

(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11月17日(17.11.2022)



(10) 国際公開番号

WO 2022/239129 A1

(51) 国際特許分類:
H04L 9/08 (2006.01)

(21) 国際出願番号: PCT/JP2021/017943

(22) 国際出願日: 2021年5月11日(11.05.2021)

(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: 中 邑 聡 史 (NAKAMURA, Satoshi); 〒1808585 東京都武蔵野市緑町3丁目9-

1 1 N T T 知的財産センタ内 Tokyo (JP).
齋藤 恒和 (SAITO, Tsunekazu); 〒1808585 東京都武蔵野市緑町3丁目9-1 1 N T T 知的財産センタ内 Tokyo (JP).

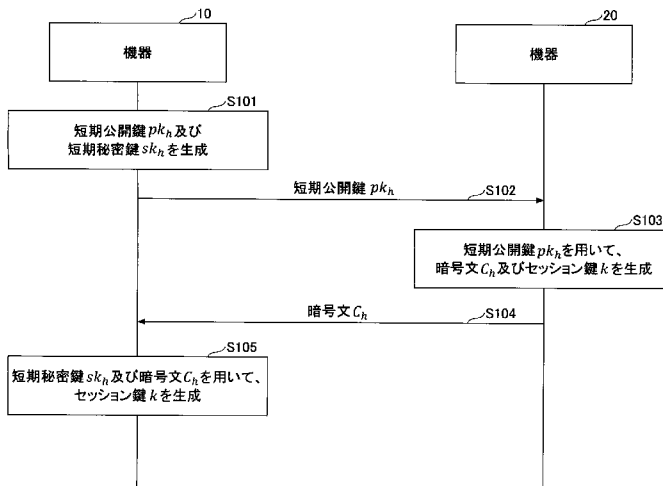
(74) 代理人: 伊東 忠重, 外 (ITO, Tadashige et al.); 〒1000005 東京都千代田区丸の内二丁目1番1号 丸の内 M Y P L A Z A (明治安田生命ビル) 16階 Tokyo (JP).

(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,

(54) Title: KEY EXCHANGE SYSTEM, DEVICE, KEY EXCHANGE METHOD, AND PROGRAM

(54) 発明の名称: 鍵交換システム、機器、鍵交換方法、及びプログラム

[図2]



10, 20 Device
S101 Generate short-term public key pk_h and short-term private key sk_h
S102 Short-term public key pk_h
S103 Use short-term public key pk_h to generate ciphertext C_h and session key k
S104 Ciphertext C_h
S105 Use short-term private key sk_h and ciphertext C_h to generate session key k

(57) Abstract: A key exchange system according to one embodiment has: a key generation unit that generates a first short-term private key and a first short-term public key of a quantum-resistant first key encapsulation mechanism, and a second short-term private key and a second short-term public key of a second key encapsulation mechanism, said second key encapsulation mechanism being traditional compared to the first key encapsulation mechanism, and generates a third short-term private key in which the first short-term private key and the second short-term private key are linked, and a third short-term public key in which the first short-term public key and the second short-term public key are linked; an encryption unit that uses the third short-term public key to generate a first ciphertext and a first shared key of the first key encapsulation mechanism, and a second ciphertext and a second shared key of the second key encapsulation mechanism, and generates a third shared key using a key generation function that treats the first shared key, the second shared key, the third short-term public key, the first ciphertext, and the second ciphertext as inputs; and a decryption unit that uses the

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,
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))

third short-term private key to decrypt each of the first ciphertext and the second ciphertext and generate the first shared key and the second shared key, and generates the third shared key using the key generation function that treats the first shared key, the second shared key, the third short-term public key, the first ciphertext, and the second ciphertext as inputs.

(57) 要約：一実施形態に係る鍵交換システムは、耐量子性を持つ第1の鍵カプセル化メカニズムの第1の短期秘密鍵及び第1の短期公開鍵と、前記第1の鍵カプセル化メカニズムに対して古典的な第2の鍵カプセル化メカニズムの第2の短期秘密鍵及び第2の短期公開鍵とを生成し、前記第1の短期秘密鍵と前記第2の短期秘密鍵とを連結した第3の短期秘密鍵と、前記第1の短期公開鍵と前記第2の短期公開鍵とを連結した第3の短期公開鍵とを生成する鍵生成部と、前記第3の短期公開鍵を用いて、前記第1の鍵カプセル化メカニズムの第1の暗号文及び第1の共有鍵と、前記第2の鍵カプセル化メカニズムの第2の暗号文及び第2の共有鍵とを生成し、前記第1の共有鍵と前記第2の共有鍵と前記第3の短期公開鍵と前記第1の暗号文と前記第2の暗号文を入力とする鍵生成関数により第3の共有鍵を生成する暗号化部と、前記第3の短期秘密鍵を用いて、前記第1の暗号文と前記第2の暗号文とをそれぞれ復号して前記第1の共有鍵と前記第2の共有鍵とを生成し、前記第1の共有鍵と前記第2の共有鍵と前記第3の短期公開鍵と前記第1の暗号文と前記第2の暗号文を入力とする前記鍵生成関数により前記第3の共有鍵を生成する復号部と、を有する。

明 細 書

発明の名称：

鍵交換システム、機器、鍵交換方法、及びプログラム

技術分野

[0001] 本発明は、鍵交換システム、機器、鍵交換方法、及びプログラムに関する。

背景技術

[0002] 量子計算機の実用化により、既存の暗号方式の安全性基盤となる数学的問題（例えば、素因数分解問題、離散対数問題）を現実的な時間内で解けるようになることが知られている。このため、既存の暗号方式であるRSA暗号や楕円曲線暗号等が危殆化する恐れがあり、量子計算機でも解読できない暗号（耐量子計算機暗号）への移行が必要となる。

[0003] 鍵カプセル化技術（KEM: Key Encapsulation Mechanism）と呼ばれる技術が知られている。鍵カプセル化技術とは、公開鍵暗号を利用して共有鍵をカプセル化し、1回の通信により共有鍵を受信者に配送する技術である。耐量子のKEMとしては、NIST（National Institute of Standards and Technology）等のコンテストで提案されている（例えば、非特許文献1参照）。

先行技術文献

非特許文献

[0004] 非特許文献1：NISTの耐量子計算機暗号標準化活動，インターネット<URL : <https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions>>

発明の概要

発明が解決しようとする課題

[0005] しかしながら、耐量子のKEMは新しい技術であるため、十分に安全性の検証が行われた従来の暗号方式とは異なり、現在安全性の検証を行っている

最中である。このため、全く新しい攻撃が発見され、それにより危殆化する可能性がある。

[0006] 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、安全性が検証された暗号方式と耐量子暗号方式とのハイブリッド方式の鍵カプセル化技術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

[0007] 上記目的を達成するため、一実施形態に係る鍵交換システムは、耐量子性を持つ第1の鍵カプセル化メカニズムの第1の短期秘密鍵及び第1の短期公開鍵と、前記第1の鍵カプセル化メカニズムに対して古典的な第2の鍵カプセル化メカニズムの第2の短期秘密鍵及び第2の短期公開鍵とを生成し、前記第1の短期秘密鍵と前記第2の短期秘密鍵とを連結した第3の短期秘密鍵と、前記第1の短期公開鍵と前記第2の短期公開鍵とを連結した第3の短期公開鍵とを生成する鍵生成部と、前記第3の短期公開鍵を用いて、前記第1の鍵カプセル化メカニズムの第1の暗号文及び第1の共有鍵と、前記第2の鍵カプセル化メカニズムの第2の暗号文及び第2の共有鍵とを生成し、前記第1の共有鍵と前記第2の共有鍵と前記第3の短期公開鍵と前記第1の暗号文と前記第2の暗号文を入力とする鍵生成関数により第3の共有鍵を生成する暗号化部と、前記第3の短期秘密鍵を用いて、前記第1の暗号文と前記第2の暗号文とをそれぞれ復号して前記第1の共有鍵と前記第2の共有鍵とを生成し、前記第1の共有鍵と前記第2の共有鍵と前記第3の短期公開鍵と前記第1の暗号文と前記第2の暗号文を入力とする前記鍵生成関数により前記第3の共有鍵を生成する復号部と、を有する。

発明の効果

[0008] 安全性が検証された暗号方式と耐量子暗号方式とのハイブリッド方式の鍵カプセル化技術を実現することができる。

図面の簡単な説明

[0009] [図1]本実施形態に係る鍵交換システムの全体構成の一例を示す図である。

[図2]本実施形態に係る鍵交換処理の一例を示すシーケンス図である。

[図3]本実施形態に係る機器のハードウェア構成の一例を示す図である。

発明を実施するための形態

[0010] 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、十分に安全性の検証が行われた暗号方式と耐量子暗号方式とを組み合わせたハイブリッド方式の鍵カプセル化技術を提案し、この鍵カプセル化技術により鍵交換を行う鍵交換システム1について説明する。

[0011] <鍵カプセル化技術>

鍵カプセル化技術KEMは、3つのアルゴリズム ($KeyGen$, $Encap$, $Decap$) で構成される。なお、これらのアルゴリズムは関数や手続き等と称されてもよい。

[0012] $KeyGen() \rightarrow (sk, pk)$: $KeyGen$ アルゴリズムは、短期秘密鍵 sk と短期公開鍵 pk とを出力する。なお、 $KeyGen$ アルゴリズムは、例えば、鍵のサイズ等のパラメータを入力としてもよい。

[0013] $Encap(pk) \rightarrow (k, C)$: $Encap$ アルゴリズムは、短期公開鍵 pk を入力し、セッション鍵 k と暗号文 C とを出力する。

[0014] $Decap(sk, C) \rightarrow k / error$: $Decap$ アルゴリズムは、短期秘密鍵 sk と暗号文 C とを入力し、セッション鍵 k 又は復号失敗を示す $error$ を出力する。

[0015] 以下では、耐量子暗号方式のKEM（以下、耐量子KEMともいう。）を $KEM_{POSTQ} = (KeyGen_{POSTQ}, Encap_{POSTQ}, Decap_{POSTQ})$ とする。

[0016] また、これらのアルゴリズムの入力及び出力を、

$$KeyGen_{POSTQ}() \rightarrow (sk_{POSTQ}, pk_{POSTQ})$$

$$Encap_{POSTQ}(pk_{POSTQ}) \rightarrow (k_{POSTQ}, C_{POSTQ})$$

$$Decap(sk_{POSTQ}, C_{POSTQ}) \rightarrow k_{POSTQ} / error$$

とする。

[0017] また、十分に安全性の検証が行われ、従来から存在する暗号方式（このような暗号方式は耐量子暗号方式に対して古典的な暗号方式であるため、以下

、古典KEMともいう。)を $KEM_{PREQ} = (KeyGen_{PREQ}, Encap_{PREQ}, Decap_{PREQ})$ とする。

[0018] また、これらのアルゴリズムの入力及び出力を、

$$KeyGen_{PREQ}() \rightarrow (sk_{PREQ}, pk_{PREQ})$$

$$Encap_{PREQ}(pk_{PREQ}) \rightarrow (k_{PREQ}, C_{PREQ})$$

$$Decap(sk_{PREQ}, C_{PREQ}) \rightarrow k_{PREQ} / error$$

とする。

[0019] なお、耐量子 KEM_{POSTQ} の具体例としては、例えば、NISTの耐量子コンテストで提案されている技術等が挙げられる（これらの技術については、上記の非特許文献1を参照されたい。）。一方で、古典 KEM_{PREQ} の具体例としては、例えば、PSEC-KEMやRSA-KEM等が挙げられる。PSEC-KEMについては以下の参考文献1、RSA-KEMについては以下の参考文献2等をそれぞれ参照されたい。

[0020] 参考文献1：PSEC-KEM Specification version 2.2, インターネット<URL : https://info.isl.ntt.co.jp/crypt/psec/dl/iso/psec-kem_v2.2_20080414e.pdf>

参考文献2：Use of the RSA-KEM Key Transport Algorithm in the Cryptographic Message Syntax (CMS), インターネット<URL : <https://tools.ietf.org/pdf/rfc5990.pdf>>

ただし、上記の具体例は一例であって、耐量子 KEM_{POSTQ} としては任意の耐量子KEMを採用することができるし、古典 KEM_{PREQ} としては任意の古典KEM（特に、十分に安全性の検証が行われたKEM）を採用することができる。

[0021] 以上の耐量子 KEM_{POSTQ} と古典 KEM_{PREQ} とを用いて、これらのハイブリッド方式のKEM（以下、ハイブリッドKEMともいう。）を構成する。ハイブリッドKEMを $KEM_h = (KeyGen_h, Encap_h, Decap_h)$ とする。

[0022] $KeyGen_h = KeyGen_{POSTQ} || KeyGen_{PREQ}$ とする。

[0023] 具体的には、 $\text{KeyGen}_h() \rightarrow (s k_h, p k_h) = (s k_{\text{POSTQ}} || s k_{\text{PREQ}}, p k_{\text{POSTQ}} || p k_{\text{PREQ}})$ とする。ここで、 $||$ は連結（ビット列の連結、結合、コンカチネート、又は単にコンカチ、等とも呼ばれる。）を表す。

[0024] すなわち、ハイブリッド KEM_h の短期秘密鍵 $s k_h$ を、耐量子 $\text{KEM}_{\text{POSTQ}}$ の短期秘密鍵 $s k_{\text{POSTQ}}$ と古典 KEM_{PREQ} の短期秘密鍵 $s k_{\text{PREQ}}$ とを連結したものとする。同様に、ハイブリッド KEM_h の短期公開鍵 $p k_h$ を、耐量子 $\text{KEM}_{\text{POSTQ}}$ の短期公開鍵 $p k_{\text{POSTQ}}$ と古典 KEM_{PREQ} の短期公開鍵 $p k_{\text{PREQ}}$ とを連結したものとする。

[0025] $\text{Encap}_h = \text{Encap}_{\text{POSTQ}} || \text{Encap}_{\text{PREQ}}$ とする。

[0026] 具体的には、 $\text{Encap}_h(p k_h) \rightarrow (k, C_h)$ として、以下とする。

[0027] $C_h = C_{\text{POSTQ}} || C_{\text{PREQ}}$

$k_h = k_{\text{POSTQ}} || k_{\text{PREQ}}$

$k = \text{KDF}(k_h || p k_h || C_h)$

ここで、 $\text{KDF}()$ は鍵導出関数である。

[0028] $\text{Decap}_h = \text{Decap}_{\text{POSTQ}} || \text{Decap}_{\text{PREQ}}$ とする。

[0029] 具体的には、 $\text{Decap}_h(s k_h, C_h) \rightarrow k = \text{KDF}(k_h || p k_h || C_h) / \text{error}$ とする。

[0030] このように、耐量子 $\text{KEM}_{\text{POSTQ}}$ と古典 KEM_{PREQ} とを用いて、ハイブリッド $\text{KEM}_h = (\text{KeyGen}_h, \text{Encap}_h, \text{Decap}_h)$ を構成する。このとき、セッション鍵 k を生成する際に、単純に k_{POSTQ} と k_{PREQ} とを連結した鍵 k_h をセッション鍵とするのではなく、短期公開鍵 $p k_h$ と暗号文 C_h とも連結した上で、鍵導出関数 KDF によりセッション鍵 $k = \text{KDF}(k_h || p k_h || C_h)$ を生成する。言い換えれば、鍵交換におけるセッションIDとして短期公開鍵 $p k_h$ と暗号文 C_h も含め、そのセッションIDで鍵導出関数によりセッション鍵 k を生成する。

[0031] これにより、例えば、耐量子 $\text{KEM}_{\text{POSTQ}}$ に対する突発的な攻撃による危険性を低減することができる。また、セッション鍵 k の生成の際に短期公開鍵

$p k_h$ と暗号文 C_h も鍵導出関数 $K D F$ に入力しているため、仮にセッション鍵 k が漏洩したとしても、他のセッションには影響がない。

[0032] <全体構成>

次に、上記のハイブリッド $K E M_h$ により鍵交換を実現する鍵交換システム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、本実施形態に係る鍵交換システム1の全体構成の一例を示す図である。

[0033] 図1に示すように、本実施形態に係る鍵交換システム1には、機器10と、機器20とが含まれる。また、機器10と機器20は、例えば、インターネット等の通信ネットワークNを介して通信可能に接続される。

[0034] 機器10は、 $K e y G e n_h$ アルゴリズムと $D e c a p_h$ アルゴリズムとを実行する機器である。一方で、機器20は、 $E n c a p_h$ アルゴリズムを実行する機器である。なお、機器10及び20としては、例えば、汎用サーバ、P C（パーソナルコンピュータ）、スマートフォン、タブレット端末、ウェアラブルデバイス、車載器、産業用機器、家電製品、ロボット等といった各種装置や機器等が挙げられる。

[0035] ここで、機器10は、鍵生成部101と、復号部102と、記憶部103とを有する。なお、鍵生成部101及び復号部102は、例えば、機器10にインストールされた1以上のプログラムが、C P U（Central Processing Unit）等のプロセッサに実行させる処理により実現される。また、記憶部103は、例えば、H D D（Hard Disk Drive）やS S D（Solid State Drive）、フラッシュメモリ等の各種メモリ装置により実現される。

[0036] 鍵生成部101は、 $K e y G e n_h$ アルゴリズムを実行し、短期秘密鍵 $s k_h$ と短期公開鍵 $p k_h$ を生成する。また、鍵生成部101は、短期公開鍵 $p k_h$ を機器20に送信する。

[0037] 復号部102は、機器20から暗号文 C_h を受信すると、 $D e c a p_h$ アルゴリズムを実行し、セッション鍵 k を生成する。

[0038] 記憶部103は、 $K e y G e n_h$ アルゴリズムや $D e c a p_h$ アルゴリズムの実行に用いられる各種情報、それらのアルゴリズムの出力等を記憶する。

[0039] また、機器 20 は、暗号化部 201 と、記憶部 202 とを有する。なお、暗号化部 201 は、例えば、機器 20 にインストールされた 1 以上のプログラムが、CPU 等のプロセッサに実行させる処理により実現される。また、記憶部 202 は、例えば、HDD や SSD、フラッシュメモリ等の各種メモリ装置により実現される。

[0040] 暗号化部 201 は、 $Encap_h$ アルゴリズムを実行し、暗号文 C_h とセッション鍵 k を生成する。また、暗号化部 201 は、暗号文 C_h を機器 10 に送信する。

[0041] 記憶部 202 は、 $Encap_h$ アルゴリズムに用いられる各種情報、このアルゴリズムの出力等を記憶する。

[0042] <鍵交換処理>

次に、本実施形態に係る鍵交換処理について、図 2 を参照しながら説明する。図 2 は、本実施形態に係る鍵交換処理の一例を示すシーケンス図である。

[0043] まず、機器 10 の鍵生成部 101 は、 $KeyGen_h()$ により短期秘密鍵 $s k_h$ と短期公開鍵 $p k_h$ を生成する（ステップ S101）。なお、短期秘密鍵 $s k_h$ 及び短期公開鍵 $p k_h$ は記憶部 103 に格納される。

[0044] 次に、機器 10 の鍵生成部 101 は、上記のステップ S101 で生成した短期公開鍵 $p k_h$ を機器 20 に送信する（ステップ S102）。

[0045] 機器 20 の暗号化部 201 は、短期公開鍵 $p k_h$ を受信すると、 $Encap_h(p k_h)$ によりセッション鍵 k と暗号文 C_h を生成する（ステップ S103）。

[0046] ここで、 $p k_h = p k_{POSTQ} || p k_{PREQ}$ であるため、暗号化部 201 は、 $p k_h$ を $p k_{POSTQ}$ と $p k_{PREQ}$ に分割した上で、 $Encap_{POSTQ}(p k_{POSTQ}) \rightarrow (k_{POSTQ}, C_{POSTQ})$ と $Encap_{PREQ}(p k_{PREQ}) \rightarrow (k_{PREQ}, C_{PREQ})$ とを実行し、以下によりセッション鍵 k を生成する。

[0047] $C_h = C_{POSTQ} || C_{PREQ}$
 $k_h = k_{POSTQ} || k_{PREQ}$

$$k = \text{KDF} (k_h || p k_h || C_h)$$

なお、セッション鍵 k は記憶部 202 に格納される。

[0048] 次に、機器 20 の暗号化部 201 は、上記のステップ S103 で生成した暗号文 C_h を機器 10 に送信する（ステップ S104）。

[0049] 機器 10 の復号部 102 は、暗号文 C_h を受信すると、 $\text{Decap}_h (s k_h, C_h)$ によりセッション鍵 k を生成する（ステップ S105）。

[0050] ここで、 $C_h = C_{\text{POSTQ}} || C_{\text{PREQ}}$ 及び $s k_h = s k_{\text{POSTQ}} || s k_{\text{PREQ}}$ であるため、復号部 102 は、 C_h を C_{POSTQ} と C_{PREQ} に分割すると共に $s k_h$ を $s k_{\text{POSTQ}}$ と $s k_{\text{PREQ}}$ に分割した上で、 $\text{Decap} (s k_{\text{POSTQ}}, C_{\text{POSTQ}}) \rightarrow k_{\text{POSTQ}} / \text{error}$ と $\text{Decap} (s k_{\text{PREQ}}, C_{\text{PREQ}}) \rightarrow k_{\text{PREQ}} / \text{error}$ とを実行する。そして、 k_{POSTQ} と k_{PREQ} が得られた場合は、復号部 102 は、以下によりセッション鍵 k を生成する。

$$k_h = k_{\text{POSTQ}} || k_{\text{PREQ}}$$

$$k = \text{KDF} (k_h || p k_h || C_h)$$

なお、セッション鍵 k は記憶部 103 に格納される。

[0052] 以上により、機器 10 と機器 20 との間でセッション鍵 k が共有され、鍵交換処理が終了する。したがって、これ以降、機器 10 及び 20 は、当該セッション鍵 k を用いて暗号化通信を実現することができる。

[0053] <応用例>

以下、本実施形態で説明したハイブリッド KEM_n の応用例として、耐量子 DMKD のハイブリッド化について説明する。

[0054] 多者間鍵交換技術には、メッシュ型の鍵交換である GKE (Group Key Exchange) とスター型の鍵交換である MKD (Multi Key Distribution) とがある。これらの鍵交換は参加人数に比例して通信コストがあがる、サーバに共有鍵を伝達してしまう等といった課題がある。これらの課題を解決したのが DMKD (Multi-Cast Key Distribution: Scalable, Dynamic and Provably Secure Construction) と呼ばれる鍵交換技術（例えば、以下の参考文献 3 を参照されたい。）である。DMKD では、参加人数に依らず定数 R_{oun}

dで鍵交換を行うことができると共に、サーバに対して共有鍵を秘匿できる。また、DMKDの鍵交換の部分に耐量子方式を適用可能としたDMKDプロトコルの構成法が提案されている（例えば、以下の参考文献4を参照されたい。）。

[0055] 参考文献3：Kazuki Yoneyama, Reo Yoshida, Yuto Kawahara, Tetsutaro Kobayashi, Hitoshi Fuji, Tomohide Yamamoto, Multi-Cast Key Distribution : Scalable, Dynamic and Provably Secure Construction, ProvSec(2016)

参考文献4：金城皓羽，岡野裕樹，齋藤恆和，草川恵太，小林鉄太郎，星野文学，KEMを用いた動的多者鍵配布プロトコル，暗号と情報セキュリティシンポジウム(2018)

耐量子方式が適用可能なDMKDプロトコルは、(Setup, Dist, Join, Leave, Update)の5つのアルゴリズムで構成される。また、これらのアルゴリズムは、属性ベース暗号、公開鍵暗号、鍵カプセル化技術、コミットメント、メッセージ認証の各アルゴリズムを利用する。

[0056] 本応用例では、耐量子DMKDをハイブリッド化するために、公開鍵系である属性ベース暗号、公開鍵暗号、鍵カプセル化技術、及びコミットメントに対してハイブリッド方式を用いる。このとき、鍵カプセル化技術のハイブリッド化には、本実施形態で説明したハイブリッドKEM_hを用いる。一方で、鍵カプセル化技術以外については、単純な連結でハイブリッド化を実現できる。つまり、鍵カプセル化技術以外の技術（属性ベース暗号、公開鍵暗号、及びコミットメント）のハイブリッド方式の任意のアルゴリズムを $A \mid g_h$ 、耐量子暗号方式の当該アルゴリズムを $A \mid g_{POSTQ}$ 、古典的な暗号方式の当該アルゴリズムを $A \mid g_{PREQ}$ とすれば、 $A \mid g_h = A \mid g_{POSTQ} \parallel A \mid g_{PREQ}$ とすればよい。このとき、鍵や各種情報等も単純に連結すればよい。

[0057] なお、属性ベース暗号の具体例としては、例えば、古典的な暗号方式にはインテリ暗号等があり、耐量子暗号方式には格子ベースの属性ベース暗号等がある。インテリ暗号については以下の参考文献5、格子ベースの属性ベー

ス暗号については以下の参考文献6等をそれぞれ参照されたい。

[0058] 参考文献5 : Okamoto, Tatsuaki, and Katsuyuki Takashima. "Fully secure functional encryption with general relations from the decisional linear assumption." Annual cryptology conference. Springer, Berlin, Heidelberg, 2010.

参考文献6 : Yongtao Wang, Lattice Ciphertext Policy Attribute-based Encryption in the Standard Model, International Journal of Network Security, Vol.16, No.6, PP.444-451, Nov. 2014.

公開鍵暗号及び鍵カプセル化技術の具体例としては、例えば、古典的な暗号方式にはPSECKEM等があり、耐量子暗号方式にはNISTの耐量子コンテストで提案されている技術等がある。

[0059] コミットメントの具体例としては、例えば、古典的な暗号方式にはECDSAやEdDSA等があり、耐量子暗号方式にはNISTの耐量子コンテストで提案されている技術等がある。

[0060] ただし、上記の具体例は一例であって、これらの具体例に限定されるものはない。

[0061] <ハードウェア構成>

最後に、本実施形態に係る機器10及び20のハードウェア構成について、図3を参照しながら説明する。図3は、本実施形態に係る機器10及び20のハードウェア構成の一例を示す図である。なお、機器10及び20は同様のハードウェア構成で実現可能なため、以下では、機器10のハードウェア構成について説明する。

[0062] 図3に示すように、本実施形態に係る機器10は、入力装置301と、表示装置302と、外部I/F303と、通信I/F304と、プロセッサ305と、メモリ装置306とを有する。これらの各ハードウェアは、それぞれがバス307により通信可能に接続される。

[0063] 入力装置301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302は、例えば、ディスプレイ等である。なお、機器10は、

例えば、入力装置 301 及び表示装置 302 のうちの少なくとも一方を有していなくてもよい。

[0064] 外部 I/F 303 は、記録媒体 303a 等の外部装置とのインタフェースである。機器 10 は、外部 I/F 303 を介して、記録媒体 303a の読み取りや書き込み等を行うことができる。なお、記録媒体 303a 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。

[0065] 通信 I/F 304 は、機器 10 を通信ネットワーク N に接続するためのインタフェースである。プロセッサ 305 は、例えば、CPU 等の各種演算装置である。メモリ装置 306 は、例えば、HDD や SSD、フラッシュメモリ、RAM (Random Access Memory)、ROM (Read Only Memory) 等の各種記憶装置である。

[0066] 本実施形態に係る機器 10 及び 20 は、図 3 に示すハードウェア構成を有することにより、上述した鍵交換処理を実現することができる。なお、図 3 に示すハードウェア構成は一例であって、機器 10 及び 20 は、例えば、複数のプロセッサを有していたり、複数のメモリ装置を有していたりしてもよく、様々なハードウェア構成を有していてもよい。

[0067] 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

[0068]

1	鍵交換システム
10	機器
20	機器
101	鍵生成部
102	復号部
103	記憶部

2 0 1	暗号化部
2 0 2	記憶部
3 0 1	入力装置
3 0 2	表示装置
3 0 3	外部 I / F
3 0 3 a	記録媒体
3 0 4	通信 I / F
3 0 5	プロセッサ
3 0 6	メモリ装置
3 0 7	バス

請求の範囲

[請求項1] 耐量子性を持つ第1の鍵カプセル化メカニズムの第1の短期秘密鍵及び第1の短期公開鍵と、前記第1の鍵カプセル化メカニズムに対して古典的な第2の鍵カプセル化メカニズムの第2の短期秘密鍵及び第2の短期公開鍵とを生成し、前記第1の短期秘密鍵と前記第2の短期秘密鍵とを連結した第3の短期秘密鍵と、前記第1の短期公開鍵と前記第2の短期公開鍵とを連結した第3の短期公開鍵とを生成する鍵生成部と、

前記第3の短期公開鍵を用いて、前記第1の鍵カプセル化メカニズムの第1の暗号文及び第1の共有鍵と、前記第2の鍵カプセル化メカニズムの第2の暗号文及び第2の共有鍵とを生成し、前記第1の共有鍵と前記第2の共有鍵と前記第3の短期公開鍵と前記第1の暗号文と前記第2の暗号文を入力とする鍵生成関数により第3の共有鍵を生成する暗号化部と、

前記第3の短期秘密鍵を用いて、前記第1の暗号文と前記第2の暗号文とをそれぞれ復号して前記第1の共有鍵と前記第2の共有鍵とを生成し、前記第1の共有鍵と前記第2の共有鍵と前記第3の短期公開鍵と前記第1の暗号文と前記第2の暗号文を入力とする前記鍵生成関数により前記第3の共有鍵を生成する復号部と、

を有する鍵交換システム。

[請求項2] 前記暗号化部は、

前記第1の共有鍵と前記第2の共有鍵と前記第3の短期公開鍵と前記第1の暗号文と前記第2の暗号文とを連結した値を前記鍵生成関数に入力することで、前記第3の共有鍵を生成し、

前記復号部は、

前記第1の共有鍵と前記第2の共有鍵と前記第3の短期公開鍵と前記第1の暗号文と前記第2の暗号文とを連結した値を前記鍵生成関数に入力することで、前記第3の共有鍵を生成する、請求項1に記載の

鍵交換システム。

[請求項3] 耐量子性を持つ第1の鍵カプセル化メカニズムの第1の短期秘密鍵及び第1の短期公開鍵と、前記第1の鍵カプセル化メカニズムに対して古典的な第2の鍵カプセル化メカニズムの第2の短期秘密鍵及び第2の短期公開鍵とを生成し、前記第1の短期秘密鍵と前記第2の短期秘密鍵とを連結した第3の短期秘密鍵と、前記第1の短期公開鍵と前記第2の短期公開鍵とを連結した第3の短期公開鍵とを生成する鍵生成部と、

通信ネットワークを介して接続される他の機器に対して、前記第3の短期公開鍵を送信する送信部と、

前記第3の短期秘密鍵を用いて、前記他の機器から受信した暗号文を復号して前記第1の鍵カプセル化メカニズムの第1の共有鍵と前記第2の鍵カプセル化メカニズムの第2の共有鍵とを生成し、前記第1の共有鍵と前記第2の共有鍵と前記第3の短期公開鍵と前記暗号文を入力とする鍵生成関数により、前記他の機器との間で共有される第3の共有鍵を生成する復号部と、

を有する機器。

[請求項4] 通信ネットワークを介して接続される他の機器から受信した短期公開鍵を用いて、耐量子性を持つ第1の鍵カプセル化メカニズムの第1の暗号文及び第1の共有鍵と、前記第1の鍵カプセル化メカニズムに対して古典的な第2の鍵カプセル化メカニズムの第2の暗号文及び第2の共有鍵とを生成し、前記第1の共有鍵と前記第2の共有鍵と前記短期公開鍵と前記第1の暗号文と前記第2の暗号文を入力とする鍵生成関数により、前記他の機器との間で共有される第3の共有鍵を生成する暗号化部、

を有する機器。

[請求項5] 耐量子性を持つ第1の鍵カプセル化メカニズムの第1の短期秘密鍵及び第1の短期公開鍵と、前記第1の鍵カプセル化メカニズムに対し

て古典的な第2の鍵カプセル化メカニズムの第2の短期秘密鍵及び第2の短期公開鍵とを生成し、前記第1の短期秘密鍵と前記第2の短期秘密鍵とを連結した第3の短期秘密鍵と、前記第1の短期公開鍵と前記第2の短期公開鍵とを連結した第3の短期公開鍵とを生成する鍵生成手順と、

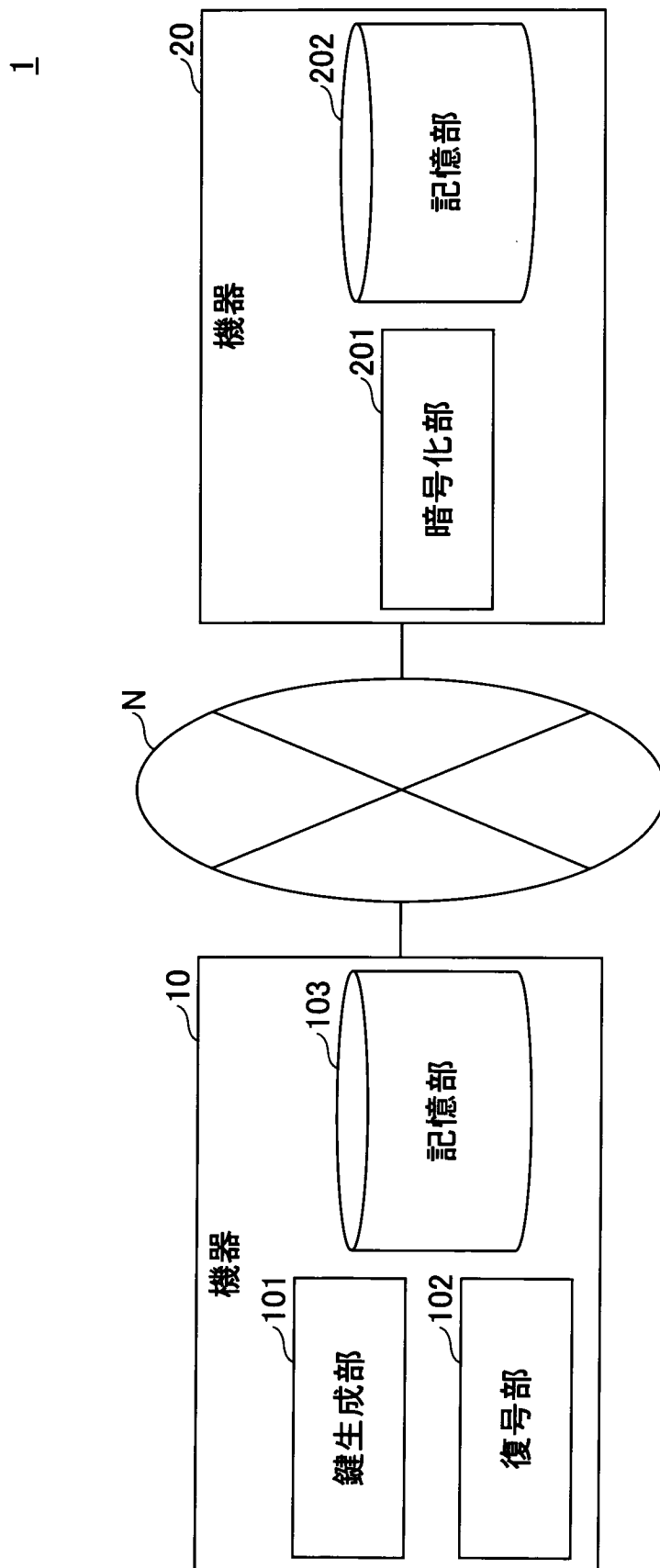
前記第3の短期公開鍵を用いて、前記第1の鍵カプセル化メカニズムの第1の暗号文及び第1の共有鍵と、前記第2の鍵カプセル化メカニズムの第2の暗号文及び第2の共有鍵とを生成し、前記第1の共有鍵と前記第2の共有鍵と前記第3の短期公開鍵と前記第1の暗号文と前記第2の暗号文を入力とする鍵生成関数により第3の共有鍵を生成する暗号化手順と、

前記第3の短期秘密鍵を用いて、前記第1の暗号文と前記第2の暗号文とをそれぞれ復号して前記第1の共有鍵と前記第2の共有鍵とを生成し、前記第1の共有鍵と前記第2の共有鍵と前記第3の短期公開鍵と前記第1の暗号文と前記第2の暗号文を入力とする前記鍵生成関数により前記第3の共有鍵を生成する復号手順と、

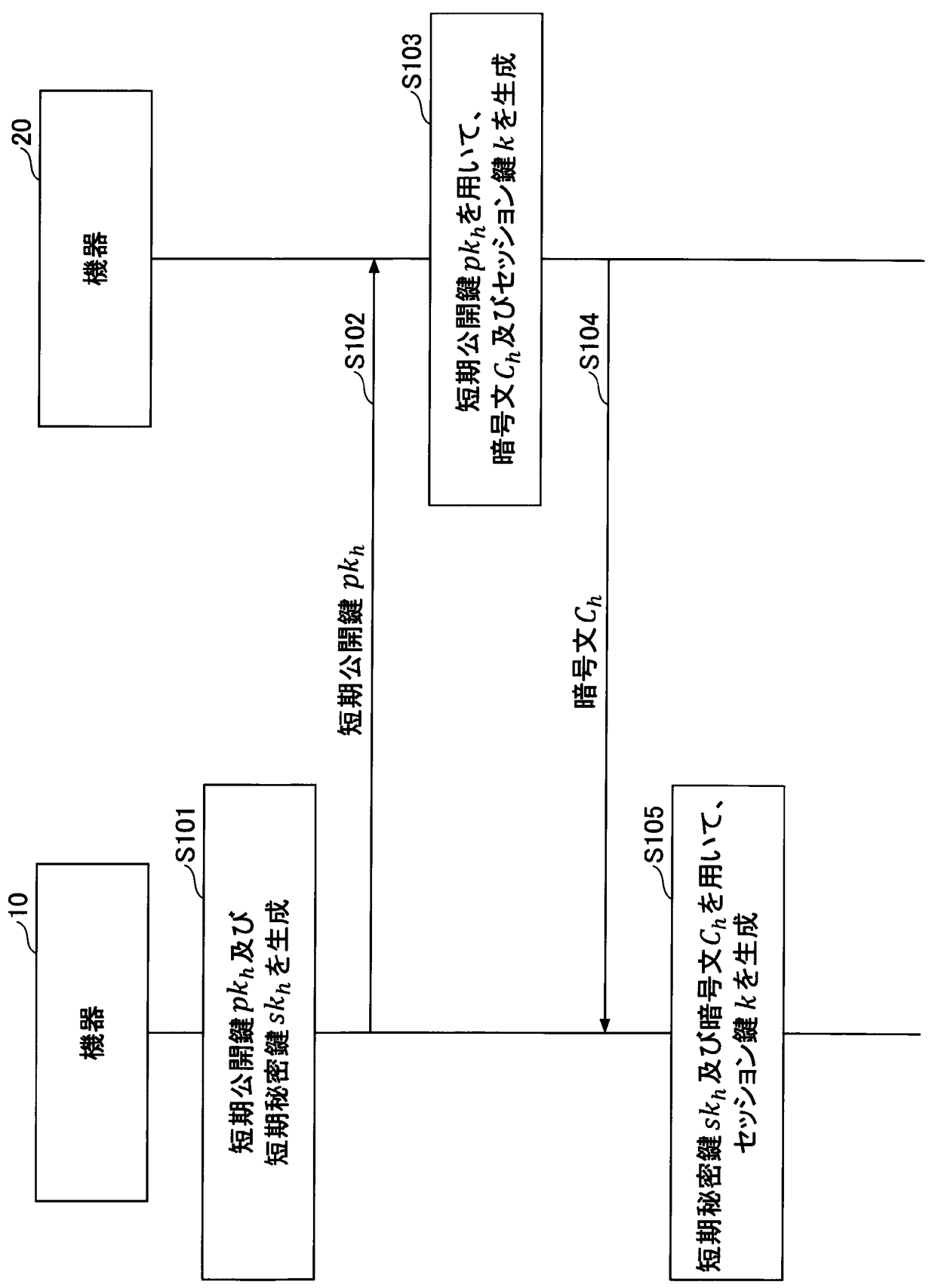
をコンピュータが実行する鍵交換方法。

[請求項6] コンピュータを、請求項1又は2に記載の鍵交換システムとして機能させるプログラム。

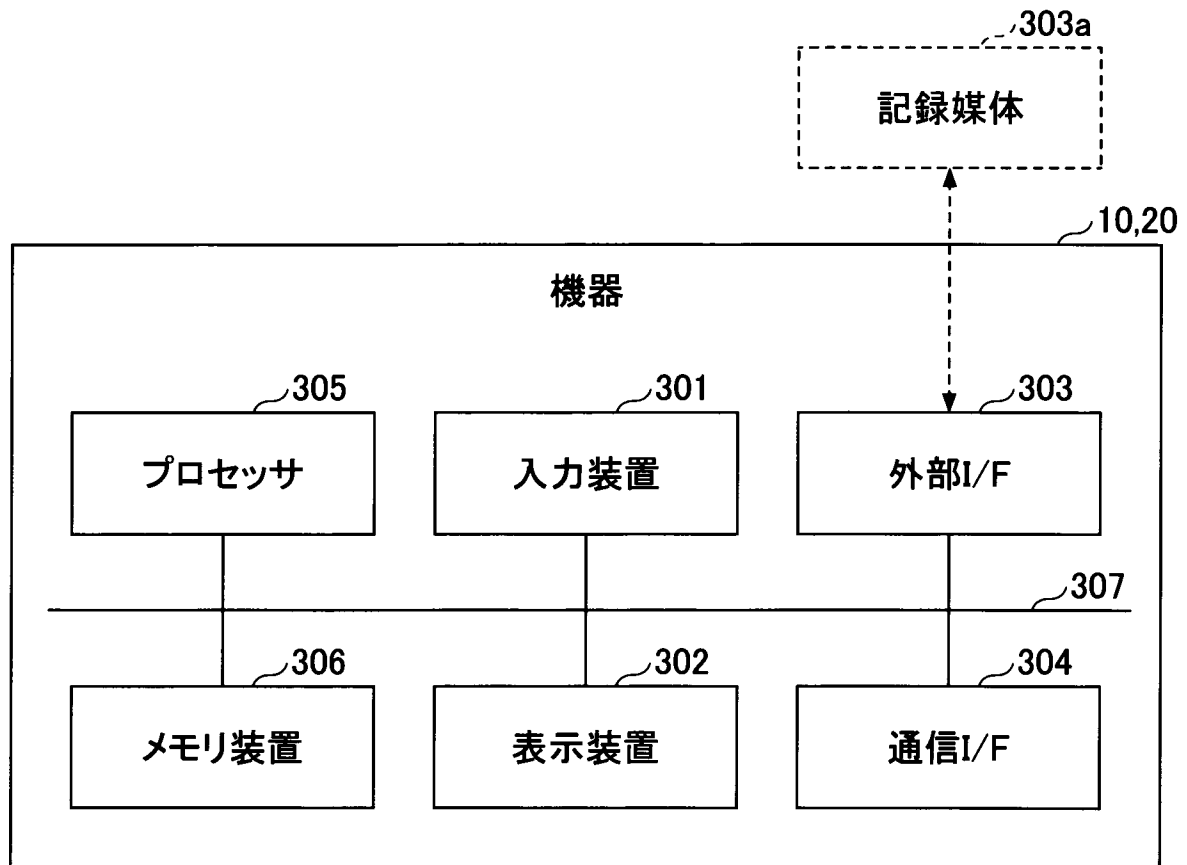
[図1]



[図2]



[図3]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2021/017943

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i

FI: H04L9/00 601C

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)

H0419/08

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)

JSTPlus/JMEDPlus/JST7580 (JDreamIII); IEEE Xplore key exchange, post-quantum cryptography

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	STEBILA, D. FLUHRER, S. GUERON, S. Hybrid key exchange in TLS 1.3, draft-ietf-tls-hybrid-design-02. [online], 14 April 2021, pp. 1-34, < https://datatracker.ietf.org/doc/draft-stebila-tls-hybrid-design/02/ >, in particular, 1. Introduction, 2. Key encapsulation mechanisms, 3. Construction for hybrid key exchange	1-6
Y	株式会社レビダム, ハイブリッドモードの技術動向調査, [online], December 2020, pp. 1-30, < URL:https://www.cryptrec.go.jp/ex_reports.html >, in particular, 3.2 The specific configuration example of hybrid mode: Hybrid key exchange, (LEPIDUM CO. LTD. Survey of technology trends in Hybrid Mode for Post-Quantum Cryptography.)	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

15 July 2021 (15.07.2021)

Date of mailing of the international search report

03 August 2021 (03.08.2021)

Name and mailing address of the ISA/

Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2021/017943

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CAMPAGNA, M. Hybrid-Key Exchanges as an Interim-to-Permanent Solution to Cryptographic Agility. [online], 21 June 2019, pp. 1-28, <URL:https://docbox.etsi.org/Workshop/2019/201906_ETSISECURITYWEEK/202106_DynamicNatureOfTechno/SESSION03_CHANGINGCRYPTOGRAPHY/AWS_CAMPAGNA.pdf>, in particular, Quantum-safe cryptography -recap, Hybrid key agreements, PQ-TLS 1.2-hybrid key exchange	1-6
Y	FUJIOKA, A. SUZUKI, K. XAGAWA, K. YONEYAMA, K. Strongly Secure Authenticated Key Exchange from Factoring, Codes, and Lattices. Lecture Notes in Computer Science., vol. 7293, 2012, pp. 467-484, in particular, pp. 477, 478, Generic Construction GC	1-6
A	GIACON, F. HEUER, F. POETTERING, B. KEM Combiners. Cryptology ePrint Archive, Report 2018/024. [online], 07 January 2018, pp1-29, <URL:https://eprint.iacr.org/2018/024>, in particular, 1 Introduction, 2 Preliminaries, 3 KEM combiners	1-6

A. 発明の属する分野の分類（国際特許分類（IPC）） H04L 9/08(2006.01)i FI: H04L9/00 601C														
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）） H04L9/08 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 <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922-1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971-2021年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996-2021年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994-2021年</td> </tr> </table> 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） JSTPlus/JMEDPlus/JST7580 (JDreamIII); IEEE Xplore key exchange, post-quantum cryptography			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				
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													
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												
Y	STEBILA, D., FLUHRER, S. and GUERON, S., Hybrid key exchange in TLS 1.3, draft-ietf-tls-hybrid-design-02, [online], 2021.04.14, pp.1-34, <https://datatracker.ietf.org/doc/draft-stebila-tls-hybrid-design/02/> 特に 1. Introduction, 2. Key encapsulation mechanisms, 3. Construction for hybrid key exchange	1-6												
Y	株式会社レビダム, ハイブリッドモードの技術動向調査, [online], 2020.12, pp.1-30, <URL:https://www.cryptrec.go.jp/ex_reports.html> 特に 3.2 具体的なハイブリッドモード構成例：ハイブリッド鍵交換	1-6												
Y	CAMPAGNA, M, Hybrid-Key Exchanges as an Interim-to-Permanent Solution to Cryptographic Agility, [online], 2019.06.21, pp.1-28, <URL:https://docbox.etsi.org/Workshop/2019/201906_ETSISECURITYWEEK/202106_DynamicNatureOfTechno/SESSION03_CHANGINGCRYPTOGRAPHY/AWS_CAMPAGNA.pdf> 特に Quantum-safe cryptography -recap, Hybrid key agreements, PQ-TLS 1.2-hybrid key exchange	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。														
<table border="0"> <tr> <td>* 引用文献のカテゴリー</td> <td>"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</td> </tr> <tr> <td>"A" 特に関連のある文献ではなく、一般的な技術水準を示すもの</td> <td>"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</td> </tr> <tr> <td>"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</td> <td>"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</td> </tr> <tr> <td>"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）</td> <td>"&" 同一パテントファミリー文献</td> </tr> <tr> <td>"O" 口頭による開示、使用、展示等に言及する文献</td> <td></td> </tr> <tr> <td>"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</td> <td></td> </tr> </table>			* 引用文献のカテゴリー	"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	"A" 特に関連のある文献ではなく、一般的な技術水準を示すもの	"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	"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	"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	"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）	"&" 同一パテントファミリー文献	"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	
* 引用文献のカテゴリー	"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													
"A" 特に関連のある文献ではなく、一般的な技術水準を示すもの	"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													
"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	"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													
"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）	"&" 同一パテントファミリー文献													
"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														
国際調査を完了した日 15.07.2021		国際調査報告の発送日 03.08.2021												
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） 中里 裕正 5S 9364 電話番号 03-3581-1101 内線 3546												

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
Y	FUJIOKA, A., SUZUKI, K. XAGAWA, K. and YONEYAMA, K., Strongly Secure Authenticated Key Exchange from Factoring, Codes, and Lattices, Lecture Notes in Computer Science, Vol.7293, 2012, pp.467-484 特に pp.477,478 Generic Construction GC	1-6
A	GIACON, F., HEUER, F. and POETTERING, B., KEM Combiners, Cryptology ePrint Archive, Report 2018/024, [online], 2018.01.07, ppl-29, <URL:https://eprint.iacr.org/2018/024> 特に 1 Introduction, 2 Preliminaries, 3 KEM combiners	1-6