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 0556/14 - 3.5.06

Application Number: 03018048.3

Publication Number: 1365308

IPC: G06F21/00, G06F7/72

Language of the proceedings: EN

Title of invention:
Method of masking a private key used in a cryptographic operation

Patent Proprietor:
Certicom Corp.

Opponent:
Müller, Christoph

Headword:
Masking a private key/CERTICOM

Relevant legal provisions:
EPC 1973 Art. 54, 56, 100
EPC Art. 52, 54(3), 123(2)

Keyword:
The protection of a cryptographic computation against power analysis attacks is a technical effect
Inventive step - after amendment (yes)

Decisions cited:
T 1173/97, T 0641/00

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

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 0556/14 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 28 July 2016

Appellant: (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)
Respondent: (Opponent)	Müller, Christoph Ludwigstr. 22 79104 Freiburg im Breisgau (DE)
Representative:	Fechner, Benjamin Wendelsteinstrasse 29A 82031 Grünwald b. München (DE)
Decision under appeal:	**Decision of the Opposition Division of the European Patent Office posted on 29 October 2013 revoking European patent No. 1365308 pursuant to Article 101(3)(b) 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 opposition division, with reasons dated 29 October 2013, to revoke European patent No. 03 018 048.3, which claimed the priority of Canadian patent application CA 2258338 A1. The decision referred *inter alia* to the documents

D2: WO 1998/52319 A1 and
D3: WO 1998/35782 A1,

and gave reasons for the findings of the opposition division that the grounds for opposition under Article 100(a) EPC 1973 (in combination with Article 54(3) EPC) and Article 100(b) and (c) prejudiced maintenance of the patent as granted, and that maintenance of the patent as amended according to auxiliary request 0a did not meet the requirements of the EPC (see in particular reasons 8.1 of the decision). Further auxiliary requests were not admitted by the opposition division (see reasons 6.3 and 7.4).

II. The proprietor appealed the decision and paid the appeal fee on 7 January 2014. In its grounds of appeal dated 10 March 2014, it requested that the decision be set aside and that the European patent be maintained as amended according to a main or one of 15 auxiliary requests as filed with the grounds of appeal.

III. The respondent (opponent) requested that the appeal be dismissed.

IV. In an annex to a summons to oral proceedings, the board informed the parties of its preliminary opinion. With regard to the main request, it considered that the claimed invention did not extend beyond the application

as originally filed but that the claimed operation was insufficiently disclosed for the case in which the private key was divided into more than two parts. The board also considered that claim 1 of the main request lacked novelty over D3, which - as the priority claimed was considered valid - was relevant only under Article 54(3) EPC. Of its own volition the board raised the issue of whether a "method of masking" constituted a mere mathematical method and was hence excluded "as such" from patentability under Article 52 EPC. The board also expressed the preliminary opinion that claim 1 lacked inventive step over D2, Article 56 EPC 1973. With regard to the auxiliary request, various objections were raised.

V. In response to the summons, in a letter dated 16 May 2016 the proprietor (appellant) filed amended sets of claims according to a main and two auxiliary requests replacing the requests on file. It further argued why methods of masking had to be considered technical, and referred to three scientific articles published in August 1999, in 2005 and in 2012, respectively.

VI. Oral proceedings were held on 28 July 2016, during which the appellant filed amended claims 1 and 2 and requested that the patent be maintained on the basis of these claims in combination with the description and the drawings as granted.

VII. Claims 1 and 2 read as follows:

"1. A method of masking a private key used in a cryptographic operation of multiplying a point, P, on an elliptic curve with the private key, the method comprising the steps of:

(a) dividing said private key into a plurality of parts b_1, b_2 and storing the parts on a smart card;
(b) generating a random number π;
(c) deriving new parts $b_1 = b_1 + \pi \bmod n$ and $b_2 = b_2 - \pi \bmod n$, where n is the number of points on said elliptic curve, such that the new parts when added are equivalent to the original private key;
(d) storing the new parts on the smart card; and
(e) utilizing each of the new parts instead of the private key in said cryptographic operation by evaluating $b_1P + b_2P$.

2. A computer-readable medium comprising computer readable program code embodied thereon for causing a cryptographic processor to perform the method of claim 1."

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

Reasons for the Decision

The invention

1. The invention relates to a method for masking a private key used in cryptographic operations on a security token such as a smartcard against power analysis attacks (see paragraphs 2 and 9 of the patent).

1.1 The security of cryptographic systems relies on a particular piece of information being kept secret, and power analysis attacks try to extract information about the secret by statistically analysing the power

consumption of the security token when carrying out the cryptographic operation (paragraphs 4 and 5).

1.2 Side channel attacks in general, and power analysis attacks in particular, against cryptographic algorithms, and masking as a protection against them, are in principle well-understood by the skilled person. This was common ground between the parties and the board, but a statement to this effect is also contained in the background section of D2 (see page 2, paragraph 2: "... have been extensively studied for more than 50 years ..."). The attacker considers the security token "to be a black box which contains a known algorithm and an unknown key" (see D2, paragraph bridging pages 2 and 3) and, in order to obtain the required statistical information, repeatedly executes the algorithm with varying parameters under his control (see D2, page 2, lines 3-4). Masking is, roughly speaking, a technique of randomising the calculations carried out in each instance of the cryptographic algorithms, so that their result remains the same but no relevant statistical information about the key can be gathered by repeated execution.

1.3 The specific method according to the invention is shown in figure 5 and explained in particular in paragraphs 31 to 35 of the patent, corresponding to pages 9 and 10 of the application as originally filed.

1.4 First a private key d, which in elliptic curve cryptography is multiplied with a point P to derive a public key Q = dP, is "divided" into a plurality of parts (step (a) in claim 1). Specifically disclosed is a division into two parts b_1 and b_2 such that $d = b_1 + b_2$ (paragraph 32).

1.5 Then a random number π is generated and the values of the parts are updated as b1 = b1 + π mod n and b2 = b2 - π mod n (paragraph 34), where n is the number of points on the elliptic curve used (paragraph 31).

1.6 The cryptographic operation, in which the private key is "used" (see claim 1, preamble), is then carried out by "utilizing" the individual and modified "new parts" (see paragraphs 31 and 35, and claim 1, steps (b) and (c)).

Validity of priority and prior art

2. The respondent challenged the validity of the priority claimed.

2.1 It argued in particular (see letter of 22 July 2014, points 1.1 and 2.1-2.2) that the Canadian patent application CA 2558338 A1 did not disclose the claimed feature of "deriving new parts ... such that the new parts when added are equivalent to the original private key". Rather, in disclosing on page 9, lines 4-9, that "... the new parts are combined to be equivalent to the original private key value ..." it did not disclose the relevance of equivalence of the new parts to the *key as such* but only to its *value*.

2.2 The board considers that the skilled person would know that any randomisation used in masking must not affect the outcome of the overall cryptographic operation. As the outcome depends on the key *value* rather than the "key as such" (whatever that may actually mean) the skilled person would understand that claim 1, when specifying that the new parts must be "equivalent to the original private key", is in fact specifying an "equivalence to the originally private key *value*"

(emphasis by the board). This is reinforced by the fact that amended claim 1 in fact requires "that the new parts *when added* are equivalent to the original private key", which also clearly relates to the key value.

2.3 Therefore, the board disagrees with the respondent's objections and agrees with the opposition division in finding that the priority was validly claimed (see decision, reasons 4.3.1).

2.4 As a consequence, document D3 is prior art only under Article 54(3) EPC and thus only with regard to novelty, and the scientific articles filed with letter of 16 May 2016 are not prior art at all for the patent at issue.

Article 100(c) EPC 1973

3. The decision (see reasons 2.1.2 and 2.4-2.4.2) found claims 2 and 3 of the then main request to go beyond the application as originally filed, Article 123(2) EPC, due to the feature that generating random values and updating new parts had to occur "for each session". In this context, the decision also took issue with the feature that the new parts should be "updated with said random value" for each session. This objection is now moot because the present claims do not refer to several sessions or to a step of updating.

4. The respondent argued that claim 1 went beyond both the earlier application as originally filed and the application itself as originally filed, for essentially the same reason for which it argued that the priority claim was invalid, namely because the original application related to equivalence between the new parts and the private key value, whereas the present claims related to equivalence between the new parts and

the private key as such (see letter of 22 July 2014, points 1.2-1.3.2). The board considers this not to be the case, for the reasons given above under point 2 with regard to the priority issue.

5. The respondent further argued that neither the earlier nor the present application as originally filed disclosed a computer-readable medium as per granted claim 10 and present claim 2 (see letter of 22 July 2014, point 2).

5.1 The application as originally filed discusses known methods of protection against power analysis attacks in the particular context of portable cryptographic tokens such as smart cards (see e.g. page 1, lines 12 to 13 and 28; page 2, lines 19 to 20). When the application then establishes a need for better such protection for "current hardware environments" (see page 3, paragraph 3) and discloses the invention in the context of "processors" (see page 3, paragraph 4; figure 5; page 8, line 27 to page 10, line 2), the skilled person would, in the board's view, read this as referring in particular to processors on smart cards. The skilled person would understand that the processor on a smart card would carry out all steps of the claimed method: for step (a) see figure 5, second box, and page 9, lines 5-8; for step (b) see e.g. figure 5, third box; for steps (c) and (d) see page 9, lines 9-13; and for step (e) see page 9, lines 13-15. Moreover, the skilled person would derive from the description, directly and unambiguously, that the processor had to act on suitable "program code" which, by necessity, would have to be stored on the smart card, i.e. on a computer-readable medium.

5.2 The description and the drawings of the present and earlier applications being identical, this argument applies to the earlier application as well.

5.3 The board therefore comes to the conclusion that the reference to a computer-readable medium in claim 2 is compliant with Article 100(c) EPC 1973 and Article 123(2) EPC.

6. The board agrees with the appellant that the claimed storage of the parts of the private key and the new parts on a smart card are disclosed in the application as originally filed on page 9, lines 5-8 and 13. With reference to the equations "$dP \bmod n = b_1P + b_2P \bmod n$" and "$dP = \Sigma(b_i \pm \pi)P \bmod n$" disclosed on page 9, line 15, and in figure 5, lowest box, of the description as originally filed, the board agrees with the respondent (opponent) that it does not make sense mathematically to take the modulus of a point. However, the board also considers that the skilled person would understand, directly and unambiguously, that what was intended to be disclosed were the equations "$dP = b_1P + b_2P$" and "$dP = \Sigma(b_i \pm \pi)P$". Therefore, the board considers that the evaluation of $b_1P + b_2P$ in step (e) of claim 1 is originally disclosed, too.

7. In summary, the board concludes that neither the ground for opposition under Article 100(c) EPC 1973 nor Article 123(2) EPC prejudices maintenance of the patent in amended form, Article 101(2) and (3) EPC 1973.

Article 100(b) EPC 1973

8. The decision under appeal found that the claimed "equivalence" between the new part and the original private key, in particular since the number of parts

could be more than two, rendered the scope of then claim 1 "so broad as not to allow the skilled person to implement the invention over the whole claimed breadth without an undue burden" (see reasons 3.3.2 and 5.3.1). The opposition division also considered that "the obviously incorrect formulas of original page 9 and Fig. 5 [did] not give a clear and sufficient teaching of which and how to obtain [sic] the claimed equivalence over the entire claimed scope" (see reasons 5.3.3) and concluded that then claim 1 did not satisfy the requirements of Article 83 EPC 1973.

8.1 Since present claim 1 is now limited to only two new parts $b_1 = b_1 + \pi \bmod n$ and $b_2 = b_2 - \pi \bmod n$ and specifies that they are equivalent to the original private key "when added", the board considers it to be clear that the original private key should be the sum of b_1 and b_2. Thus limited, the board considers that the term "equivalence" is no obstacle for the skilled person to carrying out the claimed invention over the entire claimed scope without an undue burden.

8.2 Moreover, the skilled person would have, in the board's judgement, no difficulty in understanding that the occurrences of "mod n" in the equation disclosed on page 9, line 15, are erroneous and should be ignored. The board has no doubt that the skilled person would understand from the description the central idea of the invention, now that there are two parts, to be that the calculation of $Q = dP$ is replaced by $Q = b_1P + b_2P$.

9. In the decision under appeal the opposition division argued (see reasons 4.3.2-4.3.4) that the reference to n as the "number of points on an elliptic curve" did not cause any limitation to then claim 1 because such a curve always existed for any given n. As a consequence,

so the argument, this feature could not constitute a difference over D3.

9.1 As will be seen below, the novelty of present amended claim 1 over D3 does not depend on this feature.

9.2 In its letter of 22 July 2014 (points 6.1 and 6.2), the respondent argued with reference to Article 100(b) EPC 1973 that the skilled person would not, without undue experimentation, be able to find an elliptic curve the number of points on which corresponded to the value n, or, if the curve was given, to determine what to do with it.

9.3 The preamble and step (c) of amended claim 1 imply, to the board's satisfaction, that the claims relate to an operation in elliptic curve cryptography, of which the elliptic curve and the number of points n are given parameters. The board does not agree that these features, which place the claimed masking operation in the context of elliptic curve cryptography, have a negative impact on sufficiency of disclosure of the invention.

Article 52(2) and (3) EPC and Article 100(a) EPC 1973

10. Due to the express reference in claim 1 to a smart card on which the key parts and also the new parts are stored, the claimed method of masking is not a mathematical method as such which can be objected to under Article 100(a) EPC 1973 for lack of compliance with Article 52(2) and (3) EPC.

11. Moreover, due to the reference to the smart card and in view of the description, paragraphs 2 and 33, the skilled person would understand the claimed masking

operation to be an automated one to be carried out on the smart card.

Articles 100(a) and 54(1) and (2) EPC 1973 and 54(3) EPC

12. The split of the original private key into two parts, the computation of new parts $b_1 = b_1 + \pi \bmod n$ and $b_2 = b_2 - \pi \bmod n$, and the evaluation of $b_1P + b_2P$ are not known from either D2 or D3. Claim 1 is thus new.

Technical effect of masking

13. Central to any masking method is the modification of a mathematical method in such a way that its repeated execution is less prone to a statistical analysis revealing the properties of a secret.

13.1 Since the result of the computation must not change, this means that masking, in essence, relies on replacing one mathematical method by another which has an equivalent result.

13.2 However, the modified *computation* is meant to be better protected against power analysis (or other side-channel) attacks when carried out on hardware. As such, the idea of masking is well-established in the art as a protection against such attacks (see D2, page 2, paragraph 2).

13.3 The board accepts as a technical problem the protection of a cryptographic computation against power analysis attacks - if, and only if, the computation is actually carried out on hardware and thus open to such attacks.

13.4 The board also accepts that claim 1 specifies a masking method carried out on hardware. Even though claim 1

literally specifies only the storage of the key parts on a smart card, in the board's view the skilled person can only understand the method of claim 1 as a fully computer-implemented method.

14. The board therefore takes the position that the claimed randomisation steps, namely the calculation of two randomised key parts and the computation of $Q = b_1P + b_2P$ instead of $Q = dP$, does achieve some protection against power analysis attacks and thus have a technical effect.

14.1 In the board's judgement the assertion that a computation is only vulnerable to power analysis attacks when performed repeatedly and that, hence, the protective effect only materialises when the method is carried out repeatedly, is not at odds with that conclusion. The skilled person would understand that generating a *random* number - as opposed to picking just *any* number - involves carrying out a calculation which produces different numbers each time. Therefore, the protective effect of the claimed method against power analysis attacks can, in the board's judgement, be ascribed to the claimed step of generating a random number in each instance of the method.

14.2 The respondent argued that the claimed randomised split is not advantageous over other masking methods, in particular the one known from D2 proposing to replace the computation of x^d mod n with x^{d+it} mod n (page 11, paragraph 2). That is, the claimed method is neither more secure nor more efficient than that of D2.

14.3 For the question of whether the claimed method has a technical effect, these considerations are, however,

immaterial, as that must be decided without regard to the prior art (see e.g. T 1173/97, reasons 8).

14.4 The board thus finds that the claimed mathematical steps contribute to the technical character of claim 1 and therefore, following established jurisprudence of the boards of appeal (see in particular T 641/00, headnote 1), must be taken into account in the assessment of inventive step.

Article 100(a) and 56 EPC 1973

15. D3 being only relevant for the assessment of novelty, it is common ground that the most suitable starting point for the assessment of inventive step is D2. No other starting point for the inventive-step analysis was proposed by the respondent.

15.1 D2 discloses a method of masking a calculation involving a secret exponent d (see page 5, line 3) by replacing d by d plus what the appellant referred to as an "effective zero" i*t (see the appellant's letter of 16 May 2016, page 2, paragraph 4), and by then evaluating x^{d+it} mod n instead of x^{d} mod n (see D2, page 11, lines 6-9).

15.2 The differences between the claimed matter and D2 are

(a) that D2 relates to RSA whereas claim 1 relates to elliptic curve cryptography (ECC), and
(b) the masking of the secret by randomised splitting.

15.3 The problem solved by the invention over D2 can therefore be considered as adapting the masking method of D2 to other cryptographic operations.

16. The respondent argued that the randomised splitting steps do not make the claimed method more efficient than the one according to D2. On the contrary, in fact: while the method of D2 masks the given calculation by the addition of one multiplication and one addition, the claimed method would be adding two multiplications and one addition and thus be less efficient.

16.1 The board notes that the disadvantage of a method may be outweighed by an advantage it may also have. For instance, a slower method might have a statistically significant protective advantage against particular side channel attacks. The board hastens to add that the patent contains no detail whatsoever that might allow a judgement or even a sophisticated guess as to the relative security of the proposed measure against any particular power analysis attack. However, the board considers that the comparison between the claimed method and that of D2 cannot be reduced to the number of additions and multiplications.

16.2 The board also notes that inventive step is acknowledged if, having regard to the state of the art, the invention is not obvious to a person skilled in the art (Article 56 EPC 1973). It is not necessary that the invention is a technical improvement over the prior art.

17. The board is of the opinion that the claimed randomised splitting and the adding of an "effective zero" according to D2 are alternative approaches and that the change from the latter to the former is not suggested by the change from ECC to RSA. The respondent has also not put forward any fundamental mathematical considerations which would, to the board's satisfaction, suggest this change.

17.1 In particular, the respondent was not able to convince the board that the skilled person starting from D2 would be led, in an obvious way, to the randomised split according to the invention.

17.2 The board therefore judges that the claimed method shows the required inventive step over D2 by virtue in particular of difference (b).

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 European patent with the following documents:
   claims 1 and 2 as filed on 28 July 2016;
   description pages 3 and 5 as filed on 28 July 2016 and pages 2 and 4 as granted; and
   drawings, figures 1-5 as granted.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated