**Internal distribution code:**

(A) [ - ] Publication in OJ
(B) [ - ] To Chairmen and Members
(C) [ - ] To Chairmen
(D) [ X ] No distribution

# Datasheet for the decision of 13 June 2019

**Case Number:** T 1808/15 - 3.5.03

**Application Number:** 11178913.7

**Publication Number:** 2563055

**IPC:** H04W12/02, H04L29/06

**Language of the proceedings:** EN

**Title of invention:**
Method and devices for reducing detectability of an encryption key

**Applicant:**
Swisscom AG

**Headword:**
Reducing detectability of an encryption key/SWISSCOM

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

**Keyword:**
Inventive step - (no)



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

Europäisches Patentamt
European Patent Office
Office européen des brevets

**Beschwerdekammern**

**Boards of Appeal**

**Chambres de recours**

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

**Case Number: T 1808/15 - 3.5.03**

# D E C I S I O N
# of Technical Board of Appeal 3.5.03
# of 13 June 2019

| | |
|---|---|
| **Appellant:** (Applicant) | Swisscom AG<br>Alte Tiefenaustrasse 6<br>3050 Bern (CH) |
| **Representative:** | Mirza, Akram Karim<br>Swisscom (Schweiz) AG<br>GSB-Legal & Regulatory-LST<br>P.O. Box<br>3050 Bern (CH) |
| **Decision under appeal:** | **Decision of the Examining Division of the European Patent Office posted on 10 April 2015 refusing European patent application No. 11178913.7 pursuant to Article 97(2) EPC.** |

**Composition of the Board:**

| | |
|---|---|
| **Chairman** | F. van der Voort |
| **Members:** | K. Schenkel |
| | J. Geschwind |

## Summary of Facts and Submissions

I. This appeal is against the decision of the examining division refusing European patent application No. 11178913.7, with European publication number EP 2 563 055 A1. The refusal was based on the ground that the subject-matter of the independent claims 1, 7 and 13 as filed lacked inventive step having regard to the disclosure of the following document:

D1: Fabian van den Broek: "Eavesdropping on GSM: state-of-affairs", arXiv.org, 3 January 2011, URL: http://arxiv.org/abs/1101.0552

II. In its statement of grounds of appeal, the appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the claims as filed. Further, the appellant conditionally requested oral proceedings.

III. In a communication following a summons to oral proceedings, the board, without prejudice to its final decision, gave its preliminary opinion that the subject-matter of claims 1, 7 and 13 as filed did not appear to be new having regard to the disclosure of D3, and further indicated that if the subject-matter were found to be new at the oral proceedings, the question of inventive step would be discussed, taking D1 as closest prior art.

IV. With a letter dated 6 June 2019, the appellant provided further arguments and informed the board that it would not be attending the scheduled oral proceedings.

V. Oral proceedings were held on 13 June 2019 in the absence of the appellant.

The appellant requested in writing that the decision under appeal be set aside and that a patent be granted on the basis of the claims as filed.

At the end of the oral proceedings, after due deliberation, the chairman announced the board's decision.

VI. Claim 1 as filed reads as follows:

"A method of reducing detectability of an encryption key used in a communication network (1) to encrypt a message transmitted between a base station (10) and a mobile station (2), the method comprising:

determining (S31) in the message one or more selected bits (e1-e11) at random positions in the message; and

generating (S3) in the message random bit errors by inverting the selected bits (e1-e11), prior to transmitting the message over the air."

## Reasons for the Decision

1. Claim 1 - inventive step

1.1 The present application relates to a method of reducing the detectability of an encryption key used in a communication network for encrypting messages. For this purpose, random bit errors are introduced in the message before it is transmitted.

The object according to the application as filed is to provide a method for reducing detectability of an encryption key, which is not limited to random padding

or randomizing reserved bits (column 2, lines 9 to 15 and 40 to 44, and column 5, lines 42 to 48, of the application as published). The board notes that padding bits are used to pad data in GSM packets to a standard length and that padding takes place before encoding and, optionally, encrypting.

1.2 D1 is considered to represent the closest prior art. It relates to eavesdropping on the mobile communication system GSM. A GSM communication system is a communication network which includes a mobile station and a base station. D1 describes a method of capturing GSM signals and decrypting the signals by exploiting the fact that the content of several bursts sent through the air, after encryption is enabled, can be guessed for the most part, which gives known plain text samples (page 10, third paragraph). By means of a software project called "Kraken", tables are created as code books and, if a captured encrypted GSM signal can be found in the tables, the session key used for its encryption can be calculated, allowing decryption of the communication (page 10, second and fourth paragraphs). D1 notes that this approach requires the faultless reception of 64 consecutive bits.

D1 further discloses as a countermeasure against attacks against GSM a method called "random padding" (pages 12 and 13, sections "5 Countermeasures" and "5.2 Use random padding"). This method uses randomizing padding bits in order to remove a large source of known plain text messages. It is said to make Kraken attacks which aim at detecting the session key more difficult and is thus a method of reducing the detectability of an encryption key. No further details of the randomizing method are given in D1.

1.3 The method of claim 1 thus differs from the method disclosed in D1 in that the randomizing is done by determining one or more selected bits at random positions and by inverting the selected bits.

Since D1 does not provide further details on how to randomize the padding bits, the problem underlying the claimed subject-matter, taking D1 as a starting point, may be seen as finding an implementation for randomizing the bits.

The board notes that there are few ways to randomize the bits of a digital number. Bits which are selected in a deterministic way must be amended randomly. If a subset of the bits is selected randomly, these bits can be amended in a deterministic way or, albeit not necessarily, in a random way, since the bits have already been randomly selected. A skilled person using common general knowledge would have been aware of these possibilities and selecting one of them, namely randomly selecting bits and amending them in a deterministic way by inverting them, cannot therefore contribute to an inventive step. Furthermore, using this in the "random padding" method disclosed in D1 results in generating random bit errors in the message.

1.4 In view of the above, the skilled person, when starting out from the method of D1 and faced with the above-mentioned problem would, based on common general knowledge, randomize padding bits by determining at least one random position within the padding pattern and inverting the corresponding at least one bit, thereby arriving at a method which includes all the features of claim 1 without exercising inventive skill.

1.5 Appellant's arguments

1.5.1 The appellant argued that random padding is applied at the data level and not at the signal level. The board notes, however, that claim 1 does not specify when the random bit errors are generated in the message and thus does not exclude that the bit errors are generated before the message is encoded and/or encrypted. Further, claim 1 does not specify the message in which the bit errors are generated in such a way that it would exclude messages that have not yet been encoded and/or encrypted.

1.5.2 The appellant further argued that padding modifies irrelevant parts of a GSM message and has therefore no relevance for the solution according to the present application. However, since claim 1 does not exclude that the bit errors are generated in padding bits which are indeed irrelevant parts of the message, the board is not convinced by this argument.

1.5.3 The appellant further argued that the skilled person would, without applying hindsight, only draw from D1 the immediate conclusion that bad reception prevents eavesdropping and would not equate bits on the reception side with bits on the transmission side. Further, even if the skilled person had then been motivated to exploit that conclusion for prevention purposes, there would be more than one way of reducing the reception quality, for example by limiting the signal power.

The board notes, however, that D1 does not only draw the conclusion that reception errors make Kraken attacks more difficult. It also discloses countermeasures against attacks against GSM or, in other words, methods of preventing such attacks by

random padding on the transmission side (D1, page 12, section "5 Countermeasures"). It is thus not relevant whether or not there are other possible ways to reduce the reception quality.

1.6 In view of the above, the board concludes that the subject-matter of claim 1 as filed does not involve an inventive step (Articles 52(1) and 56 EPC). The request that a patent be granted on the basis of the claims as filed is therefore not allowable.

2. There being no allowable request, it follows that the appeal is to be dismissed.

**Order**

**For these reasons it is decided that:**

The appeal is dismissed.

The Registrar: The Chairman:

C. Moser F. van der Voort

Decision electronically authenticated