Appeal decision

Appeal No. 2014-24704

USA	
Appellant	QUALCOMM INCORPORATED
Tokyo, Japan	
Patent Attorney	MURAYAMA, Yasuhiko
Tokyo, Japan	
Patent Attorney	KURODA, Shimpei

The case of appeal against the examiner's decision of refusal of Japanese Patent Application No. 2013-515526, entitled "Method and apparatus for binding subscriber authentication and device authentication in communication systems" (December 22, 2011 International Publication No. WO 2011-159952, September 5, 2013 National Publication of International Patent Application No. 2013-534754) has resulted in the following appeal decision.

Conclusion

The appeal of the case was groundless.

Reason

1. History of the procedures

The application in connection with the appeal of the case (hereinafter referred to as "The Application") was originally filed on June 16, 2011 as an International Patent Application claiming a priority under the Paris Convention based on an application in the United States on June 16, 2010 (hereinafter referred to as "Priority date") and an application in the United States on June 15, 2011. The outline of history of the procedures is as follows.

December 14, 2012:	submission of national documents
December 20, 2012:	submission of document of translation of Internal Application, and written request for examination

as of December 2, 2013:	notice of reasons for refusal
April, 8, 2014:	submission of written opinion and written amendment
as of July 25, 2014:	decision of refusal (August 4, 2014 delivery of a certified copy)
December 3, 2014:	submission of written appeal and written amendment
December 25, 2014:	reconsideration report
April 7, 2015:	submission of written statement
as of August 31, 2015:	notice of reasons for refusal (the body)
December 7, 2015:	submission of written opinion and written amendment

2. The Invention

According to the scope of claims corrected in written amendment dated December 7, 2015, the Description, and Drawings, the invention described in Claim 1 of the Application (hereinafter referred to as "The Invention") is recognized as follows, as described in Claim 1 of the scope of claims.

"A method operational in a device, comprising the steps of:

performing subscriber authentication with a network entity based on a key for authenticating a subscription, to obtain a first key;

performing device authentication of the device with the network entity based on a challenge-response exchange, to obtain device authentication data including a second key received from the network entity, wherein a challenge for device authentication includes the encrypted second key;

generating a security key that binds the subscriber authentication and the device authentication, on the basis of the first key and the device authentication data;

and using the security key to secure communications between the device and a serving network."

3. Cited Document

(1) Technical matters described in Cited Document 1 and Cited Invention 1

In National Publication of International Patent Application No. 2008-547350 (published on December 25, 2008, hereinafter referred to as "Cited Document 1") distributed before the Priority date and cited in a notice of reasons of refusal (hereinafter referred to as "Reasons for refusal by the body") notified by the body on

August 31, 2015, the technical matters are described as follows, together with Drawings. (Note by the body: Underlines added by the body for reference.)

A. "[0005]

Referring to FIG. 1, the IEEE 802.16e communication system includes a Mobile Station (hereinafter referred to as "MS") MS 100, a Base Station (BS) 140, and an Authorization, Authentication, and Accounting (hereinafter referred to as "AAA") server 180. Since the IEEE 802.16e communication system operates in EAP-in-EAP, it authenticates in the twice EAP scheme. For convenience sake, authentication based on the EAP scheme is referred to as 'EAP authentication'. The first of the two EAP authentications is device authentication 120 and the second is user authentication 160 after the first EAP authentication is successful."

B. "[0037]

In order to achieve the purpose described above, the invention is a method for performing authentication using Extensible Authentication Protocol (EAP) in a Broadband Wireless Access communication system including an MS, a BS, and an Authorization, Authentication, and Accounting (AAA) server. The method includes the following steps: the MS, the BS, and the AAA server acquire a first master session key (MSK) by performing a first EAP authentication being device authentication for the MS in an EAP-in-EAP scheme; and the MS, the BS, and the AAA server acquire a second MSK by performing a second EAP authentication being user authentication for the MS in the EAP-in-EAP scheme, after the first EAP authentication.

... (omitted) ...

[0041]

FIG. 4 is a diagram illustrating a signal flow for EAP-in-EAP authentication using double Pairwise Master Keys (hereinafter referred to as 'PMK') in an IEEE 802.16e communication system according to the embodiment of the present invention."

C. "[0053]

The AAA server 480 transmits a RADIUS ACCEPT message to the BS 440, notifying of the success of the EAP authentication (step S473). The BS 440 then transmits a PKM_EAP/EAP-SUCCESS message to the MS 400 (step S475). Through the user authentication 460, the BS 440 generates a second PMK, PMK2 from MSK2, and generates an Authorization Key (hereinafter referred to as 'AK') using PMK and PMK2 (step S477). The AK creation from PMK and PMK2 in the MS 400 and the BS 440 will be described in more detail with reference to FIG. 5, thus the detailed description is omit here.

[0054]

FIG. 5 is a flowchart illustrating a procedure for generating the AK in the IEEE 802.16e communication system according to the present invention.

[0055]

This procedure takes place in both the MS and the BS, and the AK will be described herein in the context of the BS.

[0056]

Referring to FIG. 5, the BS acquires an MSK by the first EAP authentication; i.e., the device authentication in step 511, and generally creates an EIK and a PMK using the MSK in step 513. Specifically, the BS generates the EIK and the PMK with a predetermined number of bits, for example, a 160-bit EIK and a 160-bit PMK, by truncating the MSK.

[0057]

In step S515, the BS acquires a second MSK, (i.e. MSK2) through the second EAP authentication; i.e., the user authentication. The BS generates a second PMK (i.e. PMK2), for example, a 160-bit PMK2, by truncating MSK2 in step 517.

[0058]

The BS generates an AK by applying PMK and PMK2 to an AK generation function. Specifically, the BS uses PMK and PMK2 in a Dot16KDF function, for example. The Dot16KDF function can be expressed as Equation 3 or Equation 4 below.

[0059]

[Equation 3]

AK=Dot16KDF(PMK (+) PMK2,SSID|BSID|'AK',160)

[0060]

In Equation 3 above, SSID is the ID of the MS for which the EAP authentication is performed, BSID is the ID of the BS, 'AK' is the AK created by the Dot16KDF function, and 160 denotes the length of the AK, 160 bits. Hence, the Dot16KDF function generates a 160-bit AK using an XOR of PMK and PMK2 and a parameter of the SSID and the BSID in concatenation.

[0061]

[Equation 4]

AK=Dot16KDF(PMK,SSID|BSID|PMK2|'AK',160)

[0062]

In Equation 4, above, SSID is the ID of the MS for which the EAP authentication is performed, BSID is the ID of the BS, 'AK' is the AK created by the Dot16KDF function, and 160 denotes the length of the AK, 160 bits. Hence, the Dot16KDF function generates a 160-bit AK using PMK and a parameter of the SSID, the BSID, and PMK2 in concatenation.

[0063]

As described above, an AK is generated using PMK resulting from the first EAP authentication and PMK2 resulting from the second authentication during EAP-in-EAP authentication using double PMKs in the IEEE 802.16e communication system according to the embodiment of the present invention. Therefore, the man-in-the-middle-attack phenomenon, which is encountered with the typical IEEE 802.16e communication system, can be eliminated."

The matters described in Cited Document 1 are examined.

(A) According to the description in A, "the IEEE 802.16e communication system includes a Mobile Station (hereinafter referred to as 'MS') MS 100, a Base Station (BS) 140, and an Authorization, Authentication, and Accounting (hereinafter referred to as 'AAA') server 180", and the description in B, "the invention is a method for performing authentication using Extensible Authentication Protocol (EAP) in a Broadband Wireless Access communication system including an MS, a BS, and an Authorization, Authentication, and Accounting (AAA) server",

it is recognized that Cited Document 1 describes that "the communication system includes a Mobile Station MS, a Base Station, and an AAA server as an authentication server."

(B) According to the descriptions in B, "steps: the MS, the BS, and the AAA server acquire a first master session key (MSK) by performing a first EAP authentication being device authentication for the MS in an EAP-in-EAP scheme", and "Pairwise Master Keys (hereinafter referred to as 'PMK')," and the descriptions in C, "This procedure takes place in both the MS and the BS, and the AK will be described herein in the context of the BS" [0055], and "the BS acquires an MSK by the first EAP authentication; i.e., the device authentication and generally creates an EIK and a PMK using the MSK in step S513" [0056], it is recognized that Cited Document 1 describes that "the MS executes device authentication with the AAA server and generates Pairwise Master Key PMK from the acquired master session key MSK".

(C) According to the descriptions in B, "the MS, the BS, and the AAA server acquire a second MSK by performing a second EAP authentication being user authentication for the MS in the EAP-in-EAP scheme ", and "Pairwise Master Keys (hereinafter referred to as 'PMK')", and the descriptions in C, "This procedure takes place in both the MS and the BS, and the AK will be described herein in the context of the BS" [0055], and "the BS acquires a second MSK, (i.e.MSK2) through the second EAP authentication; i.e., the user authentication. The BS generates a second PMK (i.e.PMK2), for example, a 160-bit PMK2 by truncating MSK2 in step S517" [0057],

it is recognized that Cited Document 1 describes that the "MS" "executes user authentication with the AAA server and generates Pairwise Master Key PMK2 from the acquired master session key MSK2."

(D) According to the descriptions in C, "Through the user authentication 460, the BS 440 generates a second PMK, (i.e. PMK2) from MSK2 and generates an Authorization Key (hereinafter referred to as 'AK') using PMK and PMK2" [0053], "The BS generates an AK by applying PMK and PMK2 to an AK generation function. Specifically, the BS uses PMK and PMK2 in a Dot16KDF function, for example" [0058], and "an AK is generated using PMK resulting from the first EAP authentication and PMK2 resulting from the second authentication during EAP-in-EAP authentication using double PMKs in the IEEE 802.16e communication system" [0063],

it is recognized that Cited Document 1 describes that the "MS" "generates an Authorization Key AK using a Dot16KDF function, on the basis of PMK and PMK2."

(E) According to the matters examined in (A)-(D), it is recognized that Cited Document 1 describes the following invention (hereinafter referred to as "Cited Invention 1").

"A communication system including a Mobile Station MS, a Base Station BS, and an AAA server as an authentication server,

the MS executing device authentication with the AAA server, to generate a

Pairwise Master Key PMK from an obtained master session key MSK,

the MS executing user authentication with the AAA server, to generate a Pairwise Master Key PMK2 from an obtained master session key MSK2,

the MS generating an authorization key AK using a Dot16KDF function on the basis of the PMK and the PMK2."

(2) Technical matters described in Cited Document 2 and Cited Invention 2

In International Publication No. WO2009-141919 (published on November 26, 2009, hereinafter referred to as "Cited Document 2") distributed before the Priority date and cited in Reasons for refusal by the body, the technical matters are described as follows (Note by the body: Underlines added by the body for reference. The translation is based on National Publication of International Patent Application No. 2011-523105, which is a patent family member of Cited Document 2.)

D. "[0078] After successful user authentication, device authentication and key establishment are performed as shown in Fig. 8.
[0079] In step S801, the remote ISIM server 204 verifies that the remote ISIM client 208 is trusted, and vice versa.
[0080] In step S802, the remote ISIM client 208 and the remote ISIM server 204 establish an encryption key between them. After that, a secure transmission channel (e.g., a Transport Layer Security (TLS) session) is set up between them using the established key.
Therefore, according to the present embodiment, successful pairing results in establishment of a TLS session between the remote ISIM client 208 and the remote ISIM server 204.
[0081] According to the present embodiment, the remote ISIM client 208 and the remote ISIM server 204 perform the device authentication and key establishment based on a mechanism defined by 3GPP. Using this mechanism, a shared secret key (called Ks local_device) is established between the remote ISIM client 208 and the remote ISIM server 204. Then, the remote ISIM client 208 and the remote ISIM server 204 establish the TLS session using the established Ks local_device."

The matters described in Cited Document 2 are examined.

(A) According to the descriptions in D, "After successful user authentication, device authentication and key establishment are performed as shown in Fig. 8" [0078], "the remote ISIM server 204 verifies that the remote ISIM client 208 is "trusted", and vice versa" [0079], and "the remote ISIM client 208 and the remote ISIM server 204 perform the device authentication and key establishment based on a mechanism defined by 3GPP" [0081],

it is recognized that Cited Document 2 describes that "device authentication is executed between a terminal and a server after user authentication".

(B) According to the descriptions in D, "the remote ISIM client 208 and the remote ISIM server 204 establish an encryption key between them. After that, a secure transmission channel (e.g., a Transport Layer Security (TLS) session) is set up between them using the established key" [0080], and "the remote ISIM client 208 and the remote ISIM server 204 perform the device authentication and key establishment based on a mechanism defined by 3GPP" [0081],

it is recognized that Cited Document 2 describes "establishment of a key to set up a secure session".

(C) According to the matters examined in (A)-(B), it is recognized that Cited Document 2 describes the following invention (hereinafter referred to as "Cited Invention 2").

"A method of executing device authentication between a terminal and a server, after user authentication, and establishing a key to set up a secure session."

(3) Technical matters described in Cited Document 3 and Cited Invention 3

In International Publication No. WO2009-148261 (published on December 10, 2009, hereinafter referred to as "Cited Document 3") distributed before the Priority date and cited in Reasons for refusal by the body, the technical matters are described as follows (Note by the body: Underlines added by the body for reference. The translation is based on National Publication of International Patent Application No. 2011-526097, which is a patent family member of Cited Document 3.)

E. "Encryption is applied to the MAC PDU payload requested by a selected ciphersuite. <u>Generally, the mobile station and the base station need a key to perform encryption. Accordingly, in the IEEE 802.16 standard, a traffic encryption key</u>

(TEK) is defined. The TEK is generated as a random number by the base station. The base station can transfer an encrypted TEK to the mobile station through a corresponding TEK encryption algorithm.

... (Omitted) ...

A data service flow through a broadband wireless access network has a series of quality of service (QoS) parameters, and encryption and decryption are performed through a traffic encryption key (TEK). The IEEE 802.16 standard which supports one of broadband wireless access systems defines a traffic encryption key (TEK) to protect a unicast data service." (p.3 l. 22-p. 4 l. 15)

F. "In one aspect of the present invention, a method of generating a traffic encryption key (TEK) comprises the steps of obtaining a key parameter during an authentication procedure with a base station; deriving the authentication key (AK) using the key parameter; receiving, by a mobile station from the base station, a first nonce and first security materials for deriving the traffic encryption key (TEK); and deriving the traffic encryption key (TEK) using one or more of the first nonce, the authentication key (AK), and the first security materials.

...(Omitted) ...

Also, the nonce is generated using a random number generator by the base station.

The key parameter includes one or more of a pre-authentication key (PAK), a pair-wise master key (PMK), and a pair-wise master key2 (PMK2)." (p. 7 l. 14-l. 23, p. 8 l. 4-l. 8)

G. "Table 1 illustrates a method of generating a TEK. [Table 1]

Referring to Table 1, the authentication key (AK) can be generated using one or more of PAK, PMK, and PMK2. Also, the CMAC key and the HMAC key can be generated using the MAC address of the mobile station and the base station identifier (BS ID). Moreover, the base station can generate a TEK using a random number and encrypt the TEK using a KEK." (p. 20 l. 11-p. 21 l. 7)

H. "The following Equation 1 represents an example of a method of generating a TEK, which can be used in the embodiments of the present invention.

[Equation 1]

(Old, New)TEK=Dot16KDF(AK,(Old, New)Nonce|SAID|TEK,128)

In the Equation 1, new TEK and old TEK represent TEKs generated during an initial network entry procedure of the mobile station or a location update procedure of the mobile station. At this time, the mobile station and the base station can use an AK, Nonce, and SAID when generating a TEK.

Referring to the Equation 1, in the embodiments of the present invention, the AK is used when the TEK is generated. This method is different from a general method of generating a TEK using a random number in a base station. The reason that an AK is used in generating a TEK is to allow the base station and the mobile station to flexibly and efficiently process a network operation such as handoff and support a unified method of generating and updating a TEK." (p. 27 l. 1-l. 20)

The matters described in Cited Document 3 are examined.

(A) According to the descriptions in F, "the steps of obtaining a key parameter during an authentication procedure with a base station", and "The key parameter includes one or more of a pre-authentication key (PAK), a pair-wise master key (PMK), and a pair-wise master key 2 (PMK2)",

it is recognized that Cited Document 3 describes that "a mobile station obtains pair-wise master keys PMK and PMK2, as parameters, during an authentication procedure with a base station".

(B) According to the descriptions in F, "deriving the authentication key (AK) using the key parameter", and "The key parameter includes one or more of a pre-authentication key (PAK), a pair-wise master key (PMK), and a pair-wise master key 2 (PMK2)", the description in G, "the authentication key (AK) can be generated using one or more of PAK, PMK and PMK2", and the description "AK=Dot16KDF(PMK(+)PMK2,SS MAC Address|BSID|AK,160)" in Table 1,

it is recognized that Cited Document 3 describes "generating an authentication key AK using a Dot16KDF function, on the basis of PMK and PMK2".

(C) According to the descriptions in H, "At this time, the mobile station and the base station can use an AK, Nonce, and SAID when generating a TEK", and "in the embodiments of the present invention, the AK is used when the TEK is generated", the description "(Old, New)TEK=Dot16KDF(AK,(Old, New)Nonce|SAID|TEK,128)" in Equation 1, and the descriptions in E, "Generally, the mobile station and the base station need a key to perform encryption. Accordingly, in the IEEE 802.16 standard, a traffic encryption key (TEK) is defined", and "The IEEE 802.16 standard which supports one of broadband wireless access systems defines a traffic encryption key (TEK) to protect a unicast data service",

it is recognized that Cited Document 3 describes "encrypting data service communication between a mobile station and a base station, using a traffic encryption key TEK generated by use of an authentication key AK".

(D) According to the matters examined in (A)-(C), it is recognized that Cited Document 3 describes the following invention (hereinafter referred to as "Cited Invention 3").

"A method of encrypting data service communication between a mobile station and a base station, using a traffic encryption key TEK generated by use of an authentication key AK,

the mobile station obtaining pair-wise master keys PMK and PMK2, as parameters, in an authentication procedure with the base station,

to generate the authentication key AK using a Dot16KDF function, on the basis of PMK and PMK2."

4. Comparison

The Invention is compared with Cited Invention 1.

(1) The "mobile station MS" in Cited Invention 1 is a device for executing user authentication and device authentication, and corresponds to the "device" in the Invention.

The "mobile station MS", "base station" and "AAA server" in Cited Invention 1 are devices on a network, and correspond to the "network entity" in the Invention.

"User authentication" and "device authentication" in Cited Invention 1 correspond to "subscriber authentication" and "device authentication" in the Invention, obviously.

"PMK" in Cited Invention 1 is a key obtained by device authentication (device authentication), and corresponds to "device authentication data" in the Invention.

"PMK2" in Cited Invention 1 is a key obtained by user authentication (subscriber authentication), and corresponds to the "first key" in the Invention.

"AK" in Cited Invention 1 is a key generated from both a key obtained by user authentication (subscriber authentication) and a key obtained by device authentication (device authentication), and corresponds to the "security key" in the Invention.

(2) As a result of comparing the description, "the MS executes user authentication with the AAA server, to generate a pairwise master key PMK2 from a master session key MSK2" in Cited Invention 1 with "a method operational in a device" and "the step of performing subscriber authentication with a network entity based on a key for authenticating a subscription, to obtain a first key" in the Invention, they are different from each other in the points described below, according to the result of examination in (1),

while being common in the point of being "the step of executing subscriber authentication with a network entity, to obtain a first key".

(3) As a result of comparing the description, "the MS executes device authentication with the AAA server, to generate a pairwise master key PMK from a master session key MSK" in Cited Invention 1 with "the step of performing device authentication of the device with the network entity based on a challenge-response exchange, to obtain device authentication data including a second key received from the network entity, wherein a challenge for device authentication includes the encrypted second key", they are different from each other in the points described below, according to the result of examination in (1),

while being common in the point of being "the step of executing device authentication of the device with the network entity, to obtain device authentication data".

(4) As examined in (1), "PMK2" in Cited Invention 1 corresponds to the "first key" in the Invention, "PMK" in Cited Invention 1 corresponds to "device authentication data" in the Invention, "user authentication" and "device authentication" in Cited Invention 1 correspond to "subscriber authentication" and "device authentication" in the Invention. To generate "AK" on the basis of "PMK2" (first key) and "PMK" (device authentication data) in Cited Invention 1 is, in other words, to "associate" or to "bind" "subscriber authentication" (user authentication) for obtaining "PMK2" with "device authentication" (device authentication) for obtaining "PMK", definitely.

Therefore, the description in Cited Invention 1, "the MS generates the authentication key AK using a Dot16KDF function, on the basis of the PMK and the PMK2", corresponds to the "step of generating a security key that binds the subscriber authentication and the device authentication, on the basis of the first key and the device authentication data" in the Invention.

(5) As above, the Invention and Cited Invention 1 correspond in the following points, and differ in the following points.

(Corresponding features)

"A method operational in a device, comprising the steps of:

performing subscriber authentication with a network entity, to obtain a first key;

performing device authentication of the device with the network entity, to obtain device authentication data;

generating a security key that binds the subscriber authentication and the device authentication, on the basis of the first key and the device authentication data."

(Different feature 1)

In the Invention, "subscriber authentication" and "device authentication" are executed in this order,

while in Cited invention 1, "device authentication" (device authentication) and "user authentication" (subscriber authentication) are executed in this order.

(Different feature 2)

In the Invention, "the security key is used to secure communications between the device and a serving network",

while in Cited Invention 1, processing for securing communication by use of AK is not specified.

(Different feature 3)

Regarding "Subscriber authentication",

it is executed based on "a key for authenticating a subscription" in the Invention,

while Cited Invention 1 does not specify that the "key for authenticating a subscription" is used.

(Different feature 4)

Regarding "device authentication" for obtaining "device authentication data",

in the Invention, it is executed based on "a challenge-response exchange", the "challenge" including an "encrypted second key" acquired from a network entity, the obtained "device authentication data" including the "second key",

while in Cited Invention 1, the above points are not specified.

5. Judgment by the body

The above different features 1-4 are examined.

(1) Regarding Different feature 1

Cited Invention 1 executes both user authentication and device authentication between devices.

As described in Cited Document 2, "a method of executing device authentication between a terminal and a server, after user authentication, and establishing a key to set up a secure session" had been well known before the Priority date.

Cited Invention 1 and Cited Invention 2 belong to an authentication field of technology, and both include a common function in a point of executing user authentication and device authentication. Thus, a person skilled in the art could have easily conceived of applying Cited Invention 1 and Cited Invention 2 to execute "user authentication" and "device authentication" in this order, or a configuration concerning Different feature 1.

(2) Regarding Different feature 2

Cited Invention 1 generates an authorization key AK using Dot16KDF function, on the basis of pair-wise master keys PMK and PMK2,

while Cited Invention 3, "a method of encrypting data service communication between a mobile station and a base station, using a traffic encryption key TEK generated by use of an authentication key AK,

the mobile station obtaining pair-wise master keys PMK and PMK2, as parameters, in an authentication procedure with the base station,

to generate the authentication key AK using a Dot16KDF function, on the basis of PMK and PMK2", had been well known before the Priority date.

Cited Invention 1 and Cited Invention 3 belong to an authentication field of technology, and both include a common function in a point of generating a key AK using a Dot16KDF function on the basis of two pair-wise master keys generated during authentication. Thus, a person skilled in the art could have easily conceived of applying Cited Invention 1 and Cited Invention 3 to secure data service communication with "AK" by encrypting the communication with the generated keys on the basis of "AK", or a configuration concerning Different feature 2.

(3) Regarding Different feature 3

In user authentication, it is common to use a subscriber key, in the authentication field of technology. (If necessary, see National Publication of International Patent Application No. 2005-529569, which was distributed before the Priority date, paragraphs [0039]-[0045] and FIG. 2.)

The user authentication using the "subscriber key" authenticates a subscription of a subscriber. Thus, it can be said that the "subscriber key" is a "key for authenticating a subscription".

Therefore, a person skilled in the art could have easily conceived of using the "key for authenticating a subscription" in user authentication in Cited Invention 1, or a configuration concerning Different feature 3.

(4) Different feature 4

In device authentication between devices, it is common in the authentication field of technology to execute challenge-and-response authentication, which encrypts a random number generated in one device for communication, and to use the random number as a key. (If necessary, see National Publication of International Patent Application No. 2005-529569, which was distributed before the Priority date, paragraphs [0034], [0051], [0113]-[0114].)

Therefore, a person skilled in the art could have easily conceived of executing "challenge-and-response" (challenge-response exchange) device authentication with an encrypted random number (encrypted second key) obtained from a network entity, to use the random number as a key to be generated in device authentication in Cited Invention 1, or a configuration concerning Different feature 4.

(5) Summary

As examined above, Different features 1-4 are not particularly distinguished. Even if these different features are considered generally, a working effect of the Invention falls within a scope that can be predicted from a working effect of Cited Inventions 1-4 and the common means, and cannot be regarded as a particularly distinguished effect.

6. Closing

As above, the invention concerning Claim 1 of the application should not be granted a patent for the invention in accordance with the provisions of Article 29(2) of the Patent Act. The application should be rejected without examining inventions concerning other claims.

Therefore, the appeal decision shall be made as described in the conclusion.

February 24, 2016

Chief administrative judge:	ISHII, Shigekazu
Administrative judge:	TOSHIMA, Hiroshi
Administrative judge:	TSUJIMOTO, Yasutaka