Internal distribution code:

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

Datasheet for the decision of 21 September 2022

Case Number: T 1402/20 - 3.5.05

Application Number: 16737330.7

Publication Number: 3232603

IPC: H04L9/08, G09C1/00, H04L9/30

Language of the proceedings: EN

Title of invention:
KEY-EXCHANGE METHOD, KEY-EXCHANGE SYSTEM, KEY DEVICE, TERMINAL DEVICE, AND PROGRAM

Applicant:
Nippon Telegraph and Telephone Corporation

Headword:
Shared key exchange using proxy/NTT

Relevant legal provisions:
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

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

Case Number: T 1402/20 - 3.5.05

D E C I S I O N
of Technical Board of Appeal 3.5.05
of 21 September 2022

Appellant: (Applicant)	Nippon Telegraph and Telephone Corporation 5-1, Otemachi 1-chome, Chiyoda-ku, Tokyo 100-8116 (JP)
Representative:	MERH-IP Matias Erny Reichl Hoffmann Patentanwälte PartG mbB Paul-Heyse-Strasse 29 80336 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 29 January 2020 refusing European patent application No. 16737330.7 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chair	A. Ritzka
Members:	P. Cretaine
	K. Kerber-Zubrzycka

Summary of Facts and Submissions

I. This appeal is against the examining division's decision posted on 29 January 2020, refusing European patent application No. 16 737 330.7. The application was refused for lack of inventive step (Article 56 EPC) of a single request in view of:

D4: A. Fujioka et al., "Ephemeral Key Leakage Resilient and Efficient ID-AKEs That Can Share Identities, Private and Master Keys", 1 December 2010, 187-205, in combination with:

D1: EP 2 634 760 for the first group of claims of the request and in view of:

D5: S. Chatterjee et al., "Reusing Static Keys in Key Agreement Protocols", 13 December 2009, 39-56, in combination with D1 for the second group of claims of the request

II. Notice of appeal was received on 7 April 2020, and the appeal fee was paid the same day. The statement setting out the grounds of appeal was received on 4 June 2020. The appellant requested that the decision be set aside and that a patent be granted on the basis of claims 1 to 8 on which the decision was based and which were re-filed with the statement setting out the grounds of appeal. Oral proceedings were requested as an auxiliary request.

III. A summons to oral proceedings was issued on 25 January 2022. In a communication pursuant to Article 15(1) RPBA, sent on 25 July 2022, the board gave its preliminary opinion that claims 1, 4, 6 and 8 did not

meet the requirements of Article 56 EPC having regard to D4 in combination with D1 and taking into account the common general knowledge of the skilled person. Furthermore, the board gave its preliminary opinion that claims 2, 5, 7 and 8 did not meet the requirements of Article 56 EPC having regard to the combination of D5 and D1 and taking into account the common general knowledge of the skilled person.

IV. Oral proceedings were held on 21 September 2022. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of claims 1 to 8 on which the decision was based. At the end of the oral proceedings, the chair announced the board's decision.

V. **Claim 1** of the sole request reads as follows:

A key exchange method, wherein
G_1 , G_2 , and G_T are assumed to be cyclic groups whose order is a prime number q with K bit length, g_1, g_2 , and g_T are assumed to be generators of the groups G_1, G_2, and G_T, respectively, e: G_1 x G_2 → G_T is assumed to be pairing that satisfies $g_T = e(g_1, g_2)$, H: $\{0, 1\}^*$ -> $\{0, 1\}^K$, H_1 : $\{0, 1\}^*$ -> G_1 , and H_2 : $\{0, 1\}^*$ → G_2 are assumed to be cryptographic hash functions, m is assumed to be a natural number which is greater than or equal to 2, an assumption is made that i = 1, ..., m holds, $c_{i,o,o}$, $c_{i,0,1}$, $c_{i,1,0}$, and $c_{i,1,1}$ are assumed to be constants, p_i ϵ $Z_q[u_o , u_1 , v_o , v_1]$ is assumed to be m polynomials which are defined by a formula below:

$$p_i(u_0,u_1,v_0,v_1) = c_{i,0,0}u_0v_0 + c_{i,0,1}u_0v_1 + c_{i,1,0}u_1v_0 + c_{i,1,1}u_1v_1$$

,
z ϵ Z_q is assumed to be a master secret key,

$Z_1 = g_1^z \in G_i$ and $Z_2 = g_2^Z \in G_2$ are assumed to be master public keys, ID_A is assumed to be an identifier of a terminal device (1_1), $Q_{A,1} = H_1(ID_A) \in G_1$ and $Q_{A,2} = H_2(ID_A) \in G_2$ are assumed to be public keys, ID_B is assumed to be an identifier of other terminal device (1_2), $Q_{B,1} = H_1(ID_B) \in G_1$ and $Q_{B,2} = H_2(ID_B) \in G_2$ are assumed to be public keys, $D_{A,1} = Q_{A,1}^z$ and $D_{A,2} = Q_{A,2}^z$ are assumed to be secret keys of the terminal device (1_1), $D_{B,1} = Q_{B,1}^z$ and $D_{B,2} = Q_{B,2}^z$ are assumed to be secret keys of the other terminal device (1_2), $x_A \in Z_q$ is assumed to be a short-term secret key of the terminal device (1_1), $X_{A,1} = g1^{xA}$ and $X_{A,2} = g_2^{xA}$ are assumed to be short-term public keys of the terminal device (1_1), $x_B \in Z_q$ is assumed to be a short-term secret key of the other terminal device (1_2), $X_{B,1} = g_1^{xB}$ and $X_{B,2} = g_2^{xB}$ are assumed to be short-term public keys of the other terminal device (1_2), $P_{i,B}$ is assumed to be a value which is defined by a formula below:

$$P_{i,B} = Q_{B,2}^{c_{i,0,0}} X_{B,2}^{c_{i,0,1}},$$

r_{i1} and r_{i2} are assumed to be arbitrary numbers, s_{i1} and s_{i2} are assumed to be random numbers which are mutually prime, and s'_{i1} and s'_{i2} are assumed to be random numbers which satisfy a predetermined relationship with the random numbers s_{i1} and s_{i2} ,
in a storage (20) of a key device (2), the secret keys $D_{A,1}$ and $D_{A,2}$ of the terminal device (1_i) are stored, and
the key exchange method includes:
a random number generating step in which the terminal device (1_i) generates the random numbers s_{i1} , s_{i2} , s'_{i1}, and s'_{i2} ;
a proxy calculation step in which the key device (2) calculates a first commission result ζ_{i1} for

i = 1, ..., m by a formula below:

$$\varsigma_{i1} = e(D_{A,1}, g_2^{-r_{i1}})e(D_{A,1}, g_2^{r_{i1}} P_{i,B}^{s_{i1}})$$

and calculates a second commission result ζ_{i2} for i = 1, ..., m by a formula below:

$$\varsigma_{i2} = e(D_{A,1}, g_2^{-r_{i2}})e(D_{A,1}, g_2^{r_{i2}} P_{i,B}^{s_{i2}})$$;

and

a verification step in which the terminal device (1_1) verifies whether or not a first verification value and a second verification value coincide with each other for i = 1, ..., m by a formula below:

$$\varsigma_{i1}^{s_{i2}} = \varsigma_{i2}^{s_{i1}}$$,

characterized in that the key exchange method further includes:

a public keys randomizing step in which the terminal device (1_1) calculates first randomized public keys information for i = 1, ..., m by a formula below:

$$(g_2^{-r_{i1}}, g_2^{r_{i1}} P_{i,B}^{s_{i1}})$$

and calculates second randomized public keys information for i = 1, ..., m by a formula below:

$$(g_2^{-r_{i2}}, g_2^{r_{i2}} P_{i,B}^{s_{i2}})$$, and

a common key calculation step in which, if the first verification value and the second verification value coincide with each other, the terminal device (l_1) generates a common key by using values σ_1 , ..., σ_m , wherein the value σ_i for i = 1, ..., m is obtained by a formula below:

$$\sigma_i = \varsigma_i e(Z_1^{x_A}, Q_{B,2}^{c_{i,1,0}} X_{B,2}^{c_{i,1,1}}) \text{ and}$$

after calculating the commission result ζ_i for i = 1, ..., m is obtained by a formula below:

$$\varsigma_i = \varsigma_{i1}^{s'_{i1}} \varsigma_{i2}^{s'_{i2}}$$

Claim 2 of the sole request reads as follows:

A key exchange method, wherein
G is assumed to be a cyclic group whose order is a prime number q with K bit length, g is assumed to be a generator of the group G, g_1 and g_2 are assumed to be elements which are not unit elements of the group G, m is assumed to be a natural number which is greater than or equal to 2, an assumption is made that i = 1, ..., m holds, $c_{i,o,o}$, $c_{i,o,1}$, $c_{i,1,o}$, and $c_{i,1,1}$ are assumed to be constants, $p_i \in Z_q[u_o , u_1 , v_o , v_1]$ is assumed to be m polynomials which are defined by a formula below:

$$p_i(u_0, u_1, v_0, v_1) = c_{i,0,0}u_0v_0 + c_{i,0,1}u_0v_1 + c_{i,1,0}u_1v_0 + c_{i,1,1}u_1v_1$$

,

$s_A \in Z_q$ is assumed to be a secret key of a terminal device (1_1), $S_A = g^{sA} \in G$ is assumed to be a public key

of the terminal device (1_1), $s_B \in Z_q$ is assumed to be a secret key of the other terminal device (1_2), $S_B = g^{sB} \in G$ is assumed to be a public key of the other terminal device (1_2), $X_A \in Z_q$ is assumed to be a short-term secret key of the terminal device (1_1), $X_A = g^{xA} \in G$ is assumed to be a short-term public key of the terminal device (1_1), $X_B \in Z_q$ is assumed to be a short-term secret key of the other terminal device (1_2), $X_B = g^{xB} \in G$ is assumed to be a short-term public key of the other terminal device (1_2), F_A is assumed to be a homomorphism which is $F_A : G \rightarrow G$, $h \rightarrow h^{sA}$, $\alpha_{B,i}$ is assumed to be a value which is defined by a formula below:

$$\alpha_{B,i} = X_B^{c_{i,0,0}} S_B^{c_{i,0,1}},$$

s_{i1} and s_{i2} are assumed to be random numbers which are mutually prime, and s'_{i1} and s'_{i2} are assumed to be random numbers which satisfy a predetermined relationship with the random numbers s_{i1} and s_{i2} , in a storage (20) of a key device (2), the secret key s_A of the terminal device (1_1) is stored, and the key exchange method includes:

a random number generating step in which the terminal device (1_1) generates the random numbers s_{i1} , si_2 , s'_{i1}, and s'_{i2};

a proxy calculation step in which the key device (2) calculates a first commission result ζ_{i1} for $i = 1, ..., m$ by a formula below:

$$\varsigma_{i1} = F_A(g_1^{-1}) F_A(g_1 \alpha_{B,i}^{s_{i1}})$$

and calculates a second commission result ζ_{i2} for

i = 1, ..., m by a formula below:

$$\varsigma_{i2} = F_A(g_2^{-1})F_A(g_2\alpha_{B,i}^{s_{i2}})$$; and

a verification step in which the terminal device (1_1) verifies whether or not a first verification value and a second verification value coincide with each other for i = 1, ..., m by a formula below:

$$\varsigma_{i1}^{s_{i2}} = \varsigma_{i2}^{s_{i1}}$$,

characterized in that the key exchange method further includes:

a public keys randomizing step in which the terminal device (1_1) calculates first randomized public keys information for i = 1, ..., m by a formula below:

$$(g_1^{-1}, g_1\alpha_{B,i}^{s_{i1}})$$

and calculates second randomized public keys information for i = 1, ..., m by a formula below:

$$(g_2^{-1}, g_2\alpha_{B,i}^{s_{i2}})$$, and

a common key calculation step in which, if the first verification value and the second verification value coincide with each other, the terminal device (l_1) generates a common key by using values σ_1 , ..., σ_m , wherein the value σ_i for i = 1, ..., m is obtained by a formula below:

$$\sigma_i = \varsigma_i X_B^{c_{i,1,0} x_A} S_B^{c_{i,1,1} x_A}$$ and

after calculating the commission result ζ_i for i = 1, ..., m is obtained by a formula below:

$$\varsigma_i = \varsigma_{i1}^{s'_{i1}} \varsigma_{i2}^{s'_{i2}}$$

The sole request comprises further independent claims directed to:
- a system (**claim 4**), a terminal device (**claim 6**) and a computer program (**claim 8**) corresponding to claim 1
- a system (**claim 5**), a terminal device (**claim 7**) and a computer program (**claim 8**) corresponding to claim 2

Reasons for the Decision

1. Claim 1

1.1 It was common ground in the examination procedure and in the oral proceedings before the board that D4 represented the closest prior art to the subject-matter of claim 1. The appellant has not rebutted the detailed analysis of the disclosure of D4 for the features of claim 1 as stated in points 5.1 and 5.1.1 of the decision.

Based on the distinguishing features between claim 1 and D4 established in point 5.1.1, the decision formulated the objective technical problem to be solved as how to delegate the computation involving the private key to a proxy, the proxy holding the private keys but not being able to know the computed result.

However, this formulation is not in line with the principles underlying the problem-solution approach as established by the case law of the boards since it contains a pointer to part of the solution, namely to use a proxy in the computation of the common key. Thus, the board agrees with the formulation of the problem proposed by the appellant, namely to reduce computational load for the terminal device without leaking the common key.

1.2 The appellant has argued that the skilled person starting from D4 as the closest prior art and trying to solve the above-mentioned problem would not consider the disclosure of D1 since this document does not relate to the exchange of shared secrets. However, the board holds that the skilled person seeking to first reduce the computational load for the terminal device would consult D1 since it generally relates to the use of a proxy for providing a computing capability to a cryptographic apparatus without leaking secret information (see paragraph [0006]).

1.3 By trying to add the proxy scheme of D1 to the shared secret generation scheme of D4, the skilled person would have to address the following issues.

D1 discloses a capability providing apparatus, i.e. a proxy, that computes a decryption function f(x) for decrypting a ciphertext x using a decryption key s stored in the capability apparatus (see paragraphs [0044] and [0045]). Therefore, D1 is based on the assumption that the decryption key s is shared between the proxy and the terminal device requesting the decryption.

On the other hand, D4 discloses that the shared secrets σ_i necessary for calculating the session key K are, for example, given by the relation $\sigma_1 = e(D_A Z^{xA}, Q_B X_B)$ (see section 4.2, step 3). Since both $Q_B = H_1(ID_B)$ and $X_B = g^{xB}$ are satisfied, $Q_B X_B$ is encrypted data of a public key $H_1(ID_B)$ using an ephemeral private key x_B. The decision found that $Q_B X_B$ of D4 corresponds to the ciphertext x of D1 and $e(D_A Z^{xA}, Q_B X_B)$ of D4 corresponds to f(x) of D1, namely that $e(D_A Z^{xA}, x)$ corresponds f(x).

Since D1 is based on the assumption that the decryption key s used in the decryption function f(x) is shared between the terminal device and the capability providing apparatus, the process of D4 could integrate the process of D1 as long as the key $D_A Z^{xA}$ used in $e(D_A Z^{xA}, x)$ is shared between the capability providing apparatus and the terminal device. However, in the current invention defined by claim 1, the key device, i.e. the capability providing apparatus, knows the secret key D_{A1} in advance, but it will never know the short-term secret key x_A. The skilled person, when combining D4 and D1, would thus have to cope with the issue that the values σ_i in D4, i.e. in a conventional ID-AKE protocol, defined by the equation in the first line on page 5 of the statement of grounds, cannot be calculated at all by the key device since both parts of σ_i are based on a pairing calculation involving x_A.

For these reasons, the board agrees with the appellant that the combination of D4 with D1 does not lead to the subject-matter of claim 1 since the key x_A is not defined in claim 1 as being known by the key device because x_A is defined as a short-term key, and no

transfer of x_A from the terminal device to the key device is specified in claim 1.

Thus, to implement the computation disclosed in D4 without sharing the short-term secret key x_A, the skilled person must perform further steps. To this end, claim 1 involves a formula transformation that utilises the bi-linearity of the pairing operation and divides the computation into one part to be computed with the secret key D_{A1} by the capability providing apparatus, i.e. the key device, and another part to be computed with the short-term secret key x_A by the terminal device. The appellant detailed that by using the bi-linearity of the pairing e, the formula defining σ_i is transformed in claim 1 (see page 3 of claim 1, line 5 in combination with page 2, line 10) by using a formula transformation which divides the computation into two parts, one part being computed by the terminal with the short-term secret key x_A of the terminal device, and the other part being computed by the key device with the secret key of the terminal device, known to the key device.

The appellant plausibly argued that the skilled person would not make use of the above-mentioned formula transformation without the exercise of inventive skill since D1 did not hint at not sharing the key x_A.

1.4 For these reasons, the board holds that claim 1 and corresponding system claim 4, terminal device claim 6 and computer program claim 8 meet the requirements of Article 56 EPC having regard to the prior art of D4 and D1.

2. Claim 2

Similarly and based on the findings of the decision for the features distinguishing the subject-matter of independent claim 2 from D5 (see points 5.2.1 and 5.2.2), claim 2 and corresponding system claim 5, terminal device claim 7 and computer program claim 8 meet the requirements of Article 56 EPC having regard to the prior art of D5 and D1.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the examining division with the order to grant a patent in the following version.

Claims:
No. 1-8 as submitted with the statement of grounds of appeal

Description:

Pages 1, 2, 5 to 24, 26 to 33, 35 to 48, 51 to 59, 61 to 68 and 70 to 80 as originally filed

Pages 3, 4, 4a, 4b, 25, 34, 60 and 69 filed with the letter of 11 September 2018

Pages 49 and 50 filed with the letter of 1 March 2019

Drawings:

Sheets 1/13 to 13/13 as originally filed

The Registrar: The Chair:

K. Götz-Wein A. Ritzka

Decision electronically authenticated