BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS	**BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE**	**CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS**

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

Datasheet for the decision of 31 January 2011

Case Number:	T 1131/07 - 3.4.03
Application Number:	00113051.7
Publication Number:	1073021
IPC:	G07F 7/10
Language of the proceedings:	EN

Title of invention:
Information processing apparatus, card and information processing system

Patentee:
Hitachi, Ltd., et al

Opponent:
-

Headword:
-

Relevant legal provisions:
-

Relevant legal provisions (EPC 1973):
EPC Art. 56

Keyword:
"Inventive step (yes)"

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 1131/07 - 3.4.03

DECISION
of the Technical Board of Appeal 3.4.03
of 31 January 2011

Appellant:

Hitachi, Ltd.
6 Kanda Surugadai 4-chome
Chiyoda-ku
Tokyo 100-8010 (JP)

Representative:

Beetz & Partner
Patentanwälte
Steinsdorfstraße 10
D-80538 München (DE)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted 12 January 2007 refusing European patent application No. 00113051.7 pursuant to Article 97(1) EPC 1973.

Composition of the Board:

Chairman: G. Eliasson
Members: R. Q. Bekkering
T. Bokor

Summary of Facts and Submissions

I. This is an appeal against the refusal of application No. 00 113 051 for lack of inventive step, Article 56 EPC 1973 (main request), over document

D1: WO 98 16883 A,

and for added subject-matter, Article 123(2) EPC (auxiliary request).

II. The appellant applicant requested that the decision under appeal be set aside and a patent granted on the basis of the following documents:

Claim:	Claim 1 filed with letter dated 17 November 2010;
Description:	Pages 1, 2 and 4 to 160 filed with letter dated 29 June 2010; Pages 3 and 3a filed with letter dated 17 November 2010; Pages 161 and 162 as originally filed;
Drawings:	Sheets 1-15, 17-33 as originally filed; Sheet 16 filed with letter dated 18 May 2005.

III. Claim 1 reads:

"A data processing apparatus comprising at least

a first information processing device (1401, 1501, 1601, 1701), *a second information processing device (1402, 1502, 1602, 1702) connected to said first information processing device by a data signal line (1410, 1510, 1611, 1709),*

a first encryption device (1403, 1503, 1603, 1703) between said first information processing device and said data signal line,

a first decryption device (1404, 1504, 1604, 1704) between said data signal line and said first information processing device,

a second encryption device (1411, 1505, 1605, 1705) between said second information processing device and said data signal line,

a second decryption device (1412, 1506, 1606, 1706) between said data signal line and said second information processing device, and

a key automatic reconfiguration device for automatically reconfiguring a key to be used in encryption and decryption in said first and second encryption and decryption devices,

wherein

a data signal from said first information processing device is encrypted in the first encryption device using said key and sent to said data signal line, and said encrypted signal from said first information processing device is received from said data signal line and decrypted in the second decryption device using said key before being supplied in an unencrypted state to said second information processing device;

a data signal from said second information processing device is encrypted using said key in the second encryption device and sent to said data signal line, and said encrypted signal from said second information processing device is received from said *data signal line and decrypted using said key in the first decryption device before being supplied in an unencrypted state to said first information processing device, and*

all said information processing, encryption and decryption devices and the data signal line are comprised within a single chip."

IV. The appellant essentially argued as follows:

A key point of view taken by the Examining Division in the decision under appeal was item 3.7 in the grounds on sheet 6 thereof, in which the Examining Division referred to the distributed encryption embodiment described also in citation Dl as an option thereof, and assumed that a skilled person would easily "reverse" or "turn around" the operation direction of one of the devices, thus arriving at the invention. This was erroneous for two reasons, namely
(1) a skilled person had, starting from the knowledge given by document D1, no reason for reversing the operation of one of the devices, and
(2) even if he would reverse the operation direction of one of the devices, a skilled person would arrive at a useless device.

Accordingly, the subject-matter of claim 1 involved an inventive step.

Reasons for the Decision

1. The appeal is admissible.

2. *Amendments*

Claim 1 is based on claim 9 as originally filed and on the description as originally filed (page 113, line 22 to page 126, line 22) with figures 23 to 26.

The amendments, thus, comply with Article 123(2) EPC.

3. *Novelty*

3.1 Document D1

3.1.1 Document D1 discloses an electronic data processing circuit having an operating module such as, for example, a microprocessor, at least one data memory and a data bus extending between the data memory and the operating module. In order to prevent "tapping" of the data traffic on the data bus, with the result that the program flow in the operating module can be observed and understood in an undesirable manner, it is proposed to transport the data encrypted in the electronic data processing circuit, so that devices are provided between the data bus and data memory or the operating module and data bus in order to encrypt and to decrypt the data traffic transported on the data bus (page 1, lines 5 to 9; page 2, line 23 to page 4, line 15).

3.1.2 In particular, the embodiment of figure 3 discloses a CPU 1 as an operating module and a plurality of data memories (a ROM 2, an EEPROM 3, a FLASH memory 4 and a

RAM 5). The data memories 2, 3, 4, 5 and the CPU 1 are connected to one another through a data bus (not shown in figure 3 (instead in figure 3 the CPU 1 exchanges data with the data memories 2, 3, 4, 5 through individual data lines 6, 7, 8, 9, 10, 11, 12, 13, 14 and 15)). A latch buffer 16, 17, 18, 19 is furthermore disposed between the CPU 1 and each of the ROM 2, the EEPROM 3, the FLASH 4 and the RAM 5, respectively (page 15, lines 8 to 19).

Encryption modules 20, 21, 22 and 35, which encrypt or decrypt the data traffic on the data lines assigned to them, are provided in the region between the ROM 2 and the latch 16, in the region between the latch 17 and the CPU 1, in the region between the latches 18, 19 and the CPU 1 as well as in the CPU 1 itself (page 15, lines 21 to 26).

The encryption modules 20, 21, 22 and 35 are constructed in such a way that the data traffic on the data lines assigned to them is respectively encrypted or decrypted only partially. A complete encryption or decryption results only upon cooperation of a respective one of the encryption modules 20, 21, 22 with the encryption module 35 in the CPU (page 16, lines 4 to 10).

3.1.3 Furthermore, the data processing circuit has a multiplexer 23, which is connected to the FLASH memory 4 through a data line 24. The multiplexer 23 is connected through a data line 25 to a timer 26, which can be fed a random number by a random number generator 28 over a data line 27. The multiplexer 23 also has a control line 29, through which it is connected to the ROM 2. An output of the multiplexer 23 is connected through control lines 30, 31, 32, 33, 34 to the encryption modules 20, 21, 22, 35. The encryption modules 20, 21, 22, 35 are supplied with a new key in response to an output signal of the multiplexer 23.

During operation, the electronic data processing circuit behaves as follows: With each execution of a command "CLR C", the ROM 2 transmits a control pulse to the multiplexer 23 over the control line 29. Thereupon, the multiplexer 23 retrieves one of three keys KEY 3, KEY 2, KEY 1 from the FLASH memory 4 over the data line 24, and transmits it to the encryption modules 20, 21, 22 and 35. If a predetermined operating time of the data processing circuit is exceeded without the multiplexer 23 being activated by the ROM 2, the timer 26 moves into action. The actuation of the timer 26 transmits a random number from the random number generator 28 to the multiplexer 23 over the data line 25. The multiplexer 23 then transmits the random number to the encryption modules 20, 21, 22, 35 (page 16, line 12 to page 17, line 4).

3.1.4 The data in the ROM 2 are stored in an encrypted manner, and they are only partially decrypted by the encryption device 20 during readout in the latch 16. Consequently, the data from the ROM 2 are transported on a data line 8 while still partially encrypted as far as the CPU 1, where they are completely decrypted by the encryption module 35. It is only thereafter that the data are ready for processing in the CPU 1.

The data which are provided in an encrypted manner in the EEPROM 3 are transmitted encrypted over a data line 9 to the latch 17, and relayed from there to the encryption module 21, where they are partially decrypted. From there, the still partially encrypted data pass through a data line 11 to the CPU 1, where they are completely decrypted by the encryption module 35 and are thereafter available for processing.

Data for the FLASH memory 4 and for the RAM 5 are initially respectively encrypted partially by the encryption module 35 and the encryption module 22, before they are stored completely encrypted in the FLASH memory 4 or in the RAM 5. For this purpose, the data which are partially encrypted in the encryption module 35 of the CPU 1 are transmitted over the data line 11 to the encryption module 22, where they are completely encrypted before they are handed over through respective data lines 13 and 14 to the latches 18, 19 respectively assigned to the FLASH memory 4 and the RAM 5. The encrypted data pass from the latches 18, 19 to the respective FLASH memory 4 or RAM 5 over data lines 12, 15.

When the data are read out of the FLASH memory 4 and of the RAM 5, they are initially respectively decrypted partially by the encryption module 22 and by the encryption module 35 before they are available for processing completely decrypted in the CPU 1 (page 17, line 6 to page 18, line 6).

By disposing the two encryption modules at different locations in the electronic data processing circuit, encryption of the data traffic is performed at two different locations. A typical manipulator will possibly perform only one encryption at a single location, specifically in the case of a single encryption module, and nevertheless not arrive at a useful result when employing the encryption. In the case of two encryption modules, which are accommodated at different locations, it is particularly difficult to perform an encryption, since two different locations of a microstructure can only be observed simultaneously in a particularly difficult way. The encryption modules which are thus constructed can, for example, be constructed in such a way that one encryption module encrypts or decrypts the lower four bits of a data bus at one location, while the other encryption module encrypts or decrypts the remaining bits of the data bus (page 10, lines 7 to 34).

3.1.5 Thus, document D1 discloses, using the terminology of claim 1, a data processing apparatus comprising at least

a first information processing device (CPU 1),

a second information processing device (eg RAM 5) connected to said first information processing device by a data signal line (11, 14, 15),

a first encryption device (35) between said first information processing device and said data signal line,

a first decryption device (35) between said data signal line and said first information processing device,

a second encryption device (22) between said second information processing device and said data signal line, a second decryption device (22) between said data signal line and said second information processing device, and

a key automatic reconfiguration device (23, 4) for automatically reconfiguring a key to be used in encryption and decryption in said first and second encryption and decryption devices.

Furthermore, in D1 a data signal from said first information processing device (CPU 1) is (partially) encrypted in the first encryption device (35) using said key and sent to said data signal line (11).

Moreover, in D1 an encrypted signal from said second information processing device is received from said data signal line and (partially) decrypted using said key in the first decryption device (35) before being supplied in an unencrypted state to said first information processing device (CPU 1).

Finally, in D1 all said information processing, encryption and decryption devices and the data signal line are comprised within a single chip (cf page 3, lines 5 to 10; page 4, lines 17 to 23).

3.1.6 However, as discussed above, in D1 the data in the second information processing device (eg RAM 5) are present in encrypted form.

Thus, D1 does not disclose the following features of claim 1:

- said encrypted signal from said first information processing device is received from said data signal line and decrypted in the second decryption device using said key before being supplied in an unencrypted state to said second information processing device; and

– a data signal from said second information processing device is encrypted using said key in the second encryption device and sent to said data signal line.

The subject-matter of claim 1 is, thus, new over document D1 (Articles 54(1) and (2) EPC 1973).

3.2 The subject-matter of claim 1 is also new over the remaining cited prior art which is more remote.

4. *Inventive step*

4.1 The closest prior art is considered to be provided by document D1 discussed above.

The above distinguishing features of claim 1 over document D1 result in the data being present in both the first and second information processing devices in unencrypted form. This, as argued by the appellant, avoids the need for key administration. In particular, where eg data are stored in a memory in encrypted form, any retrieval of this data at a later point in time requires the use of the same key for decryption. When altering encryption and decryption keys are used, track must be kept of the respective key used requiring some form of key administration and, thus, adding complexity to the data processing apparatus.

Accordingly, the objective problem to be solved relative to D1 is to simplify the apparatus in this respect.

4.2 In the decision under appeal (point 3.6) it is argued that the skilled person would select without any inventive step, among the limited number of obvious possibilities for the encryption/decryption sequence of the data exchanged between the data processing/storage components, the option in which the second encryption/decryption device (see D1, figure 3, ref 20, 21, 22) is used to decrypt, rather than further encrypt, the encrypted data before storing them in the second information processing device, in order to achieve greater interoperability, at the expense of the security of the apparatus disclosed in D1.

However, as argued by the appellant, there is nothing in D1 or otherwise suggesting the skilled person to modify D1 so as to store the data in the memory devices in plain-text (decrypted form). Neither would it simply suffice to reverse the operation of eg component 22 in the embodiment of figure 3 of D1. As discussed above, encryption module 22 receives parts (eg the lower four bits of the data bus) of the data in unencrypted (plain-text) form from data line 11, encrypts the data and supplies them in encrypted form to eg RAM 5 for storage. Other parts of the data (eg the upper four bits of the data bus) are encrypted in encryption module 35 and supplied via data line 11 in encrypted form to eg RAM 5 for storage. Reversing the operation of encryption module 22 would result in decrypting the unencrypted (plain-text) data received from the data line and supplying them to eg RAM 5 for storage. The result of this odd operation would neither result in the data being supplied in an unencrypted (plain-text) state to the second information processing device (eg RAM 5) as per claim 1, nor would it obviate the need for key administration as presumably the same key is needed when retrieving the date at a later point in time.

4.3 Accordingly, in the board's judgement, the subject-matter of claim 1, having regard to document D1, is not considered to be obvious to the person skilled in the art.

Furthermore, none of the remaining cited prior art documents render the claimed solution obvious.

Accordingly, the subject-matter of claim 1, having regard to the available state of the art, is not considered to be obvious to the person skilled in the art and, thus, involves an inventive step (Article 56 EPC 1973).

5. The patent application as amended also meets the remaining requirements of the EPC, so that a patent can be granted on the basis of these documents.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the department of first instance with the order to grant a patent in the following version:

   Claim: Claim 1 filed with letter dated 17 November 2010;

   Description: Pages 1, 2 and 4 to 160 filed with letter dated 29 June 2010;
   Pages 3 and 3a filed with letter dated 17 November 2010;
   Pages 161 and 162 as originally filed;

   Drawings: Sheets 1-15, 17-33 as originally filed;
   Sheet 16 filed with letter dated 18 May 2005.

Registrar:	Chair:
S. Sánchez Chiquero	G. Eliasson