computer hardware-implemented cryptographic method comprising a modular polynomial reduction operation in a binary finite field, the modular polynomial reduction operation comprising:

precomputing and storing in memory a polynomial constant u(x) representing a bit-scaled reciprocal of a multi-word polynomial modulus m(x) having a length defined by a number of words;

estimating an approximate polynomial quotient q(x) for a polynomial p(x) to be reduced modulo m(x), wherein said estimating is executed upon p(x) in a computation unit by a polynomial multiplication over the binary finite field by said constant u(x);

characterized by:

generating in a random number generator a random polynomial error value E(x) having a degree that falls within a predetermined range and applying said polynomial error value to said approximate polynomial quotient to obtain a randomized polynomial quotient q'(x) = q(x) + E(x); and

calculating a polynomial remainder r'(x) = p(x) + q'(x) · m(x) in said computation unit by performing word-size shifts, said remainder r'(x) being of higher degree than said modulus m(x) but congruent to p(x) modulo m(x) and where the degree of p(x) is less than or equal to 2k+w, w being a word size in bits of the computer hardware and k being the length in bit number of the words representing the modulus m(x)."

Claim 5 of the main request reads as follows:

"A computational hardware for executing a cryptographic program comprising a polynomial modular reduction operation over a binary finite field, the hardware comprising:

a computation unit adapted to perform word-wide finite-field multiply and accumulate steps on polynomial operands retrieved from a memory and polynomial coefficient intermediate results from a set of working registers;

a random number generator for generating a random polynomial error value E(x) having a degree that falls within a predetermined range;

an operations sequencer comprising logic circuitry for controlling the computation unit and random number generator in accord with program instructions so as to carry out the method of one of claims 1 to 4."

The wording of the claims according to the dependent claims is immaterial for this decision.

VI. Oral proceedings were held in absence of the appellant on the scheduled day. At the end of oral proceedings, the chairman announced the decision of the board.

## Reasons for the Decision

*The invention*

1. The application relates to cryptographic methods based on modular arithmetic in finite fields. Such methods, the AES/Rijndael cipher being mentioned as one example (p. 1, lines 20-26), rely on polynomial reduction by a specified modulus.

1.1 Since this reduction operation is one of the most expensive operations in cryptography, a number of dedicated fast methods have been developed, one of which by Barrett. The application presents the necessary formulae for Barrett's algorithm adapted to modular reduction of polynomials in a binary finite field (see p. 8, lines 29-34, and p. 9, esp. lines 18 and 28).

1.2 The application mentions in general terms that "[m]athematical computations performed by cryptographic systems may be susceptible to power analysis and timing attacks" (p. 1, lines 26-28). Elsewhere, reference is made to "crypt[]analytic attacks that rely upon consistency in power usage to determine the modulus" (p. 11, lines 6-8).

1.3 The invention sets out to make Barrett's algorithm "more secure against crypt[]analysis attacks, while still providing fast and accurate results". To achieve this effect, the application proposes to "[inject] a random polynomial error E(x) [...] into the computed polynomial quotient to obtain a randomized quotient" (p. 10, lines 4-7).

1.4 The description discloses the mathematical steps to be performed in a "polynomial reduction operation", and then that "[f]or a modulus of high degree (multi-word) the operation can be performed with word shifts rather than bit shifts" (p. 9, lines 20-32). To this end, the formulae used are reformulated in terms of the "word size w", more precisely in terms of divisions by $x^{(2k+w)}$ and $x^{(k-w)}$ (see p. 9, lines 32-34). This is said to "simplif[y] handling of the polynomial quantities on computational hardware" (see p. 9, line 35 - p. 10, line 3).

1.5 The description further explains that the multi-word modular reduction is to be carried out on computational hardware which locates the operands within the RAM by means of a pointer and an indication of the operand length in terms of number of words (see p. 4, lines 7-25, esp. lines 20-25).

2. In the board's opinion it is evident for the skilled reader that "the operation" mentioned on page 9, line 31, refers to the polynomial reduction operation as a whole and, in particular, to the calculation of q(x) and u(x). Furthermore, in the board's view, the statement that the operation "can be performed with word shifts rather than bit shifts" (emphasis by the board) must be read as stating that bit shifts are replaced by word shifts throughout the operation.

2.1 In its summons the board had noted that divisions by $x^{(2k+w)}$ and $x^{(k-w)}$ correspond to word-size right shifts only if k is a multiple of w. The appellant agreed with this observation and argued that this was a matter of necessity and thus self-evident for the skilled reader (see letter of 4 March 2015, p. 2, 6th para., and the declaration by the inventor).

2.2 The board follows the appellant's argument and considers that the description, by introducing the modified formulae as enabling an implementation "with word shifts rather than bit shifts", discloses implicitly that for the purpose of the modified algorithm the degree k of the modulus must be a multiple of w.

*The prior art*

3. D1 discloses a variant of Barrett's method generalized to polynomial reduction in a binary finite field which is substantially equivalent to the one presented in the application (see D1, abstract, lines 6-7, and in particular p. 204, equation (1)) except for the exponents in the central formula (*loc. cit.*) which define the number of bit shifts to be performed. The central formula is based on bit shifts defined in terms of p, the degree of the modulus N(x), and "some value of β to be defined later" (see sec. 2, the para. just above equation (1)). In the sequel of the paper, it is noted that the calculation can be simplified for "$\beta \geq \alpha$" and, in particular, for "$\beta = \alpha$", where $\alpha = deg(U)-deg(N)$ is the difference between the degrees of the polynomial to be reduced and of the modulus (see sec. 1, 1st para. and the sentences just below equations (4) and (7)).

*Article 84 EPC*

4. The decision under appeal objected (see points 1 - 1.1.3) that the independent claims lacked clarity due to the reference of the pertinent binary finite field as $GF(2^n)$ and the lack of a definition of the relative

sizes of n and the degree k of the modulus. Since the reference to GF($2^n$) was deleted from the claims, this clarity objection has become moot. The board is also of the opinion that referring to a binary finite field without mentioning n does not cause any clarity problems in its own right. The board notes that present claims 1 and 5 now explicitly specify that the claimed operation is part of a computer-hardware implemented cryptographic method, as suggested by the examining division (see decision under appeal, point 1.2, penult. sentence). The board is also of the opinion that the operation being masked is properly and clearly referred to as a "modular polynomial reduction operation" even if, for inappropriate choices of E(x) vis-à-vis p(x), the operation may not actually be a reduction (see decision under appeal, point 1.2). The board not having any clarity concerns of its own is thus satisfied that the claims of the main request conform with Article 84 EPC 1973.

*Article 123 (2) EPC and claim construction*

5. Claim 1 is substantially based on claim 1 as originally filed. That the modulus has a "length defined by a number of words" is disclosed on page 4 (lines 20-25) which explains that the operand lengths are given in "number[s] of word" (see also original claim 8), that w is the word size of the computer hardware is disclosed *inter alia* in original claim 9, and that k is "the length in bit number of the words representing the modulus m(x)" is disclosed by the last paragraph on page 9 according to the interpretation given above.

5.1 Claim 1 of the main request contains the phrase "calculating a polynomial remainder $r'(x)=p(x)+q'(x)\cdot m(x)$ in said computation by performing word-size shifts" which literally suggests that the word-size shifts are used in particular, and possibly only, in the calculation of r'(x). In contrast, the only possibly relevant disclosure on page 9, last paragraph, states that it is "the operation [which is] performed with word shifts", *i.e.* the modular polynomial operation as a whole, and, in particular, the calculation of q(x). The calculation of the polynomial remainder r'(x) on the other hand is mentioned only on page 10, lines 23-32, based on a formula which does not require any word or bit shifts at all.

5.2 Therefore, the literal wording of claim 1 is not disclosed in the application as originally filed. At the same time, the board is of the opinion that the skilled reader of claim 1 would notice that the reference to word-size shifts cannot reasonably apply to the calculation of the polynomial remainder according to the given formula $r'(x)=p(x)+q'(x)\cdot m(x)$ alone and further in view of the description (*loc. cit.*).

5.3 The board also notes that the appellant, when it argued why amended claim 1 conformed with Article 123 (2) EPC in its submission dated 4 March 2015, explained by reference to page 9, lines 30-32, that "the computation of q(x) [...] can be performed with word shifts".

5.4 The board therefore considers that the mentioned phrase contains an obvious error by the appellant contrary to its express intentions which the skilled person would however be able to identify and interpret correctly, on the basis of the application as originally filed, as specifying "the operation" - as a whole, rather than the calculation of the polynomial remainder - "being performed by word-size shifts".

5.5 In the following, the board assumes this interpretation.

*Inventive step*

6. D1 is not concerned with cryptanalytic side channel attacks and thus has no occasion to disclose anything about protection against such attacks. D1 also does not mention the choice of β in view of the chosen hardware platform nor the exploitation of word shifts in the implementation of the algorithm.

7. The claimed invention therefore differs from D1 by

(a) the generation of a randomized polynomial quotient q'(x) based on a random polynomial error value E(x), and
(b) the calculation of the polynomial reduction operation by performing word shifts.

7.1 These features address different problems. Difference (a) is meant to increase security against crypt[]analysis attacks" (see description, p. 2, penult. para., and letter of 4 March 2015, p. 3, 6th para.) while difference (b) is argued to allow for a more efficient implementation on hardware with multi-word operands and instructions (see also p. 2, last para., and letter of 3 March 2015, p. 4, 3rd para.).

7.2 The preamble of claim 1 refers to a "cryptographic method comprising a modular polynomial reduction operation". The body of claim 1 does not state, however, where specifically in the cryptographic method the modular polynomial reduction is to be performed and what its parameters mean in that context.

7.3 For that reason, the board has its doubts - as indicated in the summons (point 6.3) - whether difference (a) in the claimed modular polynomial reduction operation could be said to increase cryptographic security as long as the claims did not specify that the masked operation indeed relate to a "secret" of the cryptographic method which might be the target of a cryptanalytic attack (see summons, point 6.3).

7.4 As regards difference (b), the board is satisfied that, as explained in the description (p. 1, lines 20-26), commonly known cryptographic methods rely on modular polynomial reduction operations, and that, therefore, such methods may profit from a different, possibly more efficient, implementation of modular polynomial reduction - independent of whether they "relate to a secret" or not.

7.5 Further with regard to difference (b), the board considers that the use of word shifts rather than bit shifts may be more efficient under certain circumstances, in particular for certain sizes of the modulus and the polynomial to be reduced, but doubts that this can be said for all such values. An increase of efficiency can hence not be attributed to the claimed method over its entire breadth, and the description provides no basis for the skilled person to determine the pertinent circumstances.

7.6 The board is, however, satisfied that the claimed implementation of the operation by word shifts, *i.e.* difference (b), enables a different implementation of the known algorithm exploiting a particular multi-word operand addressing scheme. In this regard the board notes specifically that for an operand given in terms of a pointer and a length in number of words (see description, p. 4, lines 20-25), a right shift by, say, one word can be implemented by a mere decrement of the operand length.

8. As mentioned above, D1 does not disclose or suggest the selection of the exponent β in terms of the word size w of the given computer hardware in view of implementing the algorithm in terms of word shifts. Nor do documents D2-D4 which rather relate to the security aspect of the present invention (by way of "masking", "brouillage" or "Verfremdung", resp.). Since, moreover, the board does not consider this modification of the known modular polynomial reduction operation to be obvious from common knowledge alone, the board comes to the conclusion that claim 1 shows the required inventive step over D1 in view of D2-D4, Article 56 EPC 1973. The same applies to claim 5 by virtue of its explicit reference to method claim 1.

9. As a consequence, the inventive merit of difference (a) vis-à-vis D1 and, in particular, the questions of whether it contributes to increased cryptographic security and the technical character of the claimed method can be left open.

10. According to the preceding analysis, the decision under appeal must be set aside. Moreover, the board deems the claims of the main request allowable vis-à-vis the prior art to hand. The board considered whether there was any indication on file that the claims according to the main request might not have been covered by the search, in which case the board would have had to remit the case for further prosecution under Article 111 (1) EPC. As a matter of fact, however, the claims as originally filed did refer to the algorithm modified in terms of word size (see claims 2, 4, 5, and 9-11) and some of

them had been considered as a possible basis for an allowable application according to the Extended European Search Report. The board therefore must assume that the search examiner was aware of the "word-size shift" feature and accordingly that the search must have covered this feature. The board therefore concludes that a remittal for further prosecution is not appropriate.

*The description*

11. The board notes that the description has not been adapted to the amended claims as required by Article 84 EPC 1973.

11.1 Specifically, the present description (p. 9, lines 30-32) discloses the use of word shifts as an option rather than, according to the present claims, an obligatory feature of the present invention.

11.2 The board also notes that the description mentions Barrett's method to "replac[e] the long division with multiplications and word or bit shifts [...] in order to estimate the quotient" (p. 8, lines 22-27). The board tends to consider that the mention of word shifts in this sentence may give the impression that a word-shift version of Barrett's method may have been known in the art. This is, however, contrary to the position consistently taken by the appellant in its submissions during examination and appeal according to which the word shifts were non-obvious over the prior art and established an inventive step. Since, as noted above, the search must be assumed to have covered this feature the board has no reason to question the appellant's position on this point. Even though the board therefore takes it that the reference to "word shifts" in that sentence refers to the version of Barrett's method presented in the application, the board considers that the sentence should be amended to avoid any possible confusion.

*Summary*

12. Since the board comes to the conclusion that independent claims 1 and 5 show the required inventive step and are clear and originally disclosed based on the only reasonable interpretation, the board considers that a patent should be granted based on claims 1-9 according to the main request. Given the fact, however, that the examining division must give the appellant an opportunity anyway to adapt the description, the board deems it also appropriate that the appellant should be allowed to correct the error in claim 1 to conform with the appropriate interpretation as explained above (see in particular point 5.4).

## Order

### For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the examining division with the order to grant a European patent on the basis of claims 1-9 of the main request, filed 4 March 2015, together with any necessary amendment to the description.

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