# EXHIBIT 11

## Notice of Reasons for Rejection

| | |
|---|---|
| Patent Application Number | 7th Year of Heisei (1995) Patent Appl. No. 507561 |
| Drafting Date | 15th year of Heisei (2003) April 17 |
| Patent Examiner | AOKI, Shigenori 4229 5M00 |
| Applicant's Agent | IKEUCHI, Yoshiaki (and 1 other) |
| Applicable Article(s) | The body of No. 29, No. 29(2), No. 36 |

The present application should be rejected for the reasons given below. If the applicant has any opinion about this notice, please submit your letter of opinion within 3 months of the dispatch date of this notice.

### Reason

[A] The invention relating to the following claims of the present application should not be granted a patent as it does not comply with the requirements stipulated in Japanese Patent Act, Article 29, body of paragraph 1, with respect to the following point(s).

### Record

Claims: 1-4
Remarks:

Even if an invention of a method for creating encryption by appropriately combining characters, numbers, symbols, and so forth, contributes significantly to industries, particularly to commercial transactions, and even if the creation method takes scientific precision to an extreme, because the invention does not use any type of apparatus in the process thereof, is recognized as a method of conscious expression by way of encryption if it is understood to be a communication method by way of encryption, and does not implement a technical means utilizing natural laws, it cannot be recognized as an invention defined by Japanese Patent Act, Article 2, and in principle thereby it is understood to not fulfill patent requirements for Japanese Patent Act, Article 29.

Further, the invention according to claims 1-4 of the present application defines a method for encrypting a packet as a function of a packet sequence number and a sending overflow sequence number in a communication system, and for decrypting the encrypted packet as a function of the packet sequence number and a receiving overflow sequence number, thereby essentially defines a communication method by way of encryption, and uses no type of apparatus in the process thereof. Accordingly, there is no description given of how hardware resources are used as a resolution means of a technical problem and the above principle can therefore be applied.

Therefore, the invention according to claims 1-4 cannot be recognized as an invention defined by Japanese Patent Act, Article 2 and thus does not comply with the requirements of Japanese Patent Act, Article 29.

Claims: 9
Remarks:

# Final Rejection

|  |  |
|---|---|
| Patent Application Number | 7th Year of Heisei (1995) Patent Appl. No. 507561 |
| Drafting Date | 16th year of Heisei (2004) October 13 |
| Patent Examiner | AOKI, Shigenori 4229 5M00 |
| Title of Invention | METHOD AND DEVICE TO PROVIDE ENCRYPTED PROTECTION OF A DATA STREAM IN A COMMUNICATION SYSTEM |
| Applicant | Motorola Incorporated |
| Agent | IKEUCHI, Yoshiaki (and 1 other) |

The present application should be rejected according to reason [C] described in the Notice of Reasons for Rejection dated April 17, H15 (2003).

Moreover, the content of the Argument and the Amendment was examined, but sufficient grounds to overturn the Reasons for Rejection were not found.

Remarks

1. The applicant asserts in a submitted Argument dated October 30, H15 (2003) that the invention according to claims 1-10 of the present application (hereafter referred to as "the invention of the present application") has patentability and gives as a reason the point that in 'D. W. Davies and W. L. Price / Translation supervised by Tadahiro Uezono, "Network Security", Japan, Nikkei McGraw Hill, Inc., December 5, 1985, 1st Ed. 1st Printing, pg. 307-312' (hereafter referred to as "Citation 1") and Japanese Unexamined Patent Application Publication No. S63-167588 (hereafter referred to as "Citation 2") given in the aforementioned Notice of Reasons for Rejection, the use of a packet sequence number and an overflow sequence number to encrypt and decrypt data is not a simple selection of one from among a large number of variables used as keys.

The following examination was conducted on the Reason and the Assertion.

2. First, we will examine whether the Reason is valid to support the Assertion.

The submitted Argument dated October 30, H15 (2003) states that the packet sequence number is data embedded in converted respective data packets, and the data are not transformed or repeated by the packet. Meanwhile, in the scrambling process described in Citation 2, the initial value data is data superimposed on the scrambled source video signal and is regularly modified. Such being the case, the packet sequence number and the initial value data are both used as the data to generate a pseudo random bit stream as well as have similar data modification and conversion means with the other side, and therefore the packet sequence number of the invention of the present application, with respect to protecting a data stream through encryption, corresponds to the initial value data described in Citation 2.

Furthermore, in the submitted Argument dated October 30, H15 (2003), a description is given in that the overflow sequence numbers in the invention of the present application are by no means transmitted to the terminal of the communication path, and are neither embedded into the data packet, nor derived from data embedded in the data packet, and are determined independently by the respective communication device for sending and the communication device for receiving. Meanwhile, with the scrambling process described in Citation 2, the transmission count control means and the transmission count

| | |
|---|---|
| [Document Name] | Amendment (Formal) |
| [Control Number] | P-1178HOSH |
| [Date Submitted] | Heisei 17 (2005) April 6 |
| [Attention] | Director General of the Patent Office |
| [Indication of Case] | |
| [Judgment Number] | Objection 2005-1002 |
| [Application Number] | H07-507561 |
| [Amending Party] | |
| [Identification Number] | 390009597 |
| [Name] | Motorola Incorporated |
| [Citizenship] | United States of America |
| [Agent] | |
| [Identification Number] | 100083574 |
| [Patent Attorney] | |
| [Name] | IKEUCHI, Yoshiaki |
| [Telephone Number] | 045-211-2795 |
| [Dispatch Number] | 016811 |
| [Amendment 1] | |
| [Amended Document Name] | Demand for Trial |
| [Amended Item Name] | Reason for Request |
| [Method of Amendment] | Modification |
| [Content of Amendment] | |

[Reason for Request]

[Procedural History]

| | |
|---|---|
| International Date of Application | Heisei 6 (1994) July 11 |
| (Date of Submitting Translation) | (Heisei 7 (1995) April 24) |
| Notice of Reasons for Rejection (First Time) | Heisei 15 (2003) April 30 (Dispatched) |
| Argument | Heisei 15 (2003) October 30 |
| Amendment | Heisei 15 (2003) October 30 |
| Notice of Reasons for Rejection (Second Time) | Heisei 15 (2003) Dec 16 (Dispatched) |
| Argument | Heisei 16 (2004) June 14 |
| Final Rejection | Heisei 16 (2004) October 13 |
| Transmittal of the Examiners Decision | Heisei 16 (2004) October 19 |
| Demand for Trial | Heisei 17 (2005) January 17 |
| Amendment | Heisei 17 (2005) February 16 |

[Main Points of the Final Rejection]

(a) The Reasons for Rejection given in the original decision are as follows: because the invention of the present application is an invention that can be easily achieved by a person skilled in the art on the basis of the published article "Network Security" (Citation 1) and the invention described in Japanese Unexamined Patent Application Publication No. S63-167588 (Citation 2) which have been in circulation in Japan prior to the application date of the present application.

(b) The reason therefor, in essence, is as follows: as an I field encryption method for encrypting a packet described in Citation 1, with adoption of technology to create a pseudo random bit stream described in Citation 2, conceiving a functional configuration of using information that corresponds to an overflow sequence number and information that corresponds to a packet sequence number in order to encrypt and decrypt data does not exceed the range which could be easily achieved by a person skilled in the art as indicated in the Notice of Reasons for Rejection dated April 17, H15 (2003).

[Reason that the Invention of the Present Application should be Granted a Patent]

(1) Description of the Invention of the Present Application

The invention of the present application relates to a communication device and a method for providing protection through encryption of a data stream in a communication system having a physical layer, data link layer, and network layer, and is characterized in that, by using an overflow sequence number not transmitted from one end to the other end of a communication path, each of a communication device for receiving and a communication device for sending can independently execute an algorithm for such overflow sequence number independently from the output of an algorithm executed by another communication device, and without such output being known.

The invention of the present application, on the basis of this type of essential configuration, is significantly simpler than the conventional configuration, and achieves a superior effect namely in providing a technique in which the processing load is lighter. Because new uses are continuously added to cellular phones and so forth, processing performance and battery life are increasingly critical, and therefore, reducing the processing load as well as thereby increasing the battery life is an extremely important matter. The invention of the present application is an invention which allows such needs to be suitably dealt with.

(2) Indication of the Grounds for Correction

The corrections comprising, "as a function of the packet sequence number, intermittently incrementing the sending overflow sequence number," and "as a function of the packet sequence number, intermittently incrementing the receiving overflow sequence number," of the patent claims in the Amendment dated February 16, H17 (2005) are based, for instance, on a description of page 7, lines 21-24 of the Specification of the initial application. In other words, this indicates that, as shown also in Figure 1, when the sequence number (116) completes one cycle, the 24 bit length overflow counter 124 is incremented as instructed by, for example, the overflow signal 122. In other words, it is thought that the wording "incrementing" is better suited to the description in the Specification than the wording "updating" in the preceding claims for the overflow sequence number. Further, the wording, "intermittently" applies to the fact that the overflow sequence number is not incremented with respect to each respective data packet, but is incremented only when the overflow signal 122 is generated after the packet sequence number completes one cycle.

(3) A Comparison between the Description of the Cited Examples and the Invention of the Present Application

In the Argument submitted by the applicant on June 14, H16 (2004) in the steps of the examination, the applicant, with respect to the invention of the present application, also stated that the overflow sequence number is determined on the basis of the roll over of the packet sequence number, and the overflow sequence number is determined and maintained internally within each device, thereby enabling interception and so forth to be prevented without transmitting outside of either device. In other words, even if a specific packet were intercepted, the overflow sequence number used for encryption and decryption of the packet cannot be detected; the overflow sequence number is by no means embedded in the packet and cannot be retrieved from other data of specific packet(s) without the packet sequence number rolling over. During the rollover of the packet sequence number, the overflow sequence number used for encryption and decryption of the packet is independent from the data embedded in the packet and is not a function of the data in the packet, which is to say that it cannot be retrieved from data in the packet.

In addition, the applicant makes it possible by encrypting a packet by using an overflow sequence number, so that the respective communication device for sending and communication device for receiving can determine independently whether or not to increment the overflow sequence number, and at the same time, can preserve these overflow sequence numbers in a synchronized state without the need of transferring the overflow sequence number from one end to the other end of the communication path. In other words, the overflow sequence numbers are independently determined by the respective communication device for sending and the communication device for receiving, and this means that the respective sending and receiving communication devices can independently determine their own respective sending and receiving overflow sequence numbers. By independently determining their respective sending and receiving overflow sequence numbers, each of the communication devices can determine the overflow sequence number independently from the output of algorithms executed by other communication devices and without such output being known.

In regard to this, Citations 1 and 2 are cited in the steps of the examination, and the invention of the present application was deemed to be an invention which can be easily conceived on the basis of the combination of these Citations.

However, the applicant of the present application believes the configuration of the invention of the present application is obviously different for the reasons given below from that obtained by combining Citations 1 and 2.

In regards to Citation 1, the Remarks field for Reason [C] of the Notice of Reasons for Rejection dated April 17, H15 (2003) (dispatch date: April 30, H15 (2003)) states that a description is given of an I field encryption method for encrypting only information fields (data link service data unit) as encryption at the data link layer of the OSI protocol.

Further, in regards to Citation 2, the detailed opinion of the examiner is indicated in the Reasons for Rejection of the original decision. In Citation 2, as also indicated in Figure 1 thereof, the synchronization counter (transmission count control means 14) counts the synchronization signals of each respective packet, generates a count value of 1-N (or 0- (N-1)), which then returns to 1 (or 0). Each time the count reaches N, the transmission count control means 14 provides a timing signal to the initial value generation means 15, and such timing signal generates a new initial value by triggering the initial value generation means. The timing signal is also used in order to reset the count to 1 (or 0). The respective count values and the initial value generated by the initial value generation means are transferred to the initial value conversion means 16. The initial value conversion means 16 generates a "random number signal" on the basis of the received count value and initial value. The information signal that is to be transferred next is scrambled by using this random number signal. Between the timing signals (received only once at each N count), the initial value conversion means latches the received initial value from the initial value generation means and uses the same initial value to generate each random number.

Next, the receiving side (decoder side) of Citation 2 also determines the count value on the basis of the synchronization signal and determines the timing signal on the basis of the count value. However, such timing signal is only used to reset the count value. What should be noticed here is that the receiving side (decoders could) does not have an initial value generation means, but instead, the initial value data is extracted from the transmitted signal (with a data extraction means 21).

When comparing the configuration in Citation 2 with that of the invention of the present application, the count value generated by the synchronization counter (transmission count control means 14) of Citation 2 can be seen as similar to the packet sequence number of the invention of the present application. This is the value that changes from one packet to the next packet and which can be directly drawn out from the data in each packet. Accordingly, with sufficient time and processing resources, scrambling by means of the synchronization count can be intercepted and detected by a third-party.

However, the timing signal generated by the synchronization counter of Citation 2 does not change at the base of each packet and therefore cannot be drawn out from the data of the respective packets. What the examiner, in the Reasons for Rejection of the original decision, judged to be similar to the overflow sequence number of the invention of the present application seems to be the timing signal of Citation 2, and more specifically, the operation of the timing signal combined with the new value generation means 15 -- in which a new initial value is generated only intermittently and not for each packet -- is seen to be judged as similar to the overflow sequence number of the invention of the present application.

However, what is critical to note is that what is used to scramble the information signal is not the timing signal but the new initial value generated each time a new timing signal is generated. In addition, unlike the overflow sequence number described in the amended claims of the present application, the timing signal of Citation 2 is absolutely not incremented and is nothing more than a trigger signal transmitted to the initial value generation means.

The configuration in Citation 2 has several weaknesses in comparison to that of the invention of the present application. The use of the timing signal in combination with an initial value requires a more complicated circuit configuration which includes a random number generator in order to generate a new initial value each time the timing signal is generated, and obviously has a greater processing burden compared to simply using an overflow sequence number stored in a buffer such as that in the invention of the present application and simply incrementing the overflow sequence number each time the packet sequence number rolls over. Accordingly, it is obvious that the configuration according to the invention of the present application is simpler and has a lighter processing load. Because new uses (applications) are continually added to cellular phones as described above, the usage potential of the processor and battery life are continually important matters, and it is obvious that lightening the load of the processor thereby extending battery life becomes increasingly important.

In addition, in Citation 2, what is used for scrambling the information signal is the initial value generated by the initial value generation means 15 and not the timing signal, and therefore, some type of adjustment of the initial value is required between the devices of the sending side and the receiving side in Citation 2. However, in Citation 2, no initial value generation means is equipped at the receiving side (decoder side), and this differs from the sending side (encoder side). In order to make this type of adjustment possible, in Citation 2, a "data extraction means 21" (Figure 1) is used at the receiving side, and the initial value is thereby extracted from the received data. (Although the decoder side detects the synchronization pattern and generates the count value (22a) and the timing signal (24a), the timing signal is used to do nothing more than to reset the count value when the count reaches N (or (N-1)) with the transmission count means 22). Accordingly, the initial value used to scramble the information signal is actually communicated from the sending side (encoder side) to the receiving side (decoder side), and is obviously not independently determined at the respective ends of the communication path. Therefore, there is a greater potential for interception by a third-party in the invention of Citation 2.

Conversely, the invention of the present application uses an overflow sequence number that is not communicated from one end to the other end of the communication path. By using an overflow sequence number, the respective receiving side communication device and sending side communication device execute an algorithm for such overflow sequence numbers independently from the output of algorithms executed by other communication devices, and without such output being known. In this way, the configuration is clearly different from the configuration at the time of the initial value used in Citation 2.

Accordingly, the use of an overflow sequence number such as that in the invention of the present application was not considered in Citation 2. Accordingly, even when combining such Citation 2 with Citation 1, it is believed that the invention of the present application could not be easily conceived by a person skilled in the art. In other words, it is believed that the invention of the present application proposes an obviously different configuration and active effect than that which would be obtained by combining Citations 1 and 2.

[Conclusion]

According to the above description, the invention of the present application is not an invention which could be easily invented by a person skilled in the art from the inventions described in Citation 1 and Citation 2.

Therefore, we request that the original Final Rejection be rescinded and that the invention of the present application be accepted for patenting.

[List of Submitted Items]

[General Power of Attorney Number] 9104678

# Decision

Objection 2005- 1002

1303 East Algonquin Road, Schaumburg, IL USA
Demandant: Motorola Incorporated

Ikeuchi International Patent Agency
2F Sekiuchi Kawashima Bldg. 1-4-2 Ohta-cho, Naka-ku, Yokohama-shi, Kanagawa-ken
Agent/Patent Attorney: IKEUCHI, Yoshiaki

The following decision has been given in regards to the Case for Trial against Examiner's Decision of Rejection for “A Method and Device for Providing Encrypted Protection of a Data Stream in a Communication System“, Patent Application Number H07-507561 (International Disclosure: March 2, H7 (1995), WO95 / 06374, domestic Japan publication date: April 2, H8 (1996), Published Japanese Translation of Foreign Application Patent Number H 08-503113, Number of Claims: 10).

Conclusion

Rescind original Final Rejection.

The invention of the present application should be granted a patent.

Reason

The present application is an application dated July 11, H6 (1994) (Priority claim, August 26, 1993 in the USA according to the Paris convention), and the invention according to claims 1 through 10 of the present application is acknowledged as specified according to the items described in claims 1 through 10.

Further, the present application should not be rejected according to the Reasons for Rejection of the original Final Rejection as a result of the investigation of the reasons.

In addition, no other reason for rejecting the present application is found.

Therefore, it is decided according to the conclusion.

May 24, H19 (2007)

Chief Trial Examiner Patent Trial Examiner ISEKI, Morizou
Patent Trial Examiner ODA, Hiroshi
Patent Trial Examiner AIZAKI, Hirotsune

[Decision Classification] P 18 . 121 - WYF (H0 4L)