(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2022年10月20日(20.10.2022)

WIPO | PCT

(10) 国際公開番号
WO 2022/219785 A1

(51) 国際特許分類:
H04L 9/32 (2006.01)

(21) 国際出願番号： PCT/JP2021/015630

(22) 国際出願日： 2021年4月15日(15.04.2021)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(71) 出願人: 日本電信電話株式会社 (**NIPPON TELEGRAPH AND TELEPHONE CORPORATION**) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目５番１号 Tokyo (JP).

(72) 発明者: 草川 恵太 (**KUSAGAWA, Keita**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP).

(74) 代理人: 伊東 忠重，外 (**ITOH, Tadashige** et al.); 〒1000005 東京都千代田区丸の内二丁目１番１号 丸の内 ＭＹ ＰＬＡＺＡ （明治安田生命ビル） １６階 Tokyo (JP).

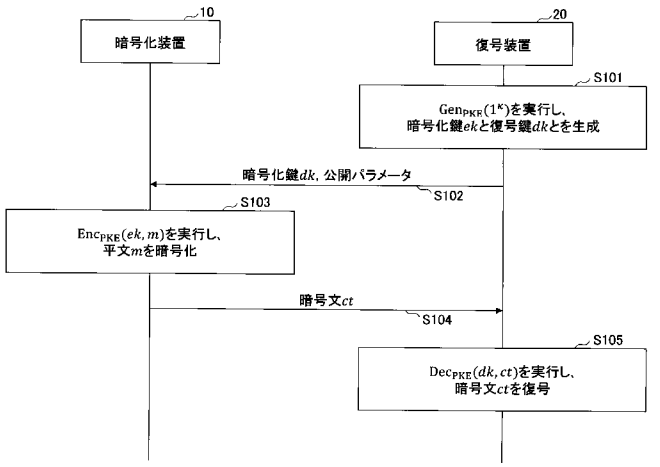
(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

WO 2022/219785 A1

(54) **Title:** CRYPTOGRAPHIC SYSTEM, ENCRYPTION DEVICE, DECRYPTION DEVICE, METHOD, AND PROGRAM

(54) 発明の名称： 暗号システム、暗号化装置、復号装置、方法、及びプログラム

[図3]



10 Encryption device
20 Decryption device
S101 Execute Gen_PKE(1^k), generate encryption key ek and decryption key dk
S102 Encryption parameter dk, public parameter
S103 Execute Enc_PKE(ek, m), encrypt plaintext m
S104 Coded text
S105 Execute Dec_PKE(dk, ct), decrypt coded text ct

(57) **Abstract:** This cryptographic system encrypts and decrypts with a public key cryptography schema involving tag-based encryption TBE=(Gen_{TBE}, Enc_{TBE}, Dec_{TBE}), a weak commitment scheme wCom=(Init, S, R) and a message authentication code MAC=(T, V), and is provided with: a key generation unit which, with κ as a security parameter, generates an encryption key ek_{TBE} and a decryption key dk^{TBE} on the basis of a key generation algorithm $Gen_{TBE}(1_{\kappa})$, generates a common parameter pub on the basis of an initialization algorithm Init (1^{κ}), and sets the encryption key ek_{TBE} and the common parameter pub as the encryption key ek in the public key encryption scheme, and the decryption key dk_{TBE} as the decryption key dk in the public key encryption scheme; an encryption unit which generates a random number r, a commitment com and a decommitment dec on the basis of a sender algorithm S (1^{κ}, pub), generates a coded text c on the basis of the encryption algorithm Enc_{TBE} (ek_{TBE}, com, (m, dec)) with m as

［続葉有］

ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一　国際調査報告（条約第21条(3)）

the plaintext to be encrypted, generates a tag σ by means of the MAC generation algorithm T (r, c), and sets the commitment com, the coded text c and the tag σ as the coded text ct in the public key encryption scheme; and a decryption unit which parses the coded text ct into the commitment com, the coded text c and the tag σ, generates a plaintext m and a decommitment dec by means of a decryption algorithm Dec_{TBE} (dk_{TBE}, com, c), verifies whether it was possible to commit to the random number r by means of the receiver algorithm R (pub, com, dec), and if the commit was successful, verifies the tag σ by means of a verification algorithm V(r, c, σ).

(57) 要約：一実施形態に係る暗号システムは、タグベース暗号方式ＴＢＥ＝（$Ｇｅｎ_{ＴＢＥ}$，$Ｅｎｃ_{ＴＢＥ}$，$Ｄｅｃ_{ＴＢＥ}$）と弱いコミットメント方式ｗＣｏｍ＝（Ｉｎｉｔ，Ｓ，Ｒ）とメッセージ認証符号方式ＭＡＣ＝（Ｔ，Ｖ）とで構成される公開鍵暗号方式により暗号化及び復号を行う暗号システムであって、安全性パラメータをκとして、鍵生成アルゴリズム$Ｇｅｎ_{ＴＢＥ}$（1^{κ}）により暗号化鍵$ｅｋ_{ＴＢＥ}$及び復号鍵$ｄｋ_{ＴＢＥ}$を生成すると共に、初期化アルゴリズムＩｎｉｔ（1^{κ}）により共通パラメータｐｕｂを生成し、前記暗号化鍵$ｅｋ_{ＴＢＥ}$と前記共通パラメータｐｕｂとを前記公開鍵暗号方式の暗号化鍵ｅｋ、前記復号鍵$ｄｋ_{ＴＢＥ}$を前記公開鍵暗号方式の復号鍵ｄｋとする鍵生成部と、送信者アルゴリズムＳ（1^{κ}，ｐｕｂ）により乱数ｒとコミットメントｃｏｍとデコミットメントｄｅｃとを生成し、暗号化対象の平文をｍとして暗号化アルゴリズム$Ｅｎｃ_{ＴＢＥ}$（$ｅｋ_{ＴＢＥ}$，ｃｏｍ，（ｍ，ｄｅｃ））により暗号文ｃを生成し、ＭＡＣ生成アルゴリズムＴ（ｒ，ｃ）によりタグσを生成し、前記コミットメントｃｏｍと前記暗号文ｃと前記タグσとを前記公開鍵暗号方式の暗号文ｃｔとする暗号化部と、前記暗号文ｃｔを前記コミットメントｃｏｍと前記暗号文ｃと前記タグσとにパースし、復号アルゴリズム$Ｄｅｃ_{ＴＢＥ}$（$ｄｋ_{ＴＢＥ}$，ｃｏｍ，ｃ）により平文ｍとデコミットメントｄｅｃを生成し、受信者アルゴリズムＲ（ｐｕｂ，ｃｏｍ，ｄｅｃ）により乱数値ｒにコミットできたか否かを検証し、前記コミットに成功した場合は検証アルゴリズムＶ（ｒ，ｃ，σ）により前記タグσを検証する復号部と、を有する。

明　細　書

発明の名称 ：

暗号システム、暗号化装置、復号装置、方法、及びプログラム

技術分野

[0001] 本発明は、暗号システム、暗号化装置、復号装置、方法、及びプログラムに関する。

背景技術

[0002] ＩＤベース暗号やタグベース暗号からＢｏｎｅｈ－Ｋａｔｚ変換（以下、ＢＫ変換ともいう。）によりＩＮＤ－ＣＣＡ安全な公開鍵暗号を構成する方法が知られている。例えば、非特許文献１には、ＩＤベース暗号からＢＫ変換によりＩＮＤ－ＣＣＡ安全な公開鍵暗号を構成する方法が記載されている。

先行技術文献

非特許文献

[0003] 非特許文献1：Dan Boneh, Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity-based encryption. SIAM J. Comput., 36(5):1301-1328, 2007.

発明の概要

発明が解決しようとする課題

[0004] しかしながら、非特許文献１等に記載されている従来方法では、暗号文の中に公開鍵を入れておくと、暗号文から誰宛て暗号文かが分かる等、十分に匿名性が確保できない、といった問題が存在する。

[0005] 本発明の一実施形態は、上記の点に鑑みてなされたもので、匿名性を確保した安全な公開鍵暗号を実現することを目的とする。

課題を解決するための手段

[0006] 上記目的を達成するため、一実施形態に係る暗号システムは、タグベース

暗号方式ＴＢＥ＝（$Ｇｅｎ_{TBE}$，$Ｅｎｃ_{TBE}$，$Ｄｅｃ_{TBE}$）と弱いコミットメント方式ｗＣｏｍ＝（Ｉｎｉｔ，Ｓ，Ｒ）とメッセージ認証符号方式ＭＡＣ＝（Ｔ，Ｖ）とで構成される公開鍵暗号方式により暗号化及び復号を行う暗号システムであって、安全性パラメータをκとして、鍵生成アルゴリズム$Ｇｅｎ_{TBE}$（１^{κ}）により暗号化鍵$ｅｋ_{TBE}$及び復号鍵$ｄｋ_{TBE}$を生成すると共に、初期化アルゴリズムＩｎｉｔ（１^{κ}）により共通パラメータｐｕｂを生成し、前記暗号化鍵$ｅｋ_{TBE}$と前記共通パラメータｐｕｂとを前記公開鍵暗号方式の暗号化鍵ｅｋ、前記復号鍵$ｄｋ_{TBE}$を前記公開鍵暗号方式の復号鍵ｄｋとする鍵生成部と、送信者アルゴリズムＳ（１^{κ}，ｐｕｂ）により乱数ｒとコミットメントｃｏｍとデコミットメントｄｅｃとを生成し、暗号化対象の平文をｍとして暗号化アルゴリズム$Ｅｎｃ_{TBE}$（$ｅｋ_{TBE}$，ｃｏｍ，（ｍ，ｄｅｃ））により暗号文ｃを生成し、ＭＡＣ生成アルゴリズムＴ（ｒ，ｃ）によりタグσを生成し、前記コミットメントｃｏｍと前記暗号文ｃと前記タグσとを前記公開鍵暗号方式の暗号文ｃｔとする暗号化部と、前記暗号文ｃｔを前記コミットメントｃｏｍと前記暗号文ｃと前記タグσとにパースし、復号アルゴリズム$Ｄｅｃ_{TBE}$（$ｄｋ_{TBE}$，ｃｏｍ，ｃ）により平文ｍとデコミットメントｄｅｃを生成し、受信者アルゴリズムＲ（ｐｕｂ，ｃｏｍ，ｄｅｃ）により乱数値ｒにコミットできたか否かを検証し、前記コミットに成功した場合は検証アルゴリズムＶ（ｒ，ｃ，σ）により前記タグσを検証する復号部と、を有する。

発明の効果

[0007] 匿名性を確保した安全な公開鍵暗号を実現することができる。

図面の簡単な説明

[0008] [図1]本実施形態に係る暗号システムの全体構成の一例を示す図である。

[図2]コンピュータのハードウェア構成の一例を示す図である。

[図3]本実施形態に係る暗号システムの全体処理の流れの一例を示すシーケンス図である。

発明を実施するための形態

[0009] 以下、本発明の一実施形態について説明する。本実施形態では、匿名性を確保した安全な公開鍵暗号（以下、匿名公開鍵暗号ともいう。）を実現する暗号システム１について説明する。

[0010] ＜準備＞

以下では、匿名公開鍵暗号を説明するために必要な構成要素を準備する。

[0011] ≪公開鍵暗号≫

公開鍵暗号方式ＰＫＥは、３つのアルゴリズム（Gen_{PKE}，Enc_{PKE}，Dec_{PKE}）で構成される。

[0012] ・Gen_{PKE}（1^{κ}）→（ｅｋ，ｄｋ）

鍵生成アルゴリズムGen_{PKE}は、安全性パラメータκを使った1^{κ}を入力とし、鍵のペア（ｅｋ，ｄｋ）を出力する。ｅｋを暗号化鍵、ｄｋを復号鍵と呼ぶ。なお、1^{κ}は１のκビット列を表す。正確にはκのことを安全性パラメータというが、誤解がない場合は1^{κ}のことを安全性パラメータと呼んでもよい。

[0013] ・Enc_{PKE}（ｅｋ，ｍ）→ｃ

暗号化アルゴリズムEnc_{PKE}は、暗号化鍵ｅｋと平文ｍ∈Ｍを入力とし、暗号文ｃ∈Ｃを出力する。なお、Ｍは平文空間、Ｃは暗号文空間を表す。

[0014] ・Dec_{PKE}（ｄｋ，ｃ）→ｍ／⊥

復号アルゴリズムDec_{PKE}は、復号鍵ｄｋと暗号文ｃを入力とし、平文ｍ∈Ｍ又は拒否を表す記号⊥を出力する。なお、拒否を表す記号⊥は暗号文ｃの復号に失敗したことを意味し、平文空間Ｍには含まれない。

[0015] ≪タグベース暗号≫

タグベース暗号方式ＴＢＥは、３つのアルゴリズム（Gen_{TBE}，Enc_{TBE}，Dec_{TBE}）で構成される。

[0016] ・Gen_{TBE}（1^{κ}）→（ｅｋ，ｄｋ）

鍵生成アルゴリズムGen_{TBE}は、安全性パラメータκを使った1^{κ}を入力とし、鍵のペア（ｅｋ，ｄｋ）を出力する。

[0017] ・Enc_{TBE}（ｅｋ，τ，ｍ）→ｃ

暗号化アルゴリズムEnc_{TBE}は、暗号化鍵ｅｋとタグτと平文m∈Mを入力とし、暗号文ｃ∈Ｃを出力する。

[0018] ・Dec_{TBE}（ｄｋ，τ，ｃ）→m／⊥

復号アルゴリズムDec_{TBE}は、復号鍵ｄｋとタグτと暗号文ｃを入力とし、平文m∈M又は拒否を表す記号⊥を出力する。

[0019] ≪弱いコミットメント≫

弱いコミットメント方式ｗＣｏｍは、３つのアルゴリズム（Ｉｎｉｔ，Ｓ，Ｒ）で構成される。

[0020] ・Ｉｎｉｔ（1^{κ}）→ｐｕｂ

初期化アルゴリズムＩｎｉｔは、安全性パラメータκを使った1^{κ}を入力とし、共通パラメータｐｕｂを出力する。

[0021] ・Ｓ（1^{κ}，ｐｕｂ）→（ｒ，ｃｏｍ，ｄｅｃ）

送信者アルゴリズムＳは、安全性パラメータκを使った1^{κ}と共通パラメータｐｕｂを入力とし、乱数値ｒ∈｛０，１｝$^{\kappa}$とコミットメントｃｏｍとデコミットメントｄｅｃを出力する。なお、｛０，１｝$^{\kappa}$はκビット長のバイナリ系列を表す。

[0022] ・Ｒ（ｐｕｂ，ｃｏｍ，ｄｅｃ）→ｒ／⊥

受信者アルゴリズムＲは、公開パラメータｐｕｂとコミットメントｃｏｍとデコミットメントｄｅｃを入力とし、乱数値ｒ∈｛０，１｝$^{\kappa}$又は拒否を表す記号⊥を出力する。なお、拒否を表す記号⊥はコミットに失敗したことを意味し、｛０，１｝$^{\kappa}$に含まれない。

[0023] ≪メッセージ認証符号≫

メッセージ認証符号方式ＭＡＣは、２つのアルゴリズム（Ｔ，Ｖ）で構成される。

[0024] ・Ｔ（ｒ，μ）→σ

ＭＡＣ生成アルゴリズムＴは、鍵ｒ∈｛０，１｝$^{\kappa}$とメッセージμ∈｛０，１｝*を入力とし、タグσを出力する。なお、｛０，１｝*は任意長のバイナリ系列を表す。

[0025] ・Ｖ（ｒ，μ，σ）→Ｔ／⊥

検証アルゴリズムＶは、鍵ｒとメッセージμとタグσを入力とし、受諾を表す記号Ｔ又は拒否を表す記号⊥を出力する。なお、受諾を表す記号Ｔが出力された場合はタグσの検証に成功したことを意味し、拒否を表す記号⊥が出力された場合はタグσの検証に失敗したことを意味する。

[0026] ＜匿名公開鍵暗号＞

次に、上記で準備したタグベース暗号方式ＴＢＥと弱いコミットメント方式ｗＣｏｍとメッセージ認証符号方式ＭＡＣとを用いて、本実施形態に係る匿名公開鍵暗号方式ＰＫＥを構成する。なお、この構成方法そのものは、上記の非特許文献１に記載されているＢＫ変換である。ただし、上記の非特許文献１では、タグベース暗号方式ＴＢＥではなく、ＩＤベース暗号方式ＩＢＥを用いている。

[0027] 本実施形態に係る匿名公開鍵暗号方式ＰＫＥ＝（Gen_{PKE}，Enc_{PKE}，Dec_{PKE}）では、各アルゴリズムを以下のように構成する。なお、以下では、タグベース暗号方式ＴＢＥの暗号化鍵ｅｋ及び復号鍵ｄｋをそれぞれek_{TBE}及びdk_{TBE}と表す。

[0028] ・Gen_{PKE}（1^{κ}）→（ｅｋ，ｄｋ）

鍵生成アルゴリズムGen_{PKE}は、安全性パラメータκを使った1^{κ}を入力とし、暗号化鍵ｅｋと復号鍵ｄｋのペア（ｅｋ，ｄｋ）を出力する。このとき、鍵生成アルゴリズムGen_{PKE}は、以下のＳｔｅｐ１－１～Ｓｔｅｐ１－３により（ｅｋ，ｄｋ）を出力する。ただし、Ｓｔｅｐ１－１とＳｔｅｐ１－２は順不同である。

[0029] Ｓｔｅｐ１－１：（ek_{TBE}，dk_{TBE}）←Gen_{TBE}（1^{κ}）

Ｓｔｅｐ１－２：ｐｕｂ←Ｉｎｉｔ（1^{κ}）

Ｓｔｅｐ１－３：ｅｋ：＝（ek_{TBE}，ｐｕｂ）とｄｋ：＝dk_{TBE}を出力する。

[0030] ・Enc_{PKE}（ｅｋ，ｍ）→ｃｔ

暗号化アルゴリズムEnc_{PKE}は、暗号化鍵ｅｋと平文ｍ∈Ｍを入力とし、

暗号文ｃｔ∈Ｃを出力する。このとき、暗号化アルゴリズムEnc_{PKE}は、以下のＳｔｅｐ２－１～Ｓｔｅｐ２－４により暗号文ｃｔを出力する。

[0031] Ｓｔｅｐ２－１：（ｒ，ｃｏｍ，ｄｅｃ）←Ｓ（1^{κ}，ｐｕｂ）

Ｓｔｅｐ２－２：ｃ←Enc_{TBE}（ek_{TBE}，ｃｏｍ，（ｍ，ｄｅｃ））

Ｓｔｅｐ２－３：σ←Ｔ（ｒ，ｃ）

Ｓｔｅｐ２－４：ｃｔ：＝（ｃｏｍ，ｃ，σ）を出力する。

[0032] ・Dec_{PKE}（ｄｋ，ｃｔ）→ｍ／⊥

復号アルゴリズムDec_{PKE}は、復号鍵ｄｋと暗号文ｃｔを入力とし、平文ｍ∈Ｍ又は拒否を表す記号⊥を出力する。このとき、復号アルゴリズムDec_{PKE}は、以下のＳｔｅｐ３－１～Ｓｔｅｐ３－４により平文ｍ又は拒否を表す記号⊥を出力する。

[0033] Ｓｔｅｐ３－１：ｃｔ＝（ｃｏｍ，ｃ，σ）をパースする。なお、ｃｔをパースするとは、ｃｔからｃｏｍとｃとσを取り出すことを意味する。

[0034] Ｓｔｅｐ３－２：（ｍ，ｄｅｃ）←Dec_{TBE}（dk_{TBE}，ｃｏｍ，ｃ）；そして、（ｍ，ｄｅｃ）＝⊥である場合は、拒否を表す記号⊥を出力

Ｓｔｅｐ３－３：ｒ←Ｒ（ｐｕｂ，ｃｏｍ，ｄｅｃ）；そして、ｒ＝⊥である場合は、拒否を表す記号⊥を出力

Ｓｔｅｐ３－４：Ｖ（ｒ，ｃ，σ）＝⊥である場合は⊥を出力し、そうでない場合はｍを出力する。

[0035] ＜安全性について＞

上記で構成した匿名公開鍵暗号方式ＰＫＥは、その構成要素であるタグベース暗号方式ＴＢＥと弱いコミットメント方式ｗＣｏｍとメッセージ認証符号方式ＭＡＣの安全性に応じて、その安全性も変化する。

[0036] ・ＢＫの変換の場合（従来技術と同等）

タグベース暗号方式ＴＢＥがＩＮＤ－ｓｔ－ｗＣＣＡ安全

弱いコミットメント方式ｗＣｏｍが安全

メッセージ認証符号方式ＭＡＣがｓＥＵＦ－ＯＴ－ＣＭＡ安全

である場合は、匿名公開鍵暗号方式ＰＫＥはＩＮＤ－ＣＣＡ安全となる。

[0037] ・安全性パターン１

タグベース暗号方式ＴＢＥがＩＮＤｒ－ｓｔ－ｗＣＣＡ安全

弱いコミットメント方式ｗＣｏｍが安全かつＩＮＤｒ安全

メッセージ認証符号方式ＭＡＣがｓＥＵＦ－ＯＴ－ＣＭＡ安全かつ疑似ランダム

である場合は、匿名公開鍵暗号方式ＰＫＥはＩＮＤｒ－ＣＣＡ安全となる。

[0038] ・安全性パターン２

タグベース暗号方式ＴＢＥがＯＳ－ｓｔ－ｗＣＣＡ安全

弱いコミットメント方式ｗＣｏｍが安全かつＯＳ安全

メッセージ認証符号方式ＭＡＣがｓＥＵＦ－ＯＴ－ＣＭＡ安全かつＯＳ安全

である場合は、匿名公開鍵暗号方式ＰＫＥはＯＳ－ＣＣＡ安全となる。

[0039] このように、上記で構成した匿名公開鍵暗号方式ＰＫＥはその構成要素の安全性を変化させることで、当該匿名公開鍵暗号方式ＰＫＥの安全性も変化する。また、上記の通り、安全性パターン１及び安全性パターン２では、匿名公開鍵暗号方式ＰＫＥの安全性はそれぞれＩＮＤｒ－ＣＣＡ安全及びＯＳ－ＣＣＡ安全となる。このため、タグベース暗号方式ＴＢＥ、弱いコミットメント方式ｗＣｏｍ、及びメッセージ認証符号方式ＭＡＣの安全性として安全性パターン１又は安全性パターン２を採用することで、匿名性を確保した安全な公開鍵暗号方式ＰＫＥを実現することができる。なお、安全性パターン１の場合に匿名公開鍵暗号方式ＰＫＥがＩＮＤｒ－ＣＣＡ安全であること、安全性パターン２の場合に匿名公開鍵暗号方式ＰＫＥがＯＳ－ＣＣＡ安全であることはいずれも証明可能である。

[0040] なお、上記の各安全性の定義は一般的に知られているものであるが、必要に応じて以下の参考文献等を参照されたい。

[0041] 参考文献１：Ran Canetti and Marc Fischlin. Universally composable commitments. In Joe Kilian, editor, CRYPTO 2001, volume 2139 of LNCS, pages 19-40. Springer, Heidelberg, August 2001.

参考文献２：Charles Rackoff and Daniel R. Simon. Noninteractive zero-knowledge proof of knowledge and chosen ciphertext attack. In Joan Feigenbaum, editor, CRYPTO'91, volume 576
of LNCS, pages 433-444. Springer, Heidelberg, August 1992.

参考文献３：Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway. Relations among notions of security for public-key encryption schemes. In Hugo Krawczyk, editor, CRYPTO'98, volume 1462 of LNCS, pages 26-45. Springer, Heidelberg, August 1998.

参考文献４：Eike Kiltz. Chosen-ciphertext security from tag-based encryption. In Shai Halevi and Tal Rabin, editors, TCC 2006, volume 3876 of LNCS, pages 581-600. Springer, Heidelberg, March 2006.

＜暗号システム１の全体構成＞

次に、本実施形態に係る暗号システム１の全体構成について、図１を参照しながら説明する。図１は、本実施形態に係る暗号システム１の全体構成の一例を示す図である。

[0042] 図１に示すように、本実施形態に係る暗号システム１には、暗号化装置１０と、復号装置２０とが含まれる。また、暗号化装置１０と復号装置２０は、インターネット等の通信ネットワーク３０を介して通信可能に接続される。

[0043] 暗号化装置１０は、平文ｍを暗号化する端末や機器等の各種情報処理装置である。暗号化装置１０は、暗号化処理部１０１と、記憶部１０２とを有する。暗号化処理部１０１は、匿名公開鍵暗号方式ＰＫＥの暗号化アルゴリズムＥｎｃ$_{PKE}$により平文ｍを暗号化する。記憶部１０２には、匿名公開鍵暗号方式ＰＫＥの暗号化アルゴリズムＥｎｃ$_{PKE}$の実行に必要な各種情報（例えば、暗号化鍵ｅｋ、安全性パラメータκ、共通パラメータｐｕｂ等）が記憶される。

[0044] 復号装置２０は、暗号文ｃｔを復号する端末や機器等の各種情報処理装置である。復号装置２０は、鍵生成処理部２０１と、復号処理部２０２と、記

憶部２０３とを有する。鍵生成処理部２０１は、匿名公開鍵暗号方式ＰＫＥの鍵生成アルゴリズムGen_{PKE}により暗号化鍵ｅｋ及び復号鍵ｄｋを生成する。復号処理部２０２は、匿名公開鍵暗号方式ＰＫＥの復号アルゴリズムDec_{PKE}により暗号文ｃｔを復号する。記憶部２０３には、匿名公開鍵暗号方式ＰＫＥの鍵生成アルゴリズムGen_{PKE}や復号アルゴリズムDec_{PKE}の実行に必要な情報（例えば、安全性パラメータκ、共通パラメータｐｕｂ、復号鍵ｄｋ等）が記憶される。なお、以下では、安全性パラメータκ及び共通パラメータｐｕｂを公開パラメータともいう。

[0045] なお、図１に示す例では、匿名公開鍵暗号方式ＰＫＥの暗号化鍵ｅｋ及び復号鍵ｄｋを復号装置２０が生成しているが、これは一例であって、例えば、鍵生成局等として機能するサーバが当該暗号化鍵ｅｋ及び復号鍵ｄｋを生成してもよい。この場合、当該サーバが鍵生成処理部２０１を有しており、この鍵生成処理部２０１により暗号化鍵ｅｋ及び復号鍵ｄｋが生成され、当該復号鍵ｄｋは何等かのセキュアな方法で復号装置２０に配布される一方で、当該暗号化鍵ｅｋと公開パラメータは暗号化装置１０及び復号装置２０に公開される。

[0046] ＜暗号システム１のハードウェア構成＞

次に、本実施形態に係る暗号システム１に含まれる暗号化装置１０及び復号装置２０のハードウェア構成について説明する。これらの暗号化装置１０及び復号装置２０は、例えば、図２に示すコンピュータ５００のハードウェア構成により実現可能である。

[0047] 図２に示すコンピュータ５００は、ハードウェアとして、入力装置５０１と、表示装置５０２と、外部Ｉ／Ｆ５０３と、通信Ｉ／Ｆ５０４と、プロセッサ５０５と、メモリ装置５０６とを有する。これらの各ハードウェアは、それぞれがバス５０７を介して通信可能に接続されている。

[0048] 入力装置５０１は、例えば、キーボードやマウス、タッチパネル等である。表示装置５０２は、例えば、ディスプレイ等である。なお、コンピュータ５００は、入力装置５０１及び表示装置５０２のうちの少なくとも一方を有

していなくてもよい。

[0049] 外部Ｉ／Ｆ５０３は、記録媒体５０３ａ等の外部装置とのインタフェースである。なお、記録媒体５０３ａとしては、例えば、ＣＤ（Compact Disc）、ＤＶＤ（Digital Versatile Disk）、ＳＤメモリカード（Secure Digital memory card）、ＵＳＢ（Universal Serial Bus）メモリカード等が挙げられる。

[0050] 通信Ｉ／Ｆ５０４は、通信ネットワーク３０に接続するためのインタフェースである。プロセッサ５０５は、例えば、ＣＰＵ（Central Processing Unit）やＧＰＵ（Graphics Processing Unit）等といった各種演算装置である。メモリ装置５０６は、例えば、ＨＤＤ（Hard Disk Drive）やＳＳＤ（Solid State Drive）、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）、フラッシュメモリ等といった各種記憶装置である。

[0051] 本実施形態に係る暗号化装置１０及び復号装置２０は、図２に示すコンピュータ５００のハードウェア構成により、後述する各種処理を実現することができる。なお、図２に示すコンピュータ５００のハードウェア構成は一例であって、暗号システム１が適用される対象の用途等に応じて種々のハードウェア構成が採用されてもよい。

[0052] なお、暗号化処理部１０１は、例えば、暗号化装置１０にインストールされた１以上のプログラムが、当該暗号化装置１０を実現するコンピュータ５００のプロセッサ５０５に実行させる処理により実現される。また、記憶部１０２は、例えば、当該暗号化装置１０を実現するコンピュータ５００のメモリ装置５０６により実現される。

[0053] 同様に、鍵生成処理部２０１及び復号処理部２０２は、例えば、復号装置２０にインストールされた１以上のプログラムが、当該復号装置２０を実現するコンピュータ５００のプロセッサ５０５に実行させる処理により実現される。また、記憶部２０３は、例えば、当該復号装置２０を実現するコンピュータ５００のメモリ装置５０６により実現される。

[0054] ＜暗号システム１の全体処理＞

次に、本実施形態に係る暗号システム１の全体処理の流れについて、図３を参照しながら説明する。図３は、本実施形態に係る暗号システム１の全体処理の流れの一例を示すシーケンス図である。

[0055] まず、復号装置２０の鍵生成処理部２０１は、匿名公開鍵暗号方式ＰＫＥの鍵生成アルゴリズム$Ｇｅｎ_{PKE}$（1^{κ}）を実行し、暗号化鍵ｅｋと復号鍵ｄｋとを生成する（ステップＳ１０１）。なお、復号鍵ｄｋは記憶部２０３に保存される。

[0056] 次に、復号装置２０の鍵生成処理部２０１は、公開パラメータ（つまり、安全性パラメータκ及び共通パラメータｐｕｂ）と、上記のステップＳ１０１で生成された暗号化鍵ｅｋとを暗号化装置１０に送信する（ステップＳ１０２）。なお、本ステップでは公開パラメータと暗号化鍵ｅｋとを暗号化装置１０に送信しているが、必ずしも送信する必要はなく、例えば、暗号化装置１０が参照可能なサーバ等に保存されてもよい。

[0057] 暗号化装置１０の暗号化処理部１０１は、匿名公開鍵暗号方式ＰＫＥの暗号化アルゴリズム$Ｅｎｃ_{PKE}$（ｅｋ，ｍ）を実行し、平文ｍを暗号化する（ステップＳ１０３）。これにより、暗号文ｃｔが生成される。

[0058] 次に、暗号化装置１０の暗号化処理部１０１は、上記のステップＳ１０３で生成された暗号文ｃｔを復号装置２０に送信する（ステップＳ１０４）。

[0059] 復号装置２０の復号処理部２０２は、匿名公開鍵暗号方式ＰＫＥの復号アルゴリズム$Ｄｅｃ_{PKE}$（ｄｋ，ｃｔ）を実行し、暗号文ｃｔを復号する（ステップＳ１０５）。これにより、平文ｍが生成される。

[0060] 本発明は、具体的に開示された上記の実施形態に限定されるものではなく、請求の範囲の記載から逸脱することなく、種々の変形や変更、既知の技術との組み合わせ等が可能である。

符号の説明

[0061]

１	暗号システム
１０	暗号化装置
２０	復号装置

３０　　通信ネットワーク

１０１　　暗号化処理部

１０２　　記憶部

２０１　　鍵生成処理部

２０２　　復号処理部

２０３　　記憶部

請求の範囲

[請求項1] タグベース暗号方式ＴＢＥ＝（Gen_{TBE}，Enc_{TBE}，Dec_{TBE}）と弱いコミットメント方式ｗＣｏｍ＝（Ｉｎｉｔ，Ｓ，Ｒ）とメッセージ認証符号方式ＭＡＣ＝（Ｔ，Ｖ）とで構成される公開鍵暗号方式により暗号化及び復号を行う暗号システムであって、

安全性パラメータをκとして、鍵生成アルゴリズムGen_{TBE}（1^{κ}）により暗号化鍵ek_{TBE}及び復号鍵dk_{TBE}を生成すると共に、初期化アルゴリズムＩｎｉｔ（1^{κ}）により共通パラメータｐｕｂを生成し、前記暗号化鍵ek_{TBE}と前記共通パラメータｐｕｂとを前記公開鍵暗号方式の暗号化鍵ｅｋ、前記復号鍵dk_{TBE}を前記公開鍵暗号方式の復号鍵ｄｋとする鍵生成部と、

送信者アルゴリズムＳ（1^{κ}，ｐｕｂ）により乱数ｒとコミットメントｃｏｍとデコミットメントｄｅｃとを生成し、暗号化対象の平文をｍとして暗号化アルゴリズムEnc_{TBE}（ek_{TBE}，ｃｏｍ，（ｍ，ｄｅｃ））により暗号文ｃを生成し、ＭＡＣ生成アルゴリズムＴ（ｒ，ｃ）によりタグσを生成し、前記コミットメントｃｏｍと前記暗号文ｃと前記タグσとを前記公開鍵暗号方式の暗号文ｃｔとする暗号化部と、

前記暗号文ｃｔを前記コミットメントｃｏｍと前記暗号文ｃと前記タグσとにパースし、復号アルゴリズムDec_{TBE}（dk_{TBE}，ｃｏｍ，ｃ）により平文ｍとデコミットメントｄｅｃを生成し、受信者アルゴリズムＲ（ｐｕｂ，ｃｏｍ，ｄｅｃ）により乱数値ｒにコミットできたか否かを検証し、前記コミットに成功した場合は検証アルゴリズムＶ（ｒ，ｃ，σ）により前記タグσを検証する復号部と、

を有する暗号システム。

[請求項2] 前記タグベース暗号方式ＴＢＥがＩＮＤｒ－ｓｔ－ｗＣＣＡ安全、前記弱いコミットメント方式ｗＣｏｍが安全かつＩＮＤｒ安全、前記メッセージ認証符号方式ＭＡＣがｓＥＵＦ－ＯＴ－ＣＭＡ安全かつ疑

似ランダムである場合、前記公開鍵暗号方式は、ＩＮＤｒ－ＣＣＡ安全であり、

前記タグベース暗号方式ＴＢＥがＯＳ－ｓｔ－ｗＣＣＡ安全、前記弱いコミットメント方式ｗＣｏｍが安全かつＯＳ安全、前記メッセージ認証符号方式ＭＡＣがｓＥＵＦ－ＯＴ－ＣＭＡ安全かつＯＳ安全である場合、前記公開鍵暗号方式は、ＯＳ－ＣＣＡ安全である、請求項１に記載の暗号システム。

[請求項3] タグベース暗号方式ＴＢＥ＝（Gen_{TBE}，Enc_{TBE}，Dec_{TBE}）と弱いコミットメント方式ｗＣｏｍ＝（Ｉｎｉｔ，Ｓ，Ｒ）とメッセージ認証符号方式ＭＡＣ＝（Ｔ，Ｖ）とで構成される公開鍵暗号方式により平文ｍを暗号化する暗号化装置であって、

安全性パラメータをκ、共通パラメータをｐｕｂとして送信者アルゴリズムＳ（1^{κ}，ｐｕｂ）により乱数ｒとコミットメントｃｏｍとデコミットメントｄｅｃとを生成し、前記公開鍵暗号方式の暗号化鍵をｅｋ＝ek_{TBE}として暗号化アルゴリズムEnc_{TBE}（ek_{TBE}，ｃｏｍ，（ｍ，ｄｅｃ））により暗号文ｃを生成し、ＭＡＣ生成アルゴリズムＴ（ｒ，ｃ）によりタグσを生成し、前記コミットメントｃｏｍと前記暗号文ｃと前記タグσとを前記公開鍵暗号方式の暗号文ｃｔとする暗号化部と、

前記暗号化装置と通信ネットワークを介して接続される復号装置に前記暗号文ｃｔを送信する送信部と、

を有する暗号化装置。

[請求項4] タグベース暗号方式ＴＢＥ＝（Gen_{TBE}，Enc_{TBE}，Dec_{TBE}）と弱いコミットメント方式ｗＣｏｍ＝（Ｉｎｉｔ，Ｓ，Ｒ）とメッセージ認証符号方式ＭＡＣ＝（Ｔ，Ｖ）とで構成される公開鍵暗号方式により暗号文ｃｔを復号する復号装置であって、

安全性パラメータをκとして、鍵生成アルゴリズムGen_{TBE}（1^{κ}）により暗号化鍵ek_{TBE}及び復号鍵dk_{TBE}を生成すると共に、初

期化アルゴリズムＩｎｉｔ（1^{κ}）により共通パラメータｐｕｂを生成し、前記暗号化鍵ek_{TBE}と前記共通パラメータｐｕｂとを前記公開鍵暗号方式の暗号化鍵ｅｋ、前記復号鍵dk_{TBE}を前記公開鍵暗号方式の復号鍵ｄｋとする鍵生成部と、

前記暗号文ｃｔをコミットメントｃｏｍと暗号文ｃとタグσとにパースし、復号アルゴリズムDec_{TBE}（dk_{TBE}，ｃｏｍ，ｃ）により平文ｍとデコミットメントｄｅｃを生成し、受信者アルゴリズムＲ（ｐｕｂ，ｃｏｍ，ｄｅｃ）により乱数値ｒにコミットできたか否かを検証し、前記コミットに成功した場合は検証アルゴリズムＶ（ｒ，ｃ，σ）により前記タグσを検証する復号部と、

を有する復号装置。

[請求項5] タグベース暗号方式ＴＢＥ＝（Gen_{TBE}，Enc_{TBE}，Dec_{TBE}）と弱いコミットメント方式ｗＣｏｍ＝（Ｉｎｉｔ，Ｓ，Ｒ）とメッセージ認証符号方式ＭＡＣ＝（Ｔ，Ｖ）とで構成される公開鍵暗号方式により暗号化及び復号を行う暗号システムが、

安全性パラメータをκとして、鍵生成アルゴリズムGen_{TBE}（1^{κ}）により暗号化鍵ek_{TBE}及び復号鍵dk_{TBE}を生成すると共に、初期化アルゴリズムＩｎｉｔ（1^{κ}）により共通パラメータｐｕｂを生成し、前記暗号化鍵ek_{TBE}と前記共通パラメータｐｕｂとを前記公開鍵暗号方式の暗号化鍵ｅｋ、前記復号鍵dk_{TBE}を前記公開鍵暗号方式の復号鍵ｄｋとする鍵生成手順と、

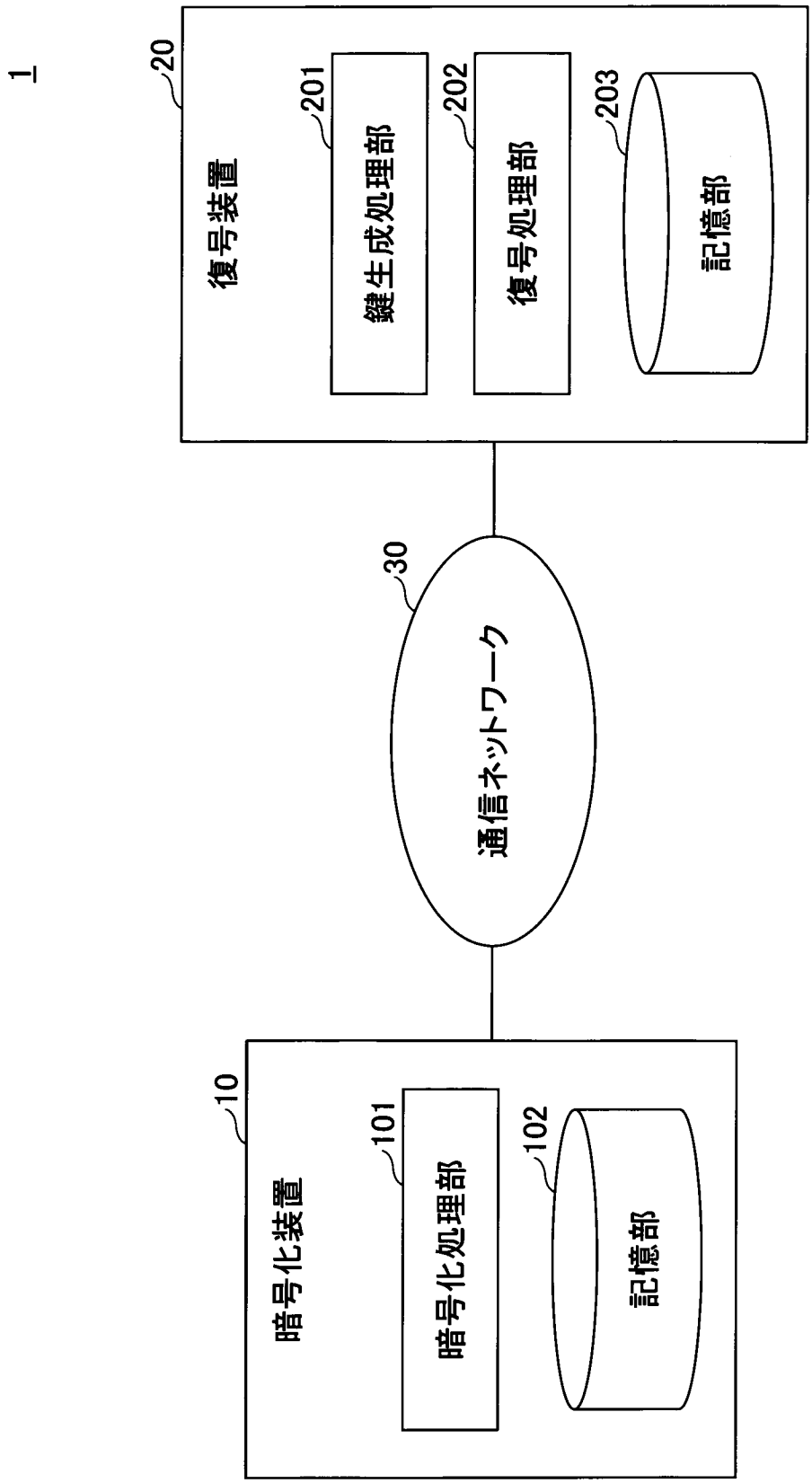
送信者アルゴリズムＳ（1^{κ}，ｐｕｂ）により乱数ｒとコミットメントｃｏｍとデコミットメントｄｅｃとを生成し、暗号化対象の平文をｍとして暗号化アルゴリズムEnc_{TBE}（ek_{TBE}，ｃｏｍ，（ｍ，ｄｅｃ））により暗号文ｃを生成し、ＭＡＣ生成アルゴリズムＴ（ｒ，ｃ）によりタグσを生成し、前記コミットメントｃｏｍと前記暗号文ｃと前記タグσとを前記公開鍵暗号方式の暗号文ｃｔとする暗号化手順と、

前記暗号文ｃｔを前記コミットメントｃｏｍと前記暗号文ｃと前記タグσとにパースし、復号アルゴリズムDec_{TBE}（dk_{TBE}，ｃｏｍ，ｃ）により平文ｍとデコミットメントｄｅｃを生成し、受信者アルゴリズムＲ（ｐｕｂ，ｃｏｍ，ｄｅｃ）により乱数値ｒにコミットできたか否かを検証し、前記コミットに成功した場合は検証アルゴリズムＶ（ｒ，ｃ，σ）により前記タグσを検証する復号手順と、

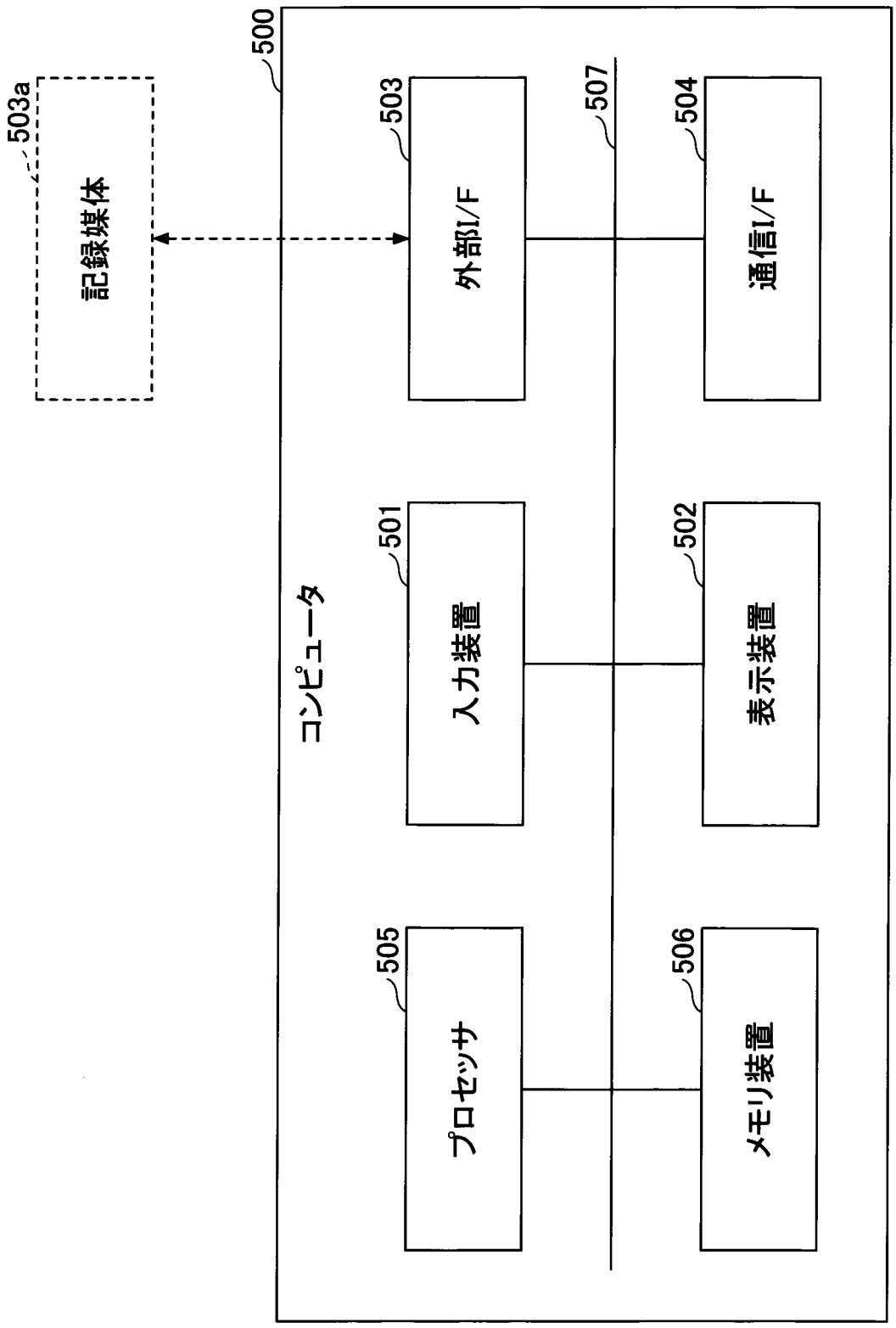
を実行する方法。

[請求項6] コンピュータを、請求項３に記載の暗号化装置、又は、請求項４に記載の復号装置、として機能させるプログラム。

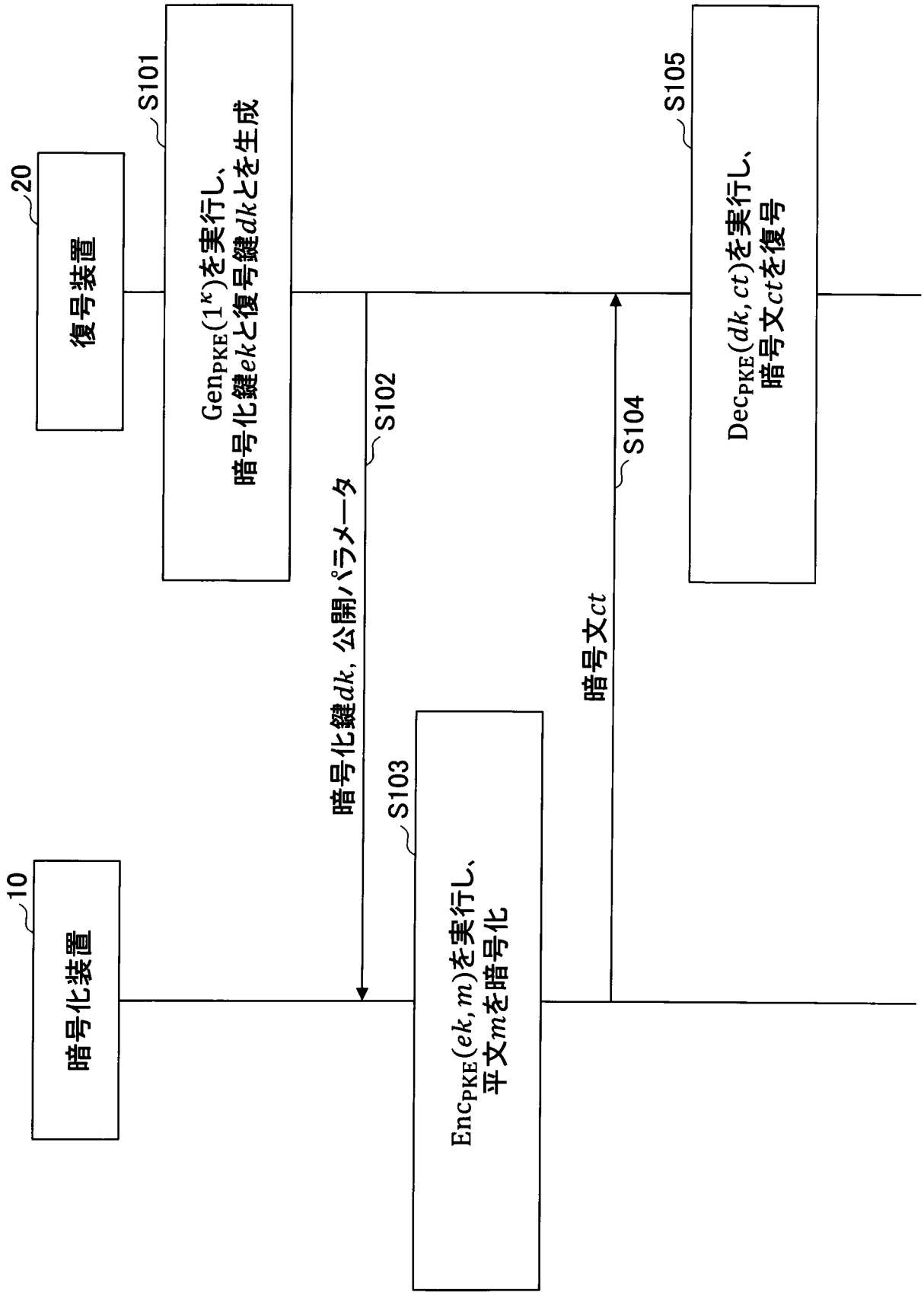
[図1]


1
20
復号装置
201
鍵生成処理部
202
復号処理部
203
記憶部
30
通信ネットワーク
10
暗号化装置
101
暗号化処理部
102
記憶部

[図2]


500
503a
記録媒体
503
外部I/F
507
504
通信I/F
501
入力装置
502
表示装置
コンピュータ
505
プロセッサ
506
メモリ装置

[図3]


20
復号装置
S101
$\mathrm{Gen}_{\mathrm{PKE}}(1^{\kappa})$を実行し、
暗号化鍵ekと復号鍵dkとを生成
S105
$\mathrm{Dec}_{\mathrm{PKE}}(dk, ct)$を実行し、
暗号文ctを復号
S102
暗号化鍵dk, 公開パラメータ
S104
暗号文ct
10
暗号化装置
S103
$\mathrm{Enc}_{\mathrm{PKE}}(ek, m)$を実行し、
平文mを暗号化

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2021/015630

A. CLASSIFICATION OF SUBJECT MATTER
H04L 9/32(2006.01)i
FI: H04L9/00 675Z

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2021
Registered utility model specifications of Japan	1996-2021
Published registered utility model applications of Japan	1994-2021

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2015-501110 A (THOMSON LICENSING) 08 January 2015 (2015-01-08) paragraph [0012]	1-6

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 June 2021 (28.06.2021)	06 July 2021 (06.07.2021)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2021/015630

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2015-501110 A	08 Jan. 2015	WO 2013/087629 A1 page 3, line 26 to page 4, line 30 US 2014/0321642 A1 EP 2792098 A1 CN 103988466 A KR 10-2014-0103269 A	

国際調査報告

国際出願番号
PCT/JP2021/015630

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

H04L 9/32(2006.01)i
FI: H04L9/00 675Z

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０２１年
日本国実用新案登録公報	１９９６－２０２１年
日本国登録実用新案公報	１９９４－２０２１年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2015-501110 A (トムソン ライセンシング) 08.01.2015 (2015-01-08) 段落［００１２］	1-6

☐ Ｃ欄の続きにも文献が列挙されている。

☑ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー
"A" 特に関連のある文献ではなく、一般的技術水準を示すもの
"E" 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
"L" 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
"O" 口頭による開示、使用、展示等に言及する文献
"P" 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
"T" 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの
"X" 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
"Y" 特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
"&" 同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
28.06.2021	06.07.2021

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
松平　英 5S 3146
電話番号 03-3581-1101 内線 3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2021/015630

引用文献	公表日	パテントファミリー文献	公表日
JP 2015-501110 A	08.01.2015	WO 2013/087629 A1 第３頁第２６行－第４頁第３０行 US 2014/0321642 A1 EP 2792098 A1 CN 103988466 A KR 10-2014-0103269 A	