United States Patent	12395322
Kind Code	B2
Date of Patent	August 19, 2025
Inventor(s)	Ueno; Mana et al.

Encryption apparatus, cypher communication system, encryption method and program

Abstract

An encryption apparatus including a key storage unit that stores a secret key and a public key of public key encryption, and an encryption unit that encrypts communication data using the secret key and the public key.

Inventors:	**Ueno; Mana (Tokyo, JP), Kobayashi; Tetsutaro (Tokyo, JP), Murakami; Keizo (Tokyo, JP)**
Applicant:	**NIPPON TELEGRAPH AND TELEPHONE CORPORATION** (Tokyo, JP)
Family ID:	**1000008766108**
Assignee:	**NIPPON TELEGRAPH AND TELEPHONE CORPORATION (Tokyo, JP)**
Appl. No.:	**18/258932**
Filed (or PCT Filed):	**January 14, 2021**
PCT No.:	**PCT/JP2021/001112**
PCT Pub. No.:	**WO2022/153456**
PCT Pub. Date:	July 21, 2022

Prior Publication Data

Document Identifier	Publication Date
US 20240048362 A1	Feb. 08, 2024

Publication Classification

Int. Cl.: **H04L9/08** (20060101)

U.S. Cl.:

CPC **H04L9/0825** (20130101); **H04L9/0844** (20130101); **H04L9/0894** (20130101);

Field of Classification Search

CPC: H04L (9/0825); H04L (9/0844); H04L (9/0894)

USPC: 713/171

References Cited

U.S. PATENT DOCUMENTS

Patent No.	Issued Date	Patentee Name	U.S. Cl.	CPC
6085320	12/1999	Kaliski, Jr.	713/168	G07F 7/1008
7373509	12/2007	Aissi	713/168	H04L 9/3247
7587590	12/2008	Yamada	713/153	H04L 9/003
8015393	12/2010	Fukasawa	713/168	H04L 9/3263
8291231	12/2011	Ueno	713/168	H04L 9/321
11018847	12/2020	Hunacek	N/A	H04L 9/0662
2004/0059908	12/2003	Yamada	713/151	H04L 9/003
2004/0208317	12/2003	Imai et al.	N/A	N/A
2004/0246350	12/2003	Sakamoto	348/241	G06T 5/92
2005/0002532	12/2004	Zhou	380/277	H04L 9/302
2005/0078825	12/2004	Ohmori	380/255	H04N 21/835
2005/0228986	12/2004	Fukasawa	713/156	H04L 9/3263
2008/0189548	12/2007	Steeves	726/25	G06F 21/602
2011/0293098	12/2010	Fu	709/206	H04L 9/321
2015/0222422	12/2014	Yung	380/30	H04L 9/30
2016/0294551	12/2015	Ichikawa	N/A	H04L 9/0861
2017/0019385	12/2016	Yoo	N/A	H04L 63/062
2019/0394018	12/2018	Isshiki et al.	N/A	N/A
2022/0167156	12/2021	Yasui	N/A	N/A

FOREIGN PATENT DOCUMENTS

Patent No.	Application Date	Country	CPC
3096487	12/2019	EP	H04L 9/0825
2000-132096	12/1999	JP	N/A
2004-246350	12/2003	JP	N/A
2017-506362	12/2016	JP	N/A
WO-2016091790	12/2015	WO	H04L 9/0838
2018/100740	12/2017	WO	N/A
2020/188679	12/2019	WO	N/A

OTHER PUBLICATIONS

Daisuke Moriyama, Ryo Nishimaki, Tatsuaki Okamoto, “Koukaikagiango no suri (Mathematics of public key encryption)”, Kyoritsu Shuppan Co., Ltd., 2011, p. 147-154. cited by applicant
Emura, K., Hanaoka, G., Nuida, K et al. Chosen ciphertext secure keyed-homomorphic public-key cryptosystems. Des. Codes Cryptogr. 86, 1623-1683 (2018). https://doi.org/10.1007/s10623-017-0417-6. cited by applicant

Primary Examiner: Lemma; Samson B

Attorney, Agent or Firm: IPUSA, PLLC

Background/Summary

TECHNICAL FIELD
(1) The present invention relates to an encryption apparatus, a cypher communication system, an encryption method, and a program.
BACKGROUND ART
(2) As a method of encrypting communication contents in online data communication, two encryption methods of common key encryption and public key encryption are known. In addition, hybrid encryption combining two encryption methods is known.
(3) For example, Non Patent Literature 1 discloses a method in which communication contents are encrypted by common key encryption and a key used in common key encryption is encrypted by public key encryption. This method is a method addressing the fact that encryption and decryption processing in public key encryption is very slow compared with those in common key encryption.
(4) Specifically, in this method, communication data is encrypted by using high-speed common key encryption to be repeated the number of times corresponding to the length of the communication data, and the key to be delivered is encrypted by using public key encryption in order to solve the key delivery problem that occurs in common key encryption.
CITATION LIST
Non Patent Literature
(5) Non Patent Literature 1: Daisuke Moriyama, Ryo Nishimaki, Tatsuaki Okamoto, “Koukaikagiango no suri (Mathematics of public key encryption)”, Kyoritsu Shuppan Co., Ltd., 2011, p. 147-154
SUMMARY OF INVENTION
Technical Problem
(6) In an online conference system, in order to perform communication in a small communication band, there is a system in which data such as voice collected from each terminal is synthesized (added) by a service providing server and transmitted to each terminal. In addition, there is a

demand for a service provider to achieve end-to-end cryptographic communication for concealing communication contents.

(7) In order to perform processing such as addition of encrypted communication contents, it is conceivable that the service providing server once converts the contents into plain text. However, in that case, the communication contents cannot be concealed from the service provider, and end-to-end cryptographic communication cannot be achieved.

(8) Therefore, complete end-to-end encryption that conceals communication contents from the service provider as well is achieved by using special homomorphic encryption that enables addition on the server in the encrypted state. In addition, it has been found in previous studies that homomorphism is in public key encryption typified by ElGamal encryption or the like.

(9) As described above, depending on the use purpose of cryptographic communication, not only the delivered key but also the communication data needs to be encrypted using public key encryption instead of common key encryption as in Non Patent Literature 1.

(10) However, encryption processing in conventional public key encryption is very slow, and there is a problem that it cannot be used for processing in real-time communication such as a video conference system.

(11) An object of the disclosed technology is to speed up encryption processing using public key encryption.

Solution to Problem

(12) The disclosed technology is an encryption device including a key storage unit that stores a secret key and a public key of public key encryption, and an encryption unit that encrypts communication data using the secret key and the public key.

Advantageous Effects of Invention

(13) Encryption processing using public key encryption can be speeded up.

Description

BRIEF DESCRIPTION OF DRAWINGS

(1) FIG. **1** is a diagram for describing an encryption device in conventional public key encryption.

(2) FIG. **2** is a diagram for describing an encryption device in public key encryption according to an embodiment of the present invention.

(3) FIG. **3** is a configuration diagram of a cryptographic communication system according to Embodiment 1.

(4) FIG. **4** is a sequence diagram illustrating cryptographic communication processing according to Embodiment 1.

(5) FIG. **5** is a configuration diagram of a cryptographic communication system according to Embodiment 2.

(6) FIG. **6** is a sequence diagram illustrating cryptographic communication processing according to Embodiment 2.

(7) FIG. **7** is a configuration diagram of a cryptographic communication system according to Embodiment 3.

(8) FIG. **8** is a sequence diagram illustrating cryptographic communication processing according to Embodiment 3.

(9) FIG. **9** is a configuration diagram of a cryptographic communication system according to Embodiment 4.

(10) FIG. **10** is a sequence diagram illustrating cryptographic communication processing according to Embodiment 4.

(11) FIG. **11** is a diagram illustrating a hardware configuration example of each device.

DESCRIPTION OF EMBODIMENTS

(12) Hereinafter, embodiments of the present invention will be described with reference to the drawings. The embodiments described below are merely examples, and embodiments to which the present invention is applied are not limited to the following embodiments.

(13) Before describing the technology according to the present embodiment, first, conventional technology related to cryptography of the present embodiment and a problem thereof will be described.

(14) (Conventional Technology)

(15) Conventional public key encryption will be described with reference to FIG. **1**.

(16) As illustrated in FIG. **1**, when receiving input of a message M and a public key pk, a conventional encryption device encrypts the message M using the public key pk and outputs a ciphertext C.

(17) However, encryption processing using the public key pk requires time to perform calculation, and thus is not suitable for cryptographic communication requiring real-time properties such as a video conference system.

(18) Hereinafter, a technology according to the present embodiment for solving the above problem will be described.

Outline of Present Embodiment

(19) First, an outline of a technology according to the present embodiment will be described. FIG. **2** is a diagram for describing an encryption device in public key encryption according to the present embodiment.

(20) In the encryption method according to the present embodiment, as illustrated in FIG. **2**, when receiving input of a message M, a public key pk, and a secret key sk, the encryption device encrypts the message M using the public key pk and the secret key sk, and outputs a ciphertext C. That is, the encryption device uses not only the public key pk but also the secret key sk in the encryption process, which is different from the conventional technology. Note that the message M is an example of communication data in cryptographic communication. In addition, the ciphertext C is an example of encrypted communication data.

Embodiment 1

(21) Hereinafter, Embodiment 1 of the present invention will be described with reference to the drawings. The embodiments described below are merely examples, and embodiments to which the present invention is applied are not limited to the following embodiments.

(22) FIG. **3** is a configuration diagram of a cryptographic communication system according to the present embodiment. As illustrated in FIG. **3**, a cryptographic communication system **1** (cypher communication system) includes an encryption device **10** (encryption apparatus), a decryption device **20** (decryption apparatus), and a key generation device **30**. The encryption device **10**, the decryption device **20**, and the key generation device **30** are communicably connected to one another via a communication network or the like.

(23) The key generation device **30** receives input of bit length designation data (**1**.sup.l), generates the public key pk and the secret key sk of public key encryption, and transmits the public key pk and the secret key sk to the encryption device **10** and the decryption device **20**.

(24) The encryption device **10** includes an encryption unit **11** and a key storage unit **12**. The key storage unit **12** stores the public key pk and the secret key sk received from the key generation device **30**. The encryption unit **11** generates the ciphertext C by encrypting the input message M using the public key pk and the secret key sk, and transmits the ciphertext C to the decryption device **20**.

(25) The decryption device **20** includes a key storage unit **22** and a decryption unit **21**. The key storage unit **22** stores the public key pk and the secret key sk received from the key generation device **30**. The decryption unit **21** obtains the message M by decrypting the ciphertext C received from the encryption device **10** using the public key pk and the secret key sk.

(26) Next, operation of the cryptographic communication system **1** according to the present

embodiment will be described. FIG. **4** is a sequence diagram illustrating cryptographic communication processing according to the present embodiment.

(27) The key generation device **30** receives input of bit length designation data (**1**.sup.l) by a user's operation or the like (step S**101**). Then, the key generation device **30** executes key generation processing of generating a key having the designated bit length (step S**102**). Specifically, the key generation device **30** generates the public key pk and the secret key sk of public key encryption.

(28) Next, the key generation device **30** transmits the public key pk and the secret key sk to the encryption device **10** (step S**103**). The key storage unit **12** of the encryption device **10** stores the received public key pk and secret key sk. Similarly, the key generation device **30** transmits the public key pk and the secret key sk to the decryption device **20** (step S**104**). The key storage unit **22** of the decryption device **20** stores the received public key pk and secret key sk.

(29) The encryption device **10** receives input of the message M by a user's operation or the like (step S**105**). The encryption unit **11** executes encryption processing (step S**106**). Specifically, the encryption unit **11** encrypts the message M using the public key pk and the secret key sk stored in the key storage unit **12** to generate the ciphertext C.

(30) The encryption device **10** transmits the ciphertext C to the decryption device **20** (step S**107**). The decryption unit **21** of the decryption device **20** executes decryption processing (step S**108**). Specifically, the decryption unit **21** decrypts the ciphertext C using both the public key pk and the secret key sk to obtain the message M.

(31) Hereinafter, some examples will be described regarding details of the processing according to the present embodiment.

Example A of Embodiment 1: RSA Encryption

(32) In Example A, an example of encryption by RSA encryption will be described. RSA encryption is one of public key encryption. The basis of security of RSA encryption is the fact that the prime factorization problem of a combined number having a large number of digits is difficult.

(33) Details of each processing using RSA encryption are as follows.

(34) (i) Key Generation Processing (FIG. **4**: Step S**102**)

(35) When 1.sup.l is input, the key generation device **30** outputs a public key pk=(n, e) and a secret key sk=(d, p, q). Here, p and q are prime numbers having bit lengths equivalent to each other. Details of specific processing executed by the key generation device **30** are as follows.

(36) (i-1) Let p and q be prime numbers having equivalent bit lengths, and let n=pq.

(37) (i-2) ϕ (n)=(p−1) (q−1).

(38) (i-3) e is a positive integer less than ϕ (n) and is coprime with ϕ (n). In addition, d is a reciprocal of e obtained by modulo ϕ (n). By these numerical value selection methods, de≡1 (mod ϕ (n)) is established.

(39) (i-4) It is assumed that n and e obtained by the above processing are public keys pk, and that d, p, and q are secret keys sk.

(40) Hereinafter, a set of integers of zero or more and less than n is represented by Zn.

(41) (ii) Encryption Processing (FIG. **4**: Step S**106**)

(42) The message M is an element of Zn.

(43) The encryption unit **11** calculates C=M.sup.e mod n and outputs the ciphertext C.

(44) (iii) Decryption Processing (FIG. **4**: Step S**108**)

(45) The decryption unit **21** performs the following calculation on the ciphertext C to obtain a plaintext message M.

M=*C*.sup.d mod *n*

(46) In particular, in (ii) encryption processing, the encryption unit **11** can use the secret key sk=(d, p, g) in addition to the public key pk=(n, e). Then, the encryption unit **11** can replace mod n with a combination of mod p and mod q according to the Chinese remainder theorem. That is, the encryption unit **11** performs a remainder calculation by converting into a divisor with a short bit length according to the Chinese remainder theorem. Therefore, the cost of the calculation can be

reduced, and the encryption processing can be speeded up.

Example B of Embodiment 1: Paillier Encryption

(47) In Example B, an example of encryption by Paillier encryption will be described. Paillier encryption is one of public key encryption satisfying a property that a ciphertext of m1+m2 can be calculated from a ciphertext of m1 and a ciphertext of m2 (additive homomorphism).

(48) Details of each processing using Paillier encryption are as follows.

(49) (i) Key Generation Processing (FIG. **4**: Step S**102**)

(50) Details of specific processing executed by the key generation device **30** are as follows.

(51) (i-1) Two large prime numbers p and q are randomly selected, and n=pq.

(52) (i-2) k is arbitrarily selected from Zn, and g=1+kn mod n.sup.2.

(53) (i-3) It is assumed that the public key pk=(n, g) and the secret key sk=(p, q)

(54) (ii) Encryption Processing (FIG. **4**: Step S**106**)

(55) (ii-1) The encryption unit **11**

(56) randomly selects r from

Z.sub.n.sub.2* [Math. 1]

(57) (ii-2) C=g.sup.m r.sup.n mod n.sup.2 is the ciphertext.

(58) (iii) Decryption Processing (FIG. **4**: Step S**108**)

(59) (iii-1) λ=lcm (p−1, q−1)

(60) (iii-1) The decryption unit **21** calculates M=L (C.sup.λ mod n.sup.2)/L (g.sup.λ mod n.sup.2) mod n, and obtains the original message.

(61) In particular, in (ii) encryption processing, the encryption unit **11** can use the secret key sk=(p, q) and a parameter k generated in the key generation processing, in addition to the public key pk=(n, g). Note that the key generation device **30** may transmit the parameter k to the encryption device **10** together with the public key pk and the secret key sk. Thus, the calculation of mod n.sup.2 in (ii-2) can be performed using the Chinese remainder theorem. That is, the encryption unit **11** performs a remainder calculation by converting into a divisor with a short bit length according to the Chinese remainder theorem. Therefore, the cost of the calculation can be reduced, and the encryption processing can be speeded up.

Embodiment 2

(62) Hereinafter, Embodiment 2 will be described with reference to the drawings. Embodiment 2 is different from Embodiment 1 in that an encryption device **10** and a decryption device **20** include a preliminary calculation unit and a preliminary calculation table storage unit. Therefore, in the following description of Embodiment 2, differences from Embodiment 1 will be mainly described, and components having functional configurations similar to those of Embodiment 1 are denoted by the same reference numerals as those used in the description of Embodiment 1, and the description thereof will be omitted.

(63) FIG. **5** is a configuration diagram of a cryptographic communication system according to Embodiment 2. A key generation device **30** according to the present embodiment receives input of a system parameter Sys in addition to the bit length designation data (**1**.sub.l), and generates a public key pk and a secret key sk of public key encryption. Then, the key generation device **30** transmits the public key pk, the secret key sk, and the system parameter Sys to the encryption device **10** and the decryption device **20**.

(64) The encryption device **10** includes a preliminary calculation unit **13** and a preliminary calculation table storage unit **14** in addition to an encryption unit **11** and a key storage unit **12**. The key storage unit **12** stores the public key pk, the secret key sk, and the system parameter Sys received from the key generation device **30**.

(65) The preliminary calculation unit **13** performs preliminary calculation. Preliminary calculation is a calculation performed in advance before the encryption processing, and is a calculation that can be performed at a stage where data to be encrypted (message M or the like) is not determined. Specifically, the preliminary calculation unit **13** performs preliminary calculation on the basis of

the public key pk and the system parameter Sys, generates a preliminary calculation table TBL, and stores the preliminary calculation table TBL in the preliminary calculation table storage unit **14**.

(66) The encryption unit **11** generates a ciphertext C by encrypting an input message M using the system parameter Sys and the preliminary calculation table TBL in addition to the public key pk and the secret key sk, and transmits the generated ciphertext C to the decryption device **20**.

(67) Similarly, the decryption device **20** includes a preliminary calculation unit **23** and a preliminary calculation table storage unit **24** in addition to a decryption unit **21** and a key storage unit **22**. The key storage unit **22** stores the public key pk, the secret key sk, and the system parameter Sys received from the key generation device **30**.

(68) Functions of the preliminary calculation unit **23** and the preliminary calculation table storage unit **24** included in the decryption device **20** are similar to those of the preliminary calculation unit **13** and the preliminary calculation table storage unit **14** included in the encryption device **10**.

(69) The decryption unit **21** obtains the message M by decrypting the ciphertext C received from the encryption device **10** using the system parameter Sys and the preliminary calculation table TBL in addition to the public key pk and the secret key sk.

(70) Next, operation of the cryptographic communication system **1** according to the present embodiment will be described. FIG. **6** is a sequence diagram illustrating cryptographic communication processing according to Embodiment 2.

(71) In cryptographic communication processing according to the present embodiment, following step S**103**, the preliminary calculation unit **13** of the encryption device **10** executes preliminary calculation processing (step S**201**). Similarly, following step S**104**, the preliminary calculation unit **23** of the decryption device **20** executes preliminary calculation processing (step S**202**).

(72) Hereinafter, some examples will be described regarding details of the processing according to the present embodiment.

Example C of Embodiment 2: ElGamal Encryption

(73) In Example C, an example of encryption by ElGamal encryption will be described. ElGamal encryption is one of public key encryption. The basis of security of ElGamal encryption is the fact that the discrete logarithm problem of a group with a large order is difficult.

(74) Details of each processing using ElGamal encryption are as follows.

(75) (i) Key Generation Processing (FIG. **6**: Step S**102**)

(76) When 1.sup.l and Sys=(G.sub.0, G) are input, the key generation device **30** outputs the public key pk=(q, H), the secret key sk=x, and the system parameter Sys=(G.sub.0, G). Details of specific processing executed by the key generation device **30** are as follows.

(77) (i-1) In a cyclic group G, an order q is a prime number, and the number of bits of q is k.

(78) (i-2) x is randomly selected from {0, 1, 2, . . . , q−1}.

(79) (i-3) Let H=xG.sub.0.

(80) (i-4) Let (q, H) be the public key pk and x be the secret key sk.

(81) (ii) Preliminary Calculation Processing (FIG. **6**: Steps S**201** and S**202**)

(82) The preliminary calculation unit **13** and the preliminary calculation unit **23** generate the preliminary calculation table TBL=(G.sub.0[0] [0], G.sub.0[0] [1], G.sub.0[0] [2] . . . G.sub.0[i] [j]) on the basis of pk=(q, H) and Sys=(G.sub.0, G).

(83) (iii) Encryption Processing (FIG. **6**: Step S**106**)

(84) Let an element M of G be a plain text.

(85) The encryption unit **11** executes the following processing.

(86) (iii-1) r is randomly selected from {0, 1, 2, . . . , q−1}.

(87) (iii-2) C1=rG.sub.0, C2=M+rH are calculated.

(88) (iii-3) Let (C1, C2) be the ciphertext.

(89) (iv) Decryption processing (FIG. **6**: step S**108**)

(90) The decryption unit **21** performs the following calculation using the received ciphertext (C1, C2).

M=*C*2−*xC*1

(91) In the above-described encryption processing and decryption processing, the encryption unit **11** and the decryption unit **21** perform elliptic scalar multiplication with a fixed basis using a fixed-base exponentiation using the preliminary calculation table TBL.

(92) In particular, in (ii) encryption processing, since the secret key sk=(x) can be used in addition to the public key pk=(q, H), the encryption unit **11** can calculate H by xG.sub.0. As a result, the preliminary calculation table storage unit **24** does not need to individually have the preliminary calculation table in the elliptic scalar multiplication of H, and can use the preliminary calculation table based on G.sub.0.

(93) Since the size of the preliminary calculation table is related to the overall calculation cost, reducing the size of the preliminary calculation table contributes to reduction of the overall calculation cost. Therefore, according to the configuration of Example C, the preliminary calculation table is smaller than that in the conventional technology, the calculation cost can be reduced, and the encryption processing can be speeded up.

Example D of Embodiment 2: KH-PKE

(94) In Example D, an example of encryption by keyed-homomorphic public-key encryption (KH-PKE) will be described. KH-PKE is an encryption method published in reference [1] below.

Reference of Example D

(95) [1] Emura, K., Hanaoka, G., Nuida, K. et al. Chosen ciphertext secure keyed-homomorphic public-key cryptosystems. Des. Codes Cryptogr. 86, 1623-1683 (2018). https://doi.org/10.1007/s10623-017-0417-6

(96) Details of each processing using KH-PKE are as follows.

(97) (i) Key Generation Processing (FIG. **6**: Step S**102**)

(98) When 1.sup.l and Sys=(G.sub.0, G.sub.1, G) are input, the key generation device **30** generates the public key pk=S and the secret key.

sk.sub.d=(*k*.sub.0,*k*.sub.1),(*{circumflex over (k)}*.sub.0,*{circumflex over (k)}*.sub.1),(*{tilde over (k)}*.sub.0,0,*{tilde over (k)}*.sub.0,1,*{tilde over (k)}*.sub.1,0,*{tilde over (k)}*.sub.1,1) [Math. 2]

is generated.

(99) (ii) Preliminary Calculation Processing (FIG. **6**: Steps S**201** and S**202**)

(100) The preliminary calculation unit **13** and the preliminary calculation unit **23** generate the preliminary calculation table TBL=((G.sub.0[0] [0], G.sub.0[0] [1], G.sub.0[0] [2] . . . G.sub.0 [i] [j]), (G.sub.1 [0] [0], G.sub.1 [0] [1], G.sub.1 [0] [2] . . . G.sub.1 [i] [j]), (S[0] [0], S[0][1], S[0][2] . . . S[i] [j])) on the basis of pk=S and Sys=(G.sub.0, G.sub.1, G).

(101) (iii) Encryption Processing (FIG. **6**: Step S**106**)

(102) The encryption unit **11** executes processing defined in the following encryption algorithm on the message M using the preliminary calculation table TBL to obtain the ciphertext C.

X.sub.0←ω*G*.sub.0

X.sub.1←ω*G*.sub.1

Π←ω*S*

E←*M*+*Π*

γ←*TCR*.sub.1(*X*.sub.0,*X*.sub.1,*E*)

{circumflex over (Π)}←{ω(*k*′.sub.0+*γ{circumflex over (k)}*.sub.1,0)*G*.sub.0+ω(*k*′.sub.1+*γ{circumflex over (k)}*.sub.1,1)*G*.sub.1}

{tilde over (Π)}←{ω(*{tilde over (k)}*′.sub.0+*γ{tilde over (k)}*.sub.1,0)*G*.sub.0+ω(*{tilde over (k)}*.sub.1+*γ{tilde over (k)}*.sub.1,1)*G*.sub.1}

τ←*TCR*.sub.2({tilde over (Π)})

C←(*X*.sub.0,*X*.sub.1,*E*,{circumflex over (Π)},τ) [Math. 3]

(iv) Decryption Processing (FIG. **6**: Step S**108**)

(103) The decryption unit **21** obtains the message M by decrypting the ciphertext C using the preliminary calculation table TBL.

(104) For comparison, a conventional method will be described. In the conventional KH-PKE, since the secret key sk is not used in the encryption processing, the following is used as the preliminary calculation table TBL.

$G_0[0][0], G_0[0][1], G_0[0][2] \ldots G_0[i][j]$
$G_1[0][0], G_1[0][1], G_1[0][2] \ldots G_1[i][j]$
$S[0][0], S[0][1], S[0][2] \ldots S[i][j]$
$S'[0][0], S'[0][1], S'[0][2] \ldots S'[i][j]$
$\hat{S}[0][0], \hat{S}[0][1], \hat{S}[0][2] \ldots \hat{S}[i][j]$
$\tilde{S}[0][0], \tilde{S}[0][1], \tilde{S}[0][2] \ldots \tilde{S}[i][j]$
$\tilde{S}_1[0][0], \tilde{S}_1[0][1], \tilde{S}_1[0][2] \ldots \tilde{S}_1[i][j]$ [Math. 4]

(105) Then, in the encryption processing, processing defined in the following encryption algorithm is executed on the message M using the preliminary calculation table TBL to obtain the ciphertext C.

$X_0 \leftarrow \omega G_0$
$X_1 \leftarrow \omega G_1$
$\Pi \leftarrow \omega S$
$E \leftarrow M + \Pi$
$\gamma \leftarrow TCR_1(X_0, X_1, E)$
$\hat{\Pi} \leftarrow \omega(S' + \gamma \hat{S})$
$\tilde{\Pi} \leftarrow \omega(\tilde{S} + \gamma \tilde{S}_1)$
$\tau \leftarrow TCR_2(\tilde{\Pi})$
$C \leftarrow (X_0, X_1, E, \hat{\Pi}, \tau)$ [Math. 5]

(106) According to the method of Example D described above, the size of the preliminary calculation table in KH-PKE can be reduced by 50% or more as compared with the conventional method. Since the size of the preliminary calculation table is related to the overall calculation cost, reducing the size of the preliminary calculation table contributes to reduction of the overall calculation cost. Therefore, according to the configuration of Example D, the preliminary calculation table is reduced, the calculation cost can be reduced, and the encryption processing can be speeded up.

Embodiment 3

(107) Hereinafter, Embodiment 3 will be described with reference to the drawings. Embodiment 3 is different from Embodiment 2 in further including a preliminary calculation device. Therefore, in the following description of Embodiment 3, differences from Embodiment 2 will be mainly described, and components having functional configurations similar to those of Embodiment 2 are denoted by the same reference numerals as those used in the description of Embodiment 2, and the description thereof will be omitted.

(108) FIG. **7** is a configuration diagram of a cryptographic communication system according to Embodiment 3. A cryptographic communication system **1** according to the present embodiment further includes a preliminary calculation device **40** in addition to the devices according to Embodiment 2.

(109) Upon receiving input of a system parameter Sys, the preliminary calculation device **40** generates a preliminary calculation table TBL_Sys and transmits the table to an encryption device **10**.

(110) A preliminary calculation unit **13** of the encryption device **10** generates a preliminary calculation table TBL_pk based on a public key pk. A preliminary calculation table storage unit **14** stores TBL_Sys and TBL_pk.

(111) An encryption unit **11** generates a ciphertext C by encrypting a message M on the basis of pk, sk, and Sys stored in a key storage unit **12** and TBL_Sys and TBL_pk stored in the preliminary calculation table storage unit **14**.

(112) Next, operation of the cryptographic communication system **1** according to the present embodiment will be described. FIG. **8** is a sequence diagram illustrating cryptographic communication processing according to Embodiment 3.

(113) In cryptographic communication processing according to the present embodiment, the preliminary calculation device **40** receives input of the system parameter Sys (step S**301**), and executes preliminary calculation processing (step S**302**). Then, the preliminary calculation device **40** transmits the generated preliminary calculation table TBL_Sys to the encryption device **10** (step S**303**).

(114) Furthermore, in preliminary calculation processing in step S**201**, the preliminary calculation unit **13** generates the preliminary calculation table TBL_pk based on the public key pk.

Example E of Embodiment 3: KH-PKE

(115) In Example E, an example of encryption by KH-PKE in the present embodiment will be described.

(116) (i) Preliminary Calculation Processing (FIG. **8**: Step S**201**)

(117) The preliminary calculation unit **13** generates the preliminary calculation table TBL_pk=(S[0][0], S[0][1], S[0][2] . . . S[i] [j]) on the basis of pk=S.

(118) is generated.

(119) (ii) Preliminary Calculation Processing (FIG. **8**: Step S**302**)

(120) The preliminary calculation device **40** generates the preliminary calculation table TBL_Sys=((G.sub.0[0][0], G.sub.0 [0] [1], G.sub.0[0] [2] . . . G.sub.0 [i] [j]), (G.sub.1 [0] [0], G.sub.1 [0] [1]G.sub.1[0] [2] . . . G.sub.1[i] [j])) on the basis of Sys=(G.sub.0, G.sub.1, G).

(121) (iii) Encryption Processing (FIG. **8**: Step S**106**)

(122) The encryption unit **11** executes processing similar to the encryption algorithm according to Embodiment 2 on the message M to obtain the ciphertext C.

(123) According to the cryptographic communication system **1** of the present embodiment, since the encryption device **10** does not perform the preliminary calculation based on the system parameter Sys, the amount of preliminary calculation can be smaller than that in Embodiment 2. Therefore, the calculation cost of the encryption device **10** can be further reduced as compared with Embodiment 2, and the encryption processing can be speeded up even more.

Embodiment 4

(124) Hereinafter, Embodiment 4 of the present invention will be described with reference to the drawings. Embodiment 4 is different from Embodiment 3 in that an encryption device **10** does not include a preliminary calculation unit. Therefore, in the following description of Embodiment 4, differences from Embodiment 3 will be mainly described, and components having functional configurations similar to those of Embodiment 3 are denoted by the same reference numerals as those used in the description of Embodiment 3, and the description thereof will be omitted.

(125) FIG. **9** is a configuration diagram of a cryptographic communication system according to Embodiment 4. The encryption device **10** according to the present embodiment does not include the preliminary calculation unit **13** according to Embodiment 3. Therefore, a preliminary calculation table storage unit **14** stores a preliminary calculation table TBL_Sys based on a system parameter Sys. That is, the preliminary calculation table storage unit **14** does not store a preliminary calculation table TBL_pk based on a public key pk).

(126) An encryption unit **11** generates a ciphertext C by encrypting a message M on the basis of pk, sk, and Sys stored in a key storage unit **12** and TBL_Sys stored in the preliminary calculation table storage unit **14**.

(127) Next, operation of the cryptographic communication system **1** according to the present embodiment will be described. FIG. **10** is a sequence diagram illustrating cryptographic communication processing according to Embodiment 4.

(128) In cryptographic communication processing according to the present embodiment, the encryption device **10** does not execute preliminary calculation processing (processing

corresponding to step S**201** in FIG. **8** does not exist in FIG. **10**).

Example F of Embodiment 4: ElGamal Encryption

(129) In Example F, an example of encryption by ElGamal encryption in the present embodiment will be described. Details of each processing using ElGamal encryption are as follows.

(130) (ii) Preliminary Calculation Processing (FIG. **10**: Step S**302**)

(131) A preliminary calculation device **40** generates a preliminary calculation table TBL=(G.sub.0[0][0], G.sub.0[0] [1], G.sub.0[0] [2] . . . G.sub.0[i][j]) on the basis of Sys=(G.sub.0, G).

(132) Since the encryption unit **11** in the ElGamal encryption performs encryption using sk, it is sufficient to use the preliminary calculation table TBL=(G.sub.0[0][0], G.sub.0[0] [1], G.sub.0[0] [2] . . . G.sub.0[i] [j]) based on the system parameter Sys=(G.sub.0, G). As a result, the encryption device **10** can be configured not to perform preliminary calculation processing.

Example G of Embodiment 4: KH-PKE

(133) (i) Preliminary Calculation Processing (FIG. **10**: Step S**302**)

(134) The preliminary calculation device **40** generates the preliminary calculation table TBL_Sys=((G.sub.0[0][0], G.sub.0 [0] [1], G.sub.0 [0] [2] . . . G.sub.0 [i] [j]), (G.sub.1 [0] [0], G.sub.1 [0] [1], G.sub.1[0] [2] . . . G.sub.1[i] [j])) on the basis of Sys=(G.sub.0, G.sub.1, G).

(135) (iii) Encryption Processing (FIG. **8**: Step S**106**)

(136) The encryption unit **11** executes processing defined in the following encryption algorithm on the message M to obtain the ciphertext C.

X.sub.0←ω*G*.sub.0

X.sub.1←ω*G*.sub.1

Π←*k*.sub.0ω*G*.sub.0+*k*.sub.1ω*G*.sub.1

E←*M*+*Π*

γ←*TCR*.sub.1(*X*.sub.0,*X*.sub.1,*E*)

{circumflex over (Π)}←{ω(*k*′.sub.0+*γ{circumflex over (k)}*.sub.1,0)*G*.sub.0+ω(*k*′.sub.1+*γ{circumflex over (k)}*.sub.1,1)*G*.sub.1}

{tilde over (Π)}←{ω(*{tilde over (k)}*.sub.0+*γ{tilde over (k)}*.sub.1,0)*G*.sub.0+ω(*{tilde over (k)}*.sub.1+*γ{tilde over (k)}*.sub.1,1)*G*.sub.1}

τ←*TCR*.sub.2({tilde over (Π)})

C←(*X*.sub.0,*X*.sub.1,*E*,{circumflex over (Π)},τ) [Math. 6]

(137) According to this encryption algorithm, the encryption unit **11** can perform encryption using the preliminary calculation table TBL_Sys=((G.sub.0[0][0], G.sub.0 [0] [1], G.sub.0 [0] [2] . . . G.sub.0[i] [ ]), (G.sub.1 [0] [0], G.sub.1[0] [1], G.sub.1[0] [2] . . . G.sub.1[i] [j])) based on the system parameter Sys=(G.sub.0, G.sub.1, G). As a result, the encryption device **10** can be configured not to perform preliminary calculation processing.

(138) According to the methods of Example F and Example G described above, since the encryption device **10** does not perform preliminary calculation processing, the calculation cost by the encryption device **10** can be further reduced. Note that in the configuration of Embodiment 4, when compared with the configuration of Embodiment 3, the load of encryption processing increases while the load of preliminary calculation decreases. Therefore, when the cryptographic communication system **1** is constructed, a more appropriate configuration can be obtained by selecting one of the forms in consideration of the trade-off between the two.

(139) (Hardware Configuration Example)

(140) The encryption device **10**, the decryption device **20**, the key generation device **30**, and the preliminary calculation device **40** (collectively referred to as “device”) can all be implemented by, for example, causing a computer to execute a program describing processing contents described in the present embodiment. Note that “computer” may be a physical machine or a virtual machine on a cloud. In a case where a virtual machine is used, “hardware” described herein is virtual hardware.

(141) The above program can be stored and distributed by being recorded in a computer-readable recording medium (portable memory or the like). Furthermore, the above program can also be

provided through a network such as the Internet or email.

(142) FIG. **11** is a diagram illustrating a hardware configuration example of the computer. The computer in FIG. **11** includes a drive device **1000**, an auxiliary storage device **1002**, a memory device **1003**, a central processing unit (CPU) **1004**, an interface device **1005**, a display device **1006**, an input device **1007**, an output device **1008**, and the like which are connected to each other by a bus B.

(143) The program for implementing the processing in the computer is provided by, for example, a recording medium **1001** such as a CD-ROM or a memory card. When the recording medium **1001** that stores the program is set in the drive device **1000**, the program is installed from the recording medium **1001** to the auxiliary storage device **1002** via the drive device **1000**. Note, however, that the program is not necessarily installed from the recording medium **1001**, and may be downloaded from another computer via a network. The auxiliary storage device **1002** stores the installed program and also stores necessary files, data, and the like.

(144) In a case where an instruction to start the program is given, the memory device **1003** reads and stores the program from the auxiliary storage device **1002**. The CPU **1004** implements a function related to the device in accordance with a program stored in the memory device **1003**. The interface device **1005** is used as an interface for connecting to the network. The display device **1006** displays a graphical user interface (GUI) or the like by the program. The input device **1007** includes a keyboard and mouse, buttons, a touch panel, or the like, and is used to input various operation instructions. The output device **1008** outputs a calculation result.

(145) In each of the above-described embodiments, an example has been described in which the key generation device **30** generates the public key pk and the secret key sk. However, the scope of the present invention is not limited to this, and the encryption device **10** or the decryption device **20** may generate the public key pk and the secret key sk.

Summary of Embodiment

(146) In the present specification, at least the encryption device, the cryptographic communication system, the encryption method, and the program described in the following clauses are described.

(147) (Clause 1)

(148) An encryption apparatus including a key storage unit that stores a secret key and a public key of public key encryption, and an encryption unit that encrypts communication data using the secret key and the public key.

(Clause 2)

(149) The encryption apparatus according to clause 1, in which the encryption unit encrypts the communication data using a preliminary calculation table generated by a device different from the encryption apparatus.

(Clause 3)

(150) The encryption apparatus according to clause 2, in which the encryption unit encrypts the communication data by ElGamal encryption or KH-PKE.

(Clause 4)

(151) The encryption apparatus according to any one of clauses 1 to 3, in which the encryption unit performs a remainder calculation by converting into a divisor with a short bit length according to a Chinese remainder theorem.

(Clause 5)

(152) The encryption apparatus according to clause 4, in which the encryption unit encrypts the communication data by RSA encryption or Paillier encryption.

(Clause 6)

(153) A cypher communication system including an encryption apparatus and a decryption apparatus that perform cryptographic communication with each other, in which: the encryption apparatus includes a key storage unit that stores a secret key and a public key of public key encryption, and an encryption unit that encrypts communication data using the secret key and the

public key; and the decryption apparatus includes a key storage unit that stores the secret key and the public key, and a decryption unit that decrypts communication data encrypted by the encryption apparatus using the secret key.

(Clause 7)

(154) An encryption method executed by an encryption apparatus that stores a secret key and a public key of public key encryption, the method including encrypting communication data using the secret key and the public key.

(Clause 8)

(155) A program for causing a computer to function as each unit in the encryption apparatus according to any one of clauses 1 to 5.

(156) While the embodiments have been described above, the present invention is not limited to such specific embodiments, and various modifications and changes can be made within the scope of the gist of the present invention described in the claims.

REFERENCE SIGNS LIST

(157) **1** Cryptographic communication system **10** Encryption device **11** Encryption unit **12** Key storage unit **13** Preliminary calculation unit **14** Preliminary calculation table storage unit **20** Decryption device **21** Decryption unit **22** Key storage unit **23** Preliminary calculation unit **24** Preliminary calculation table storage unit **30** Key generation device **40** Preliminary calculation device

Claims

1. An encryption apparatus comprising: a memory; and a processor configured to execute: storing a secret key and a public key of public key encryption, and encrypting communication data by using the secret key and the public key, wherein the encrypting includes encrypting the communication data by using a preliminary calculation table generated by a device different from the encryption apparatus, said device different from the encryption apparatus being connected with the encryption apparatus via network, said encrypting includes encrypting the communication data by KH-PKE, and wherein the processor is configured to encrypt the communication data using a preliminary calculation table that includes a plurality of values that are preliminarily generated based on a system parameter corresponding to another apparatus that communicates with the encryption apparatus.

2. The encryption apparatus according to claim 1, wherein the encrypting includes performing a remainder calculation by converting into a divisor with a short bit length according to a Chinese remainder theorem.

3. The encryption apparatus according to claim 2, wherein the encrypting includes encrypting the communication data by RSA encryption or Paillier encryption.

4. A non-transitory computer-readable recording medium having computer-readable instructions stored thereon, which when executed, cause a computer to function as each unit in the encryption apparatus according to claim 1.

5. The encryption apparatus according to claim 1, wherein the processor is further configured to receive the preliminary calculation table from the device via the network.

6. A cypher communication system comprising an encryption apparatus and a decryption apparatus that perform cryptographic communication with each other, wherein: the encryption apparatus includes a first memory; and a first processor configured to execute: storing a secret key and a public key of public key encryption, and encrypting communication data by using the secret key and the public key, wherein the encrypting includes encrypting the communication data by using a preliminary calculation table generated by a device different from the encryption apparatus, said device different from the encryption apparatus being connected with the encryption apparatus via network, said encrypting includes encrypting the communication data by KH-PKE, and wherein the

first processor is configured to encrypt the communication data using a preliminary calculation table that includes a plurality of values that are preliminarily generated based on a system parameter corresponding to the decryption apparatus; and the decryption device includes a second memory; and a second processor configured to execute: storing the secret key and the public key, and decrypting communication data encrypted by the encryption apparatus by using the secret key.

7. An encryption method executed by a computer in an encryption apparatus that stores a secret key and a public key of public key encryption, the method comprising encrypting communication data by using the secret key and the public key, wherein the encrypting includes encrypting the communication data by using a preliminary calculation table generated by a device different from the encryption apparatus, said device different from the encryption apparatus being connected with the encryption apparatus via network, said encrypting includes encrypting the communication data by KH-PKE, and wherein the method further comprises encrypting the communication data using a preliminary calculation table that includes a plurality of values that are preliminarily generated based on a system parameter corresponding to another apparatus that communicates with the encryption apparatus.