

(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  
2024年9月6日(06.09.2024)



(10) 国際公開番号

WO 2024/181563 A1

- (51) 国際特許分類:  
H04L 9/22 (2006.01) G09C 1/00 (2006.01)
- (21) 国際出願番号: PCT/JP2024/007800
- (22) 国際出願日: 2024年3月1日(01.03.2024)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:  
特願 2023-031548 2023年3月2日(02.03.2023) JP
- (71) 出願人: K D D I 株式会社 (KDDI CORPORATION) [JP/JP]; 〒1638003 東京都新宿区西新宿二丁目3番2号 Tokyo (JP).
- (72) 発明者: 仲野 有登 (NAKANO Yuto); 〒3568502 埼玉県ふじみ野市大原2丁目1番15号 株式会社 K D D I 総合研究所内 Saitama (JP). 福島 和英 (FUKUSHIMA Kazuhide); 〒3568502 埼玉県ふじみ野市大原2丁目1番15号 株式会社 K D D I 総合研究所内 Saitama (JP). 清

本 晋作 (KIYOMOTO Shinsaku); 〒3568502 埼玉県ふじみ野市大原2丁目1番15号 株式会社 K D D I 総合研究所内 Saitama (JP).

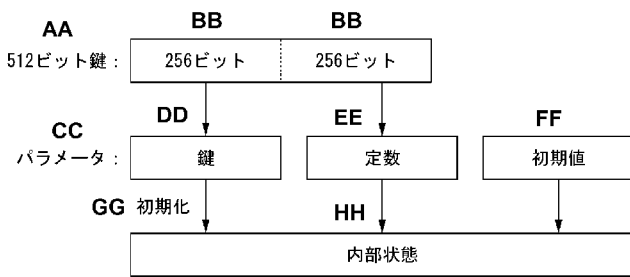
(74) 代理人: 田 ▲ 崎 ▼ 聡, 外 (TAZAKI Akira et al.); 〒1006620 東京都千代田区丸の内一丁目9番2号 Tokyo (JP).

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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.

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

(54) 発明の名称: 暗号化装置、復号装置、暗号化方法及び暗号化プログラム

【図2】



AA 512-bit key  
BB 256 bits  
CC Parameter  
DD Key  
EE Constant  
FF Initial value  
GG Initialization  
HH Internal state

(57) Abstract: This encryption device comprises: a parameter setting unit that receives an input of a key longer than a prescribed key length for use in a prescribed stream encryption system, divides a part exceeding the prescribed key length, and allocates the part as a constant which is an input parameter of the stream encryption system; an initialization processing unit that initializes the stream encryption system on the basis of the input parameter allocated by the parameter setting unit; and an encryption execution unit that executes encryption in accordance with the stream encryption system.

(57) 要約: 暗号化装置は、所定のストリーム暗号方式で用いる規定の鍵長よりも長い鍵の入力を受け付け、当該規定の鍵長を超える部分を分割し、当該ストリーム暗号方式の入力パラメータである定数として割り当てるパラメータ設定部と、パラメータ設定部により割り当てられた入力パラメータにより、ストリーム暗号方式の初期化を行う初期化処理部と、ストリーム暗号方式に従って暗号化を実行する暗号化実行部と、を備える。

[続葉有]

(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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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:

— 国際調査報告 (条約第21条(3))

## 明 細 書

発明の名称：

暗号化装置、復号装置、暗号化方法及び暗号化プログラム

### 技術分野

[0001] 本開示は、暗号方式の安全性向上のための技術に関する。

本願は、2023年3月2日に、日本に出願された特願2023-031548号に基づき優先権を主張し、その内容をここに援用する。

### 背景技術

[0002] 従来、128ビットの鍵を用いた共通鍵暗号方式が広く利用されているが、古典計算機に比べて効率的な計算アルゴリズムを実行できる量子計算機に対しては、 $\sqrt{(2^{128})}$ 程度の試行回数で解読され得る64ビット安全しか確保することができず、大規模量子計算機によって解読される可能性が指摘されている。

そこで、量子計算機に対しても128ビット安全を確保するため、256ビットの鍵長に対応した暗号化方式が提案されている（例えば、非特許文献1～3参照）。

### 先行技術文献

#### 非特許文献

- [0003] 非特許文献1：Hongjun Wu and Bart Preneel, AEGIS: A Fast Authenticated Encryption Algorithm, Selected Areas in Cryptography -- SAC 2013.
- 非特許文献2：Daniel J. Bernstein. ChaCha, a variant of Salsa20. In Workshop Record of SASC, volume 8, 2008.
- 非特許文献3：K. Sakamoto, F. Liu, Y. Nakano, S. Kiyomoto and T. Isobe. Rocca: An Efficient AES-based Encryption Scheme for Beyond 5G. IACR Transactions on Symmetric Cryptology, 2021(2), 1-30.

### 発明の概要

#### 発明が解決しようとする課題

[0004] 256ビットの鍵を用いることで、量子計算機に対しても128ビット安全を確保できるが、さらに高い安全性を実現するため、より長い鍵長をサポートする暗号方式が望まれている。

[0005] 本開示は、既存の暗号方式において、規定の鍵長よりも長い鍵に対応できる暗号化装置、復号装置、暗号化方法及び暗号化プログラムを提供することを目的の一例とする。

### 課題を解決するための手段

[0006] 本開示に係る暗号化装置は、所定のストリーム暗号方式で用いる規定の鍵長よりも長い鍵の入力を受け付け、当該規定の鍵長を超える部分を分割し、当該ストリーム暗号方式の入力パラメータである定数として割り当てるパラメータ設定部と、前記パラメータ設定部により割り当てられた前記入力パラメータにより、前記ストリーム暗号方式の初期化を行う初期化処理部と、前記ストリーム暗号方式に従って暗号化を実行する暗号化実行部と、を備える。

[0007] 前記定数は、前記ストリーム暗号方式の内部状態の一部として初期化される値であってもよい。

[0008] 前記ストリーム暗号方式は、Rocca又はRocca-Sであり、前記パラメータ設定部は、2つの128ビットの定数それぞれに対して、512ビットの鍵の一部を割り当ててもよい。

[0009] 本開示に係る復号装置は、所定のストリーム暗号方式で用いる規定の鍵長よりも長い鍵の入力を受け付け、当該規定の鍵長を超える部分を分割し、当該ストリーム暗号方式の入力パラメータである定数として割り当てるパラメータ設定部と、前記パラメータ設定部により割り当てられた前記入力パラメータにより、前記ストリーム暗号方式の初期化を行う初期化処理部と、請求項1から請求項3のいずれかに記載の暗号化装置により出力された暗号文を、前記ストリーム暗号方式に従って復号する復号実行部と、を備える。

[0010] 本開示に係る暗号化方法は、所定のストリーム暗号方式で用いる規定の鍵長よりも長い鍵の入力を受け付け、当該規定の鍵長を超える部分を分割し、

当該ストリーム暗号方式の入力パラメータである定数として割り当てるパラメータ設定ステップと、前記パラメータ設定ステップにおいて割り当てられた前記入力パラメータにより、前記ストリーム暗号方式の初期化を行う初期化処理ステップと、前記ストリーム暗号方式に従って暗号化を実行する暗号化実行ステップと、をコンピュータが実行する。

[0011] 本開示に係る暗号化プログラムは、前記暗号化装置としてコンピュータを機能させるためのものである。

### 発明の効果

[0012] 本開示によれば、一例として、既存の暗号方式において、規定の鍵長よりも長い鍵に対応できる。

### 図面の簡単な説明

[0013] [図1]実施形態における暗号化装置の機能構成を示す図である。

[図2]実施形態におけるパラメータの設定方法を例示する図である。

[図3]実施形態における復号装置の機能構成を示す図である。

### 発明を実施するための形態

[0014] 以下、本開示の実施形態の一例について説明する。

本実施形態の暗号化方法は、既存のストリーム暗号を対象とした改良手法である。

ストリーム暗号を用いてデータを暗号化する場合、第1のステップとして初期化を実施する必要がある。初期化時に暗号化プログラムに入力する値として、鍵、初期値、定数の3つがある。

本実施形態では、この3つの値のうち、定数に対して、本来の値に代えて鍵の一部を入力することで、暗号方式が本来サポートする鍵長よりも長い鍵に対応する。

[0015] 図1は、本実施形態における暗号化装置1の機能構成を示す図である。

暗号化装置1は、制御部11及び記憶部12の他、各種の通信デバイス等を備えた情報処理装置（コンピュータ）であり、サーバ又はパーソナルコンピュータ等の汎用機器の他、携帯端末又はIoT（Internet of Things）機

器等の小型ハードウェアであってもよい。

[0016] 制御部 11 は、暗号化装置 1 の全体を制御する部分であり、記憶部 12 に記憶された各種プログラムを適宜読み出して実行することにより、本実施形態における各機能を実現する。制御部は、CPU (Central Processing Unit) であってよい。

記憶部 12 は、ハードウェア群を暗号化装置 1 として機能させるための各種プログラム、及び各種データ等の記憶領域であり、ROM (Read Only Memory)、RAM (Random Access Memory)、フラッシュメモリ又はハードディスクドライブ (HDD : Hard Disk Drive) 等であってよい。

[0017] なお、暗号化装置 1 は、記憶部 12 に格納された暗号化プログラムを制御部 11 が実行する構成であってもよいが、制御部 11 及び記憶部 12 は、暗号化装置 1 に専用のハードウェア回路として実装されてもよい。

[0018] 制御部 11 は、パラメータ設定部 111 と、初期化処理部 112 と、暗号化実行部 113 とを備える。

[0019] パラメータ設定部 111 は、所定のストリーム暗号方式で用いる規定の鍵長よりも長い鍵の入力を受け付けると、この規定の鍵長を超える部分を分割し、ストリーム暗号方式の入力パラメータである定数として割り当てる。

この定数は、ストリーム暗号方式の内部状態の一部として初期化される値である。

[0020] 図 2 は、本実施形態におけるパラメータの設定方法を例示する図である。

この例では、規定の鍵長が 256 ビット、定数が 256 ビットの暗号化方式の場合を説明している。

[0021] 内部状態を初期化する際の入力パラメータは、鍵、初期値、定数の 3 つであるが、鍵として設定できるのは 256 ビットである。この暗号化方式を 512 ビットの鍵に対応させるため、パラメータ設定部 111 は、512 ビットの鍵のうち、256 ビットを分割し、定数として設定する。

なお、初期値は、初期化処理の度に異なる値が設定される。

[0022] このように設定された鍵及び定数は、暗号化側（暗号化装置 1）と復号側

（復号装置２）とで共通の値であり、この結果、暗号方式（アルゴリズム）を改変することなく、暗号化及び復号が可能となる。

[0023] 初期化処理部１１２は、パラメータ設定部１１１により割り当てられた入力パラメータにより、ストリーム暗号方式の初期化を行う。

暗号化実行部１１３は、対象のストリーム暗号方式のアルゴリズムに従って暗号化を実行する。

[0024] 図３は、本実施形態における復号装置２の機能構成を示す図である。

復号装置２は、暗号化装置１により暗号化されたデータを、対応する復号アルゴリズムにより復号する装置である。

復号装置２は、暗号化装置１と同様に、制御部２１及び記憶部２２の他、各種の通信デバイス等を備えた情報処理装置（コンピュータ）であり、サーバ又はパーソナルコンピュータ等の汎用機器の他、携帯端末又はＩｏＴ機器等の小型ハードウェアであってもよい。

[0025] 制御部２１は、復号装置２の全体を制御する部分であり、記憶部２２に記憶された各種プログラムを適宜読み出して実行することにより、本実施形態における各機能を実現する。制御部は、ＣＰＵであってよい。

記憶部２２は、ハードウェア群を復号装置２として機能させるための各種プログラム、及び各種データ等の記憶領域であり、ＲＯＭ、ＲＡＭ、フラッシュメモリ又はハードディスクドライブ（ＨＤＤ）等であってよい。

[0026] なお、復号装置２は、記憶部２２に格納された復号プログラムを制御部２１が実行する構成であってもよいが、制御部２１及び記憶部２２は、復号装置２に専用のハードウェア回路として実装されてもよい。

[0027] 制御部２１は、パラメータ設定部２１１と、初期化処理部２１２と、復号実行部２１３とを備える。

[0028] パラメータ設定部２１１及び初期化処理部２１２は、それぞれ暗号化装置１のパラメータ設定部１１１及び初期化処理部１１２と同一の機能を実行する。

すなわち、前述の通り、鍵及び定数は、暗号化側（暗号化装置１）と復号

側（復号装置 2）とで共有されて初期化が実行されることにより、暗号方式（アルゴリズム）を改変することなく、暗号化及び復号が可能となる。

[0029] 復号実行部 213 は、暗号化装置 1 の暗号化実行部 113 に対応する機能部であり、対象のストリーム暗号方式のアルゴリズムに従って、暗号化装置 1 により暗号化されたデータの復号を実行する。

[0030] ここで、対象とするストリーム暗号方式を具体的に例示して、本実施形態により改良される初期化処理を説明する。

[0031] [A E G I S]

非特許文献 1 に示されている規定の鍵長が 256 ビットの暗号方式 A E G I S-256 の場合、初期化では、6 つの内部状態 S（それぞれ 128 ビット）に対して、鍵 K、初期値 I V、定数 c o n s t が次のように設定される。

$$S(-16, 0) = K(256, 0) + I V(256, 0);$$

$$S(-16, 1) = K(256, 1) + I V(256, 1);$$

$$S(-16, 2) = c o n s t 1;$$

$$S(-16, 3) = c o n s t 0;$$

$$S(-16, 4) = K(256, 0) + c o n s t 0;$$

$$S(-16, 5) = K(256, 1) + c o n s t 1$$

（ただし、+ はビット単位の排他的論理和）

[0032] K(256, 0) 及び K(256, 1) は、それぞれ 256 ビットの鍵 K の前半 128 ビット及び後半 128 ビットである。

C o n s t 1 及び c o n s t 0 は、それぞれ定数 c o n s t の前半 128 ビット及び後半 128 ビットである。

I V(256, 0) 及び I V(256, 1) は、それぞれ初期値 I V の前半 128 ビット及び後半 128 ビットである。

[0033] ここで、パラメータ設定部 111 は、512 ビットの鍵に対応するため、例えば、前半の 256 ビットを K(256, 0) 及び K(256, 1) に 128 ビットずつ割り当て、後半の 256 ビットを c o n s t 1 及び c o n s

t<sub>0</sub>に128ビットずつ割り当てる。

これにより、暗号化装置1は、256ビットの定数部分を鍵の一部として利用することで、256ビットを超える512ビットの鍵を用いたストリーム暗号を実現できる。

[0034] [ChaCha]

非特許文献2に示されている規定の鍵長が256ビットの暗号方式ChaChaの場合、内部状態として各要素がそれぞれ32ビットの次の行列が定義される。

|                 |                 |                 |                 |
|-----------------|-----------------|-----------------|-----------------|
| x <sub>0</sub>  | x <sub>1</sub>  | x <sub>2</sub>  | x <sub>3</sub>  |
| x <sub>4</sub>  | x <sub>5</sub>  | x <sub>6</sub>  | x <sub>7</sub>  |
| x <sub>8</sub>  | x <sub>9</sub>  | x <sub>10</sub> | x <sub>11</sub> |
| x <sub>12</sub> | x <sub>13</sub> | x <sub>14</sub> | x <sub>15</sub> |

[0035] 初期化では、各要素に対して、鍵key<sub>0</sub>～key<sub>7</sub>（合計256ビット）、初期値counter<sub>0</sub>及びnonce<sub>0</sub>～nonce<sub>2</sub>、並びに定数const<sub>1</sub>～const<sub>3</sub>（合計128ビット）が次のように設定される。

|                      |                    |                    |                    |
|----------------------|--------------------|--------------------|--------------------|
| const <sub>0</sub>   | const <sub>1</sub> | const <sub>2</sub> | const <sub>3</sub> |
| key <sub>0</sub>     | key <sub>1</sub>   | key <sub>2</sub>   | key <sub>3</sub>   |
| key <sub>4</sub>     | key <sub>5</sub>   | key <sub>6</sub>   | key <sub>7</sub>   |
| counter <sub>0</sub> | nonce <sub>0</sub> | nonce <sub>1</sub> | nonce <sub>2</sub> |

[0036] ここで、パラメータ設定部111は、384ビットの鍵に対応するため、例えば、前半の256ビットをkey<sub>0</sub>～key<sub>7</sub>に32ビットずつ割り当て、後半の128ビットをconst<sub>1</sub>～const<sub>3</sub>に32ビットずつ割り当てる。

これにより、暗号化装置1は、128ビットの定数部分を鍵の一部として利用することで、256ビットを超える384ビットの鍵を用いたストリーム暗号を実現できる。

[0037] [Rocca]

非特許文献3に示されている規定の鍵長が256ビットの暗号方式Roc

c a の場合、8つの内部状態  $S$ （それぞれ128ビット）に対して、鍵  $K_0$ 、 $K_1$ （それぞれ128ビット）、初期値  $N$ 、定数  $Z_0$ 、 $Z_1$ （それぞれ128ビット）が次のように設定される。

$$\begin{aligned} S[0] &= K_1, \\ S[1] &= N, \\ S[2] &= Z_0, \\ S[3] &= Z_1, \\ S[4] &= N + K_1, \\ S[5] &= 0, \\ S[6] &= K_0, \\ S[7] &= 0 \end{aligned}$$

（ただし、 $+$ はビット単位の排他的論理和）

[0038] また、同様に規定の鍵長が256ビットの暗号方式  $Rocca-S$  の場合、7つの内部状態  $S$ （それぞれ128ビット）に対して、鍵  $K_0$ 、 $K_1$ （それぞれ128ビット）、初期値  $N$ 、定数  $Z_0$ 、 $Z_1$ （それぞれ128ビット）が次のように設定される。

$$\begin{aligned} S[0] &= K_1, \\ S[1] &= N, \\ S[2] &= Z_0, \\ S[3] &= K_0, \\ S[4] &= Z_1, \\ S[5] &= N + K_1, \\ S[6] &= 0 \end{aligned}$$

（ただし、 $+$ はビット単位の排他的論理和）

[0039] ここで、パラメータ設定部111は、512ビットの鍵に対応するため、例えば、前半の256ビットを  $K_0$ 、 $K_1$  に128ビットずつ割り当て、後半の256ビットを  $Z_0$ 、 $Z_1$  に128ビットずつ割り当てる。

これにより、暗号化装置1は、256ビットの定数部分を鍵の一部として

利用することで、本来の設計である256ビットを超える512ビットの鍵を用いたストリーム暗号を実現できる。

この結果、既存の暗号方式に大きな変更を加えることなく、本来の設計よりも長い鍵長をサポートすることができ、より安全な暗号方式を構築できる。

[0040] 本実施形態によれば、暗号化装置1及び復号装置2は、ストリーム暗号方式で用いる規定の鍵長よりも長い鍵の入力を受け付け、この規定の鍵長を超える部分を分割し、暗号方式の入力パラメータである定数として割り当てる。

これにより、既存の暗号方式において、暗号アルゴリズムを改変することなく規定の鍵長よりも長い鍵に対応できる。

[0041] 入力パラメータの定数は、通常、暗号アルゴリズムの仕様として固定の値が指定されているが、この他の値であっても、暗号化する側（暗号化装置1）と復号する側（復号装置2）とで共有できていれば実行可能である。

したがって、暗号化装置1及び復号装置2は、初期化の際に入力される通常の定数の代わりに鍵の一部を入力することで、対応する鍵サイズを従来よりも拡大できる。

[0042] なお、暗号方式によって定数のサイズは異なるが、例えば、前述の通り最大2倍又は1.5倍の長さまで鍵サイズを拡張することができる。このとき、入力される鍵に固定値をパディングすることにより、最大長に満たない鍵にも対応可能である。

また、本実施形態が改良の対象とするストリーム暗号方式の鍵長は、256ビットには限られない。本実施形態を、従来広く利用されている128ビットの鍵を用いる暗号方式、あるいは64ビットや512ビット等の暗号方式に適用することで、それぞれの安全性を強化することができる。

[0043] また、入力パラメータである定数は、ストリーム暗号方式の内部状態の一部として初期化される値であり、この値を鍵の一部に置き換えても暗号アルゴリズムに不都合が生じることはなく、既存のアルゴリズムを改変すること

なく、容易に安全性を向上させることができる。

例えば、ストリーム暗号方式として、R o c c a又はR o c c a－Sを対象とすると、2つの128ビットの定数それぞれに対して、鍵の一部（256ビット）を割り当てることにより、最大で512ビットの鍵を用いることができ、256ビットの安全性が得られる。

[0044] なお、本実施形態により、例えばストリーム暗号の安全性を向上できることから、国連が主導する持続可能な開発目標（SDGs）の目標9「レジリエントなインフラを整備し、持続可能な産業化を推進すると共に、イノベーションの拡大を図る」に貢献することが可能となる。

[0045] 以上、本開示の実施形態について説明したが、本開示は前述した実施形態に限るものではない。また、前述した実施形態に記載された効果は、本開示から生じる最も好適な効果を列挙したに過ぎず、本開示による効果は、実施形態に記載されたものに限定されるものではない。

[0046] 暗号化装置1及び復号装置2による暗号化方法及び復号方法は、ソフトウェアにより実現される。ソフトウェアによって実現される場合には、このソフトウェアを構成するプログラムが、情報処理装置（コンピュータ）にインストールされる。また、これらのプログラムは、CD-ROMのようなリムーバブルメディアに記録されてユーザに配布されてもよいし、ネットワークを介してユーザのコンピュータにダウンロードされることにより配布されてもよい。さらに、これらのプログラムは、ダウンロードされることなくネットワークを介したWebサービスとしてユーザのコンピュータに提供されてもよい。

## 産業上の利用可能性

[0047] 本開示によれば、一例として、既存の暗号方式において、規定の鍵長よりも長い鍵に対応できる。

## 符号の説明

- [0048]   1   暗号化装置  
          2   復号装置

- 1 1 制御部
- 1 2 記憶部
- 2 1 制御部
- 2 2 記憶部
- 1 1 1 パラメータ設定部
- 1 1 2 初期化処理部
- 1 1 3 暗号化実行部
- 2 1 1 パラメータ設定部
- 2 1 2 初期化処理部
- 2 1 3 復号実行部

## 請求の範囲

- [請求項1] 所定のストリーム暗号方式で用いる規定の鍵長よりも長い鍵の入力を受け付け、当該規定の鍵長を超える部分を分割し、当該ストリーム暗号方式の入力パラメータである定数として割り当てるパラメータ設定部と、
- 前記パラメータ設定部により割り当てられた前記入力パラメータにより、前記ストリーム暗号方式の初期化を行う初期化処理部と、
- 前記ストリーム暗号方式に従って暗号化を実行する暗号化実行部と、を備える暗号化装置。
- [請求項2] 前記定数は、前記ストリーム暗号方式の内部状態の一部として初期化される値である請求項1に記載の暗号化装置。
- [請求項3] 前記ストリーム暗号方式は、R o c c a又はR o c c a - Sであり、
- 前記パラメータ設定部は、2つの128ビットの定数それぞれに対して、512ビットの鍵の一部を割り当てる請求項1に記載の暗号化装置。
- [請求項4] 所定のストリーム暗号方式で用いる規定の鍵長よりも長い鍵の入力を受け付け、当該規定の鍵長を超える部分を分割し、当該ストリーム暗号方式の入力パラメータである定数として割り当てるパラメータ設定部と、
- 前記パラメータ設定部により割り当てられた前記入力パラメータにより、前記ストリーム暗号方式の初期化を行う初期化処理部と、
- 請求項1から請求項3のいずれかに記載の暗号化装置により出力された暗号文を、前記ストリーム暗号方式に従って復号する復号実行部と、を備える復号装置。
- [請求項5] 所定のストリーム暗号方式で用いる規定の鍵長よりも長い鍵の入力を受け付け、当該規定の鍵長を超える部分を分割し、当該ストリーム暗号方式の入力パラメータである定数として割り当てるパラメータ設

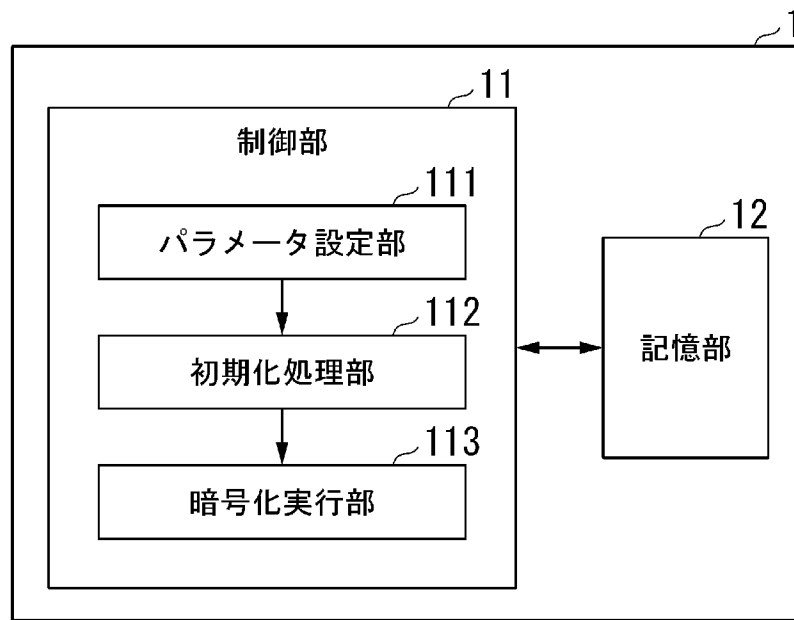
定ステップと、

前記パラメータ設定ステップにおいて割り当てられた前記入力パラメータにより、前記ストリーム暗号方式の初期化を行う初期化処理ステップと、

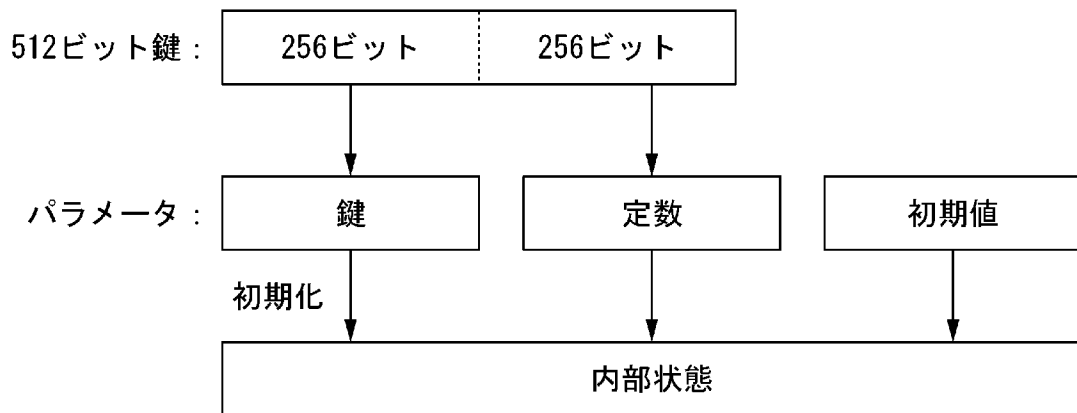
前記ストリーム暗号方式に従って暗号化を実行する暗号化実行ステップと、をコンピュータが実行する暗号化方法。

[請求項6]      請求項 1 から請求項 3 のいずれかに記載の暗号化装置としてコンピュータを機能させるための暗号化プログラム。

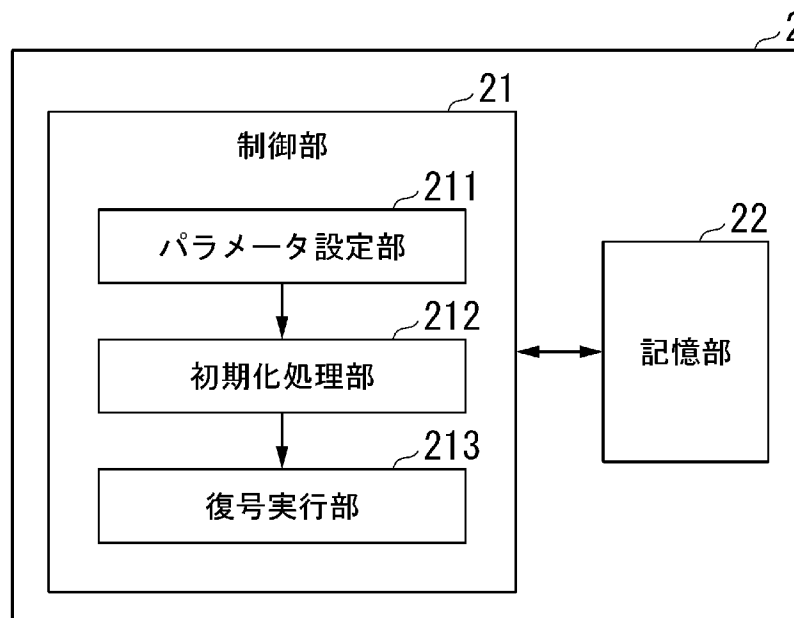
[図1]



[図2]



[図3]



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2024/007800

**A. CLASSIFICATION OF SUBJECT MATTER****H04L 9/22**(2006.01)i; **G09C 1/00**(2006.01)i

FI: H04L9/22 200; G09C1/00 610D

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)

H04L9/22; G09C1/00

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 1971-2024  
Registered utility model specifications of Japan 1996-2024  
Published registered utility model applications of Japan 1994-2024

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         | CN 114357474 A (NANJING ONE IDENTITY EXPRESS INFORMATION TECHNOLOGY CO. LTD.) 15 April 2022 (2022-04-15)<br>paragraphs [0013]-[0018], claims 4, 9                                                                                                                                                 | 1-6                   |
| A         | 戸丸辰也. 原理から理解する量子コンピュータ. 日本セキュリティ・マネジメント学会誌. 28 March 2022, vol. 35, no. 3, pp. 25-33, <DOI:10.32230/jssmjjournal.35.3_25>, (TOMARU, Tatsuya. Let us understand quantum computer from the principle. Security Management.)<br>in particular, 3.3. Relationship to Cryptography                     | 1-6                   |
| A         | 竹内信幸ほか. RoccaとAEGISファミリーのラウンド関数の安全性評価. 2022年暗号と情報セキュリティシンポジウム予稿集. 18 January 2022, pp. 1-8, (TAKEUCHI, Nobuyuki et al. Security Evaluation for Round Functions of Rocca and AEGIS Families. 2022 Symposium on Cryptography and Information Security.)<br>in particular, 3. Subject Configurations | 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  
“D” document cited by the applicant in the international application  
“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

19 April 2024

Date of mailing of the international search report

07 May 2024

Name and mailing address of the ISA/JP

Japan Patent Office (ISA/JP)  
3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915  
Japan

Authorized officer

Telephone No.

## INTERNATIONAL SEARCH REPORT

### Information on patent family members

International application No.

**PCT/JP2024/007800**

| Patent document<br>cited in search report |           |   | Publication date<br>(day/month/year) | Patent family member(s) | Publication date<br>(day/month/year) |
|-------------------------------------------|-----------|---|--------------------------------------|-------------------------|--------------------------------------|
| CN                                        | 114357474 | A | 15 April 2022                        | (Family: none)          |                                      |

A. 発明の属する分野の分類（国際特許分類（IPC））

H04L 9/22(2006.01)i; G09C 1/00(2006.01)i

FI: H04L9/22 200; G09C1/00 610D

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））

H04L9/22; G09C1/00

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 - 2024年

日本国実用新案登録公報

1996 - 2024年

日本国登録実用新案公報

1994 - 2024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<br>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<br>請求項の番号 |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------|----------------|
| A               | CN 114357474 A (NANJING ONE IDENTITY EXPRESS INFORMATION TECHNOLOGY CO. LTD.) 15.04.2022 (2022 - 04 - 15)<br>段落0013-0018, 請求項4, 9   | 1-6            |
| A               | 戸丸 辰也, 原理から理解する量子コンピュータ, 日本セキュリティ・マネジメント学会誌, 2022.03.28, 35巻, 3号, pp.25-33, <DOI:10.32230/jssmjournal.35.3_25><br>特に, 3.3節 暗号とのかかわり | 1-6            |
| A               | 竹内 信幸 ほか, R o c c a とA E G I Sファミリーのラウンド関数の安全性評価, 2022年 暗号と情報セキュリティシンポジウム予稿集, 2022.01.18, pp.1-8<br>特に, 3節 対象構成                     | 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

“D” 国際出願で出願人が先行技術文献として記載した文献

“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

19.04.2024

国際調査報告の発送日

07.05.2024

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）

行田 悦資 5S 6304

電話番号 03-3581-1101 内線 3529

様式 PCT/ISA/210（第2ページ）（2022年7月）

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/JP2024/007800

| 引用文献           | 公表日        | パテントファミリー文献 | 公表日 |
|----------------|------------|-------------|-----|
| CN 114357474 A | 15.04.2022 | (ファミリーなし)   |     |