EXHIBIT 10

7-507561

Patent 3983281

Registration Date 07.13, 2007 (H19

International Patent Application Number PCT/US94/07672

Decision —

Designation 5J Matsuo

Public Order and Morality

Pritrial PL Examination

Obejction 2005-1002

5K013

Decision

Priority Date 5 yr 8 mo 26 date

Dept.	Examiner
5W	
5M	

(Public) Int'l Patent Classification
(Subclass, Group, IPC-Subdivision Symbol and File Discrimination Symbol

(公表) 国際特許分類 (サブクラス	グループ	識別	盆
H04L 9	02		A
H04H 1	00		F
H04B 7	26	109	R

(公表) 分類の続き 有・無

併記分類

併記分類の続き 有・無

(Public) Classification Cont'd Yes.No
Joint Classification

Joint Classification Cont'd Yes.No

担当再指定分類

H04L 9/00	631

Assigned Redisignation Category

Priority Claims (Domestic)

優先権(国内)主張

Present Application No. — ( )
Present Application No. — ( )
Present Application No. — ( )

Foreign

外国

Present Application No. —

Request for Examinatino

year month date 12.8.17

5K013

1	2	3	4	5	6	7	8	9	10	11	12
送達書類	翻訳文	官公庁	パリ優先権	国優先内権	選択通知	国審際査予報備告	条補約19条正	条補約34条正	11-1方補式正	11-2方補式正	国無内効優通先知

Applicant 出願人

Int'l Publication Date 国際公開日 17.3.-2

Publication Date 公表日 8,4,02

国際公開番号 WO 95/06374

H 8 No. 503113

Int'l Publication No.

公告日 Publication Date

平成 年公告第 号 Heisei Publication vol.

保管 Storage No. [redacted]

No.

Agent 代理人 Shinnosuke Ohnuki 大貫進介 池内義明外1名 Yoshiaki Ikeuchi (and 1 other)

1. Submitted Documets, 2. Translations, 3. Offices, 4. Priority under the Paris Convention, 5. Int'l Priority, 6. Notice of Selection, 7. Int'l Preliminary Exam. Report
8. Correction under the PCT Article 19, 9. Correction under th PCT Article 3,

10. 11-1 Formality Amendment, 11. 11-2 Formality Amendment and 12. Notice of Invalidation of Internal Priority

Response to Office Action

Accepted
October 30, 2003 (H.15)

Patent Office
15.10.31
Applicant Support
Division
Tanaka

Dear Mr. Shigenori Aoki
Commissioner of the Japan Patent Office

1. Case
   Patent Application H7-507561
   (PCT/US 94/07672)

2. Title of the Invention
   Method and Apparatus for Providing Cryptographic Protection of a Data Stream in a Communication System

3. Applicant

Address	1303 East Algonquin Road Shaumburg, Illinois 60196 United States of America
Name	Motorola Incorporated
(Nationality)	United States of America

4. Agent

Address	Ikeuchi International Patent Office Sekiuchi Kawashima Building 1-4-2 Ohta-cho, Chuo-ku Yokohama, Kanagawa 231-0011 Tel: 045 (211) 2795
Name of the Agent	(8357) Yoshiaki Ikeuchi

Yoshiaki
Ikeuchi
Patent
Attorney

5. Date Office Action was received
   April 17, 2003 (H15) (sent on April 30, 2003)

Examination

Illegible

6. Reasons

(1) We received the Office Action dated on April 17, 2003 (H15) (sent on April 30, 2003 (H15)) regarding the above referenced application. Claims 1-4, 9 and 10 were rejected on the ground in which they do not meet the requirements for patentability stipulated in the main clause of the Article 29(1) of the Patent Law (Reason A).

Furthermore, the claims were rejected due to the inaccuracy of the Specification and Drawings in the application, which failed to meet the requirements for patentability stipulated in the Patent Law Article 36(4) (Reason B).

Additionally the following references,:

1. D. W. Davies and W. L. Price authors / Tadahiro Uwazono, "Network Security" Japan, Nikkei, McGraw Hill. December 5, 1985, 1st Ed. 1st Printing, pg. 307-312
2. Publication of Japanese Laid Open Patent Application S63-167588

were cited in the Office Action, and the invention in relation to Claims 1-10 in this application was denied under the Patent Law Article 29 (2) (Reason C).

Therefore, the Applicant has amended the Claims, Specification and Drawings in the application in order to clarify the nature of this invention by submitting this response and the amendment. Depending on the amended Claims, it is believed to resolve the reasons for rejection; thus, the detailed explanation will be provided in the following paragraphs.

(2) All the Claims in the previously submitted application were reexamined in this response and the amendment, and Claims 1-3 and 9-10 were corrected based upon the Specification and Drawings in the previously submitted application in order to response to Reasons A and C in the Office Action. Further, in order to match the description with the drawing in the Specification to respond to Reason B

the reference number 158 indicating “RX ARQ Buffer” in Figure 1 was corrected to 168 .

(3) It is thought that the aforementioned amended Claims should directly respond to the rejection reasons in the Office Action.

First of all, Reason A were amended in order to explain clearly methods of invention relating to each of Claims 1, 9 and 10 which occur at a transmitting or receiving communication unit. The terminology used for these corrections are based upon those seen in Claims 5-8, Abstract, the Detail Description of the Invention and Figure 1 in the original Claims.

It is believed that those corrections have clarified how specific apparatus, in other words hardware resources, should be applied in order to solve technical problems. Therefore, Claims 1-4, 9 and 10 should be considered an invention defined in the Patent Law Article 2 and it meets the patentability requirements defined in the Patent Law Article 29.

Second, the following paragraphs response to Reason B.

First, paragraph (1) includes “…as seen in Figure 1, …is performed,” which is found on lines 14-19 on page 7 of the Specification and Figure 1 itself do not agree. Thus, “on Layer 3” on line 18 on page 7 of the Specification was corrected to “within Layer 3” for further clarification.

As clearly drawn in Figure 1, a data stream 108 on Layer 3 is transferred to Layer 2 (102) by Layer 3 (110) and encryption (102) occurs at Layer 2 (102) to a data stream received from Layer 3 (a data stream on Layer 3). Therefore, the corrections match the figure with the description.

Second, regarding paragraph (2), all the radio communications meet radio communication protocols. By meeting an appropriate protocol (this protocol depends on a type of communication systems, such as cdma 2000 communication system, GSM communication system, or UMTS communication system.), it makes a cellular phone manufactured by a company such as Motorola Incorporated possible to communicate with a base unit manufactured by another company such as Lucent Technologies, and all such devices must function in accordance with the protocols. All the radio protocols define bits transmitted by a radio, including identification of what bit corresponds to the one on Layer 2 and what bit corresponds to the one on Layer 3. In other words, the protocols identify where bits on Layer 2 should be embodied and where bits on Layer 3 should be embodied. Further, identifying where on Layer 2 bits are located and where on Layer 3, including higher Layers, the ones should be located enables all the receiving communication units to extract bits on Layer 2 from a receiving data packet prior to transmitting the remaining packet to Layer 3.

The protocols do not require encryption. Encryption skills are owned properties, which means it belongs to a manufacturer of the device and it should never be controlled by the protocols. Consequently, even if a data is encrypted, it must still meet the appropriate radio protocols,

and accordingly bits on an encrypted Layer 3 or higher layers still remain the ones on Layer 3 or higher Layers respectively, and they are also embodied in a data packet on Layer 3 or the one on higher Layers. Therefore, even if bits are encrypted, how to distinguish bits on higher Layers from the ones on Layer 2 is well known so that it is followed by all the cellular systems. Hence, despite encryption, the method for separating bits on Layer 3 or the higher from the ones on Layer 2 is well known and it is perceived that those skilled in the art should easily achieve.

Moreover, the reference number 158 indicating the “RX ARQ Buffer” in Figure 1 has been corrected to 168 as seen in paragraph (3). This is believed to solve the discrepancy between the Detail Explanation of the Invention and Figure 1. Further, the reference number 158 corresponds to the data stream which flows from Layer 2 (104) to Layer 130 (160).

Next, a response to Reason C in the Office Action will be given below.

It is described in the Office Action that “the reference 1 (network security) mentions an encryption method for encrypting only the data field (data link service data unit).” Further, as an input to a random sequence generator, it describes a transmission unit which applies a value by converting an initial value data which is updated intermittently by a key data as an input to a random sequence generator, and it outputs a random signal which is used to scramble and descramble a video signal. It is a matter of design choice as to whether what data should be adopted as an intermittently updated key data.

However, it should be addressed that deciding a function used during the data encryption process is not merely a matter of design choice. Specifically, because a radio transmission is extremely vulnerable to intrusion, a function to make search more complicated is always sought. Typically, the key must be selected and transmitted to each of the terminals of the communication path in order to encrypt information with the key. In other words, prior to exchanging data, it must be transmitted to both the transmitting and receiving communication units. Even if the key can be updated during the transmission process, it needs to be initialized to some value and the initial value must be transmitted to the terminals of each of the receiving portions prior to transmitting the encrypted data. For instance, as described in the Background of the Invention in this application, the encryption technology which was proposed to prove cellular at the time of this invention includes exchange in special messages between communication units, and the messages were used to generate the shared secret data. Because the key or the data used to generate keys must be divided among communication units which are involved in communications prior to the data exchange, it is critical that a secret key is only provided to an authorized user during encryption. This is specifically said to a radio communication because it can be intercepted by similar communication units and the division of the key was also intercepted by any units with a radio receiver.

In order to solve the problem related to the key management, an encryption technology utilizing the packet sequence number, the transmit overflow sequence number and the session key for data encryption will be provided in Claim 1 of this application. The packet sequence number and transmit overflow sequence number are not the keys. They are neither identified nor divided by the communication units at each of the terminals of the communication path, nor they are derived from the divided data.

The packet sequence number is a data which is embodied in each of the exchanged data packets and which can be modified but not repeated by the data packets. Therefore, it is not necessary to exchange a key or a message to establish the key prior to communication and it also results in saving bandwidth as well as improving the stability.

Additionally, the overflow sequence number is never transmitted to the terminals of the communication path. They are neither embodied in the data packet nor derived from the data embodied in the data packet. The overflow sequence number is determined by the transmitting communication unit and the receiving communication unit. Unlike the key or the packet sequence number, there is no chance to intercept the overflow sequence number; thus, it provides a higher level of security.

Therefore, the use of the packet sequence number and the overflow sequence number to encrypt/decrypt data cannot be easily achieved by those skilled in the art, and it is merely not a choice to select a variable as a key among from many others. Thus, it is obvious that those skilled in the art cannot easily invent Claim 1 and relating Claims 2-4 in this application based upon the citations.

Furthermore, Claims 5, 7 and 9 in this application also disclose the encryption/decryption skills utilizing the packet sequence number, the transmit overflow sequence number and the session key. Thus, it also cannot be easily invented by those skilled in the art on the same ground as the above. Moreover, since Claim 6 relates to Claim 5 and so as Claims 8 and 7, it is perceived that Claims 6 and 8 have patentability.

(4) As seen above, all the Claims amended by this response and the amendment should be recognized an invention as defined by the Patent Law Article 2 and they also clarify the Specification and Drawings. Further, it cannot be easily invented by those skilled in the art by relaying on the citations. Therefore, it is perceived that this invention should not be rejected under the scope of the main clause of the Article 29(1), 36(4) and 29(2) of the Patent Law. The Applicant requests a decision to grant a patent in this application.

Patent Application H07-507561 Dispatch No.: 435917
Dispatch Date: December 16, 2003 (H15)

Office Action

Patent Application Number	7th Year of Heisei (1995)	Patent No. 507561
Drafting Date	15th year of Heisei (2003)	December 5
Patent Examiner	AOKI, Shigenori 4229 5M00	
Applicant's Agent	IKEUCHI, Yoshiaki (and 1 other)	
Applicable Article	No. 36	

The present application should be rejected for the reason given below. If the applicant has any objection against this notice, it should be submitted within three months from the date this notice was sent.

Reason

The present application does not comply with the requirements stipulated in the Patent Law Article 36(4) with respect to the following points described in the Specification and Drawings.

Note

In the invention according to Claims 1~10 of the Specification of the present application, a method for encrypting a packet at the transmitting communication unit as a function of a packet sequence number and a transmit overflow sequence number and a method for decrypting the encrypted packed as a function of the packet sequence number and the receiving overflow sequence number at the receiving communication unit.

Here, it is mentioned in the Detailed Description of the Invention of the Specification of the present application that a pseudo random bit stream used to encrypt and decrypt packetized data stream segments must be identical to the one used at the transmitting communication unit and the receiving communication unit, and the packet sequence number is transmitted to the receiving communication unit as unencrypted header information.

However, the pseudo random bit streams consist of values that depend on transmitting overflow sequence numbers and receiving overflow sequence numbers at the transmitting side and the receiving side respectively, and for example, according to the response to the Office Action submitted on October 30th of Heisei 15 (2003), the overflow sequence numbers are never transmitted to the terminals of the communication path without being embedded into the data packet and deriving from data embedded in the data packet, and judging from the description of the independent determination of the overflow sequence numbers by the respective transmitting and receiving communication units (see especially page 7 lines 6-13), the transmitting communication unit and the receiving communication unit generally take respective independent values;

therefore, the pseudo random bit streams at the sending and receiving sides cannot generate the same value.

Upon further examination, the method described in the Specification of the present application makes decryption impossible so that it cannot provide a method and apparatus for cryptographically protecting data stream in a communication system, which is the purpose of the invention of the present application.

Therefore, a description is not provided to the extent those skilled in the art can achieve based on the Drawings and Specification of the present application.

In the event that further reasons for rejection are discovered, you will be notified of such reasons.

Prior Art Examination Results

- Fields Searched: IPC 7th Edition
  H0 4L9 / 22

- Prior Art

  None in particular

The prior art examination results do not constitute the grounds for rejection.

Director / Agent	Chief Examiner / Agent	Examiner	Asst. Examiner
	INOUE, Tadashi	AOKI, Shigenori	
	8120	4229	

Response to Office Action

Accepted
June 14, 2004 (H.16)

Dear Mr. Shigenori Aoki
Commissioner of the Japan Patent Office

1. Case
   Patent Application H7-507561
   (PCT/US 94/07672)

2. Title of the Invention
   Method and Apparatus for Providing Cryptographic Protection of a Data Stream in a Communication System

3. Applicant

Address	1303 East Algonquin Road Shaumburg, Illinois 60196 United States of America
Name	Motorola Incorporated
(Nationality)	United States of America

4. Agent

Address	Ikeuchi International Patent Office Sekiuchi Kawashima Building 1-4-2 Ohta-cho, Chuo-ku Yokohama, Kanagawa 231-0011 Tel: 045 (211) 2795
Name of the Agent	(8357) Yoshiaki Ikeuchi

Yoshiaki Ikeuchi Patent Attorney

5. Date Office Action was Received
   December 5, 2003 (H15) (sent on December 16, 2003)

Patent Office
16.6.15
Applicant Support Division
Miyawaki

Formality Examination

Illegible

6. Reasons

(1) We received the Office Action dated on December 5, 2003 (H15) (sent on December 16, (H15)) regarding the above referenced application. It states that the insufficiency in the Specification and the description about the Drawing failed to meet the requirements stipulated in the Patent Law Article 36 (4).

Thus, the Applicant will provide the following explanation regarding the previously submitted response as it is believed to solve the reasons for rejection.

(2) First, lines 6-13 on page 7 of the response submitted on October 30, 2003 will be given as follows. It describes that overflow sequence number is neither transmitted to the terminals of the communication paths, nor they are embodied in a data packet nor derived from a data embodied in the data packet. It is believed not to raise any issues. However, the description of the overflow sequence number being independently determined by either the transmitting communication unit or the receiving communication unit may be misleading; therefore, it will be explained in the following paragraphs.

Regarding the claims, for example Claim 1, amended on October 30, 2003 (H15), it updates the transmit overflow sequence number as a function of the packet sequence number at the transmitting communication unit. Further, the packet sequence number is transmitted to the receiving communication unit. Also, it extracts the packed sequence number from the receiving communication unit and updates the receiving overflow sequence number as a function of the packet sequence number.

Therefore, it is considered that the transmitting overflow sequence number and the receiving overflow sequence number are not independent of each other

in a sense that they should be determined by the same packet sequence number and they are the same at a specific receiving packet. Yet, it is understood that the transmitting communication unit and the receiving communication unit are able to determine independently the overflow sequence number in a sense that each of the transmitting communication unit and the receiving communication unit implements algorithms in order to determine the overflow sequence number while independent from an output of the algorithms implemented by other communication units without knowing the output.

The Applicant meant in the response that the overflow sequence number is not derived from data embodied in a data packet because, unless the packet sequence number roles over, the overflow sequence number is neither embodied in the data packet nor derived from the data embodied in the data packet; thus, even if it intercepts a specific packet, the packet itself fails to detect the overflow sequence number used to encrypt and decrypt a packet. In other words, during the rollover of the packet sequence number, the overflow sequence number used to encrypt and decrypt a packet is independent from data embodied in a packet, and it is not a function of the data of the packet; therefore, it is not derived from data in the packet.

Each of the transmitting overflow sequence number and the receiving overflow sequence number is a function of the packet sequence number of a packet. As described in the original Specification of this application, the overflow sequence number is the number which is incremented by each of the transmitting communication unit and the receiving communication unit each time the packet sequence number rolls over. For instance, for the purpose of providing an illustrative example,

if 100 is the maximum packet sequence number, each of the transmitting communication unit and the receiving communication unit increments the overflow sequence number each time the preceding transmit/receiving packets have a packet sequence number 100 and the following transmit/receiving packets have a sequence number 1.

As a result, by examining the sequence numbers of each of the transmit/receiving packets, each of the transmitting communication unit and the receiving communication unit can determine independently whether or not the overflow sequence number should be incremented, and meanwhile, it keeps the overflow sequence numbers synchronized. This can be achieved without transmitting the overflow sequence number from one terminal of the communication path to another. Further, determining the overflow sequence number by the role over of the packet sequence number enables the overflow sequence number to determine and to maintain at the inside of each of the communication units so that it does not need to communicate outside of each of the communication units. It enables to prevent interception.

(3) As seen above, the explanation and allegations are believed to solve the issues listed in the Office Action. Moreover, it is also believed that the Claims in the present application clearly state the purpose of this invention, which is to provide a method and apparatus for protecting data stream encryption in a communication system. Therefore, this application meets the requirements stipulated in the Patent Law 36(4). The applicant requests that a patent be granted.

Decision of Refusal

Patent Application Number	7th Year of Heisei (1995) Patent 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 Office Action dated April 17, 2003 (H15).

Moreover, despite reviewing the response and the amendment no sufficient basis to overturn the earlier rejections has been found.

Remarks

1. The Applicant asserts in the response submitted on October 30, 2003 (H15) that the invention regarding Claims 1-10 of the present application (hereinafter referred to as "the invention of the present application") has patentability and by relying on D. W. Davies and W. L. Price authors / Uwazono supervisor of translation, "Network Security", Japan, Nikkei, McGraw Hill, December 5, 1985, 1st Ed. 1st Printing, pg. 307-312 (hereafter referred to as Citation 1") and Publication of Japanese Laid Open Patent Application S63-167588 (hereafter referred to as "Citation 2") which are cited in the aforementioned Office Action, 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 plurality and variety used as keys.

Therefore, the following examination was conducted on the reason and the assertion.

2. First, the validity of the reason and the assertion will be examined.

The response submitted on October 30, 2003 states that the packet sequence number is data embedded in each of the converted data packet, and the data are not transformed or repeated by the packet. Meanwhile, the initial value data in the scrambling process described in Citation 2 is data superimposed on the scrambled source video signal and is regularly modified. Upon further examination, the packet sequence number and the initial value data are both used as the data to generate a pseudo random bit stream, and additionally they also resemble in data modification and a method for exchanging with the other side so that the packet sequence

SN
‖
Initial Value Data
(Handwritten)

number of the invention of the present application corresponds to the initial value data described in Citation 2, with respect to the cryptographic protection of a data stream.

Furthermore, in the response submitted on October 30, 2003, the overflow sequence number in the invention of the present application is [not][1] transmitted to the terminal of the communication path, and they are neither embedded into the data packet nor derived from data embedded in the data packet, and are determined independently by the transmitting communication unit and the receiving communication unit respectively. On the other hand, with the scrambling process described in Citation 2, methods for controlling and counting total transmissions count and increment a vertical sync signal of a source video signal, and configuration settings for timing increments are determined independently by counting the vertical sync signal both at encoding and decoding sides without appearing in the communication path. Upon further examination, the overflow sequence number and the total transmissions are also used as data to create a pseudo random bit stream in addition to their similarities in which the information itself does not appear in the communication path but is independently detected and determined by the units so that the overflow sequence number of the invention of the present application concerning the cryptographic protection of a data stream corresponds to the total transmissions as described in Citation 2.

Looking further, as I Field Encrypting Method for encrypting a packet described in Citation 1, the use of a functional composition in order to encrypt and decrypt information that corresponds to a packet sequence number, information which corresponds to an overflow sequence number and data by adopting technology to create a pseudo random bit stream described in Citation 2 does not surpass the category which could be easily achieved by those skilled in the art as indicated in the aforementioned Office Action.

Therefore, since the above Reason states a functional composition which could be easily achieved by those skilled in the art based upon the descriptions given in Citation 1 and 2, it is not sufficient to validate the assertion.

3. Due to the foregoing, the above assertion, to the effect that the invention of the present application has patentability stated by the Applicant in the response submitted on October 30, 2003, is not based on a valid reason and therefore cannot be granted .

END

OF.SN
‖
Total transmissions
(Handwritten)

Director / Agent	Chief Examiner / Agent	Examiner	Asst. Examiner
	MIZUNO, Shigeo	AOKI, Shigenori	
	8220	4229	

[1] Translator's note: Office Action dispatch no.: 435917 from Dec 5, 2003 citing the same lines from the October 30, 2003 response states "the overflow sequence numbers are **not** transmitted to the terminal of the communication path" in contradiction to this citation of the October 2003 response.