

【公報種別】特許法第 17 条の 2 の規定による補正の掲載
 【部門区分】第 6 部門第 2 区分
 【発行日】平成30年9月27日(2018.9.27)

【公表番号】特表2017-531209(P2017-531209A)
 【公表日】平成29年10月19日(2017.10.19)
 【年通号数】公開・登録公報2017-040
 【出願番号】特願2017-518094(P2017-518094)
 【国際特許分類】

G 0 9 C 1/00 (2006.01)

【 F I 】

G 0 9 C 1/00 6 1 0 A

【手続補正書】

【提出日】平成30年8月14日(2018.8.14)

【手続補正 1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

反復暗号を用いて暗号信号を生成するための方法であって、
第1の信号を受信するステップと、
前記第1の信号から、前記反復暗号の状態値の現在のインスタンスを決定するステップ
と、
前記状態値の前記現在のインスタンスを用いて、回転距離を決定するステップと、
前記回転距離だけ、置換ボックス値を回転させるステップと、
前記回転された置換ボックス値と前記状態値の前記現在のインスタンスとを結合するス
テップと、
前記回転された置換ボックス値と前記状態値の前記現在のインスタンスとの前記結合を
用いて、前記反復暗号の前記状態値の後続のインスタンスを生成するステップと
を含む方法。

【請求項 2】

前記結合するステップが、
前記回転された置換ボックス値をマスクするステップと、
前記回転されマスクされた置換ボックス値と前記状態値の前記現在のインスタンスとを
結合するステップと
を含む、請求項1に記載の方法。

【請求項 3】

前記結合するステップが、
前記回転された置換ボックス値と前記状態値の前記現在のインスタンスとを結合するこ
とによって、前記状態値の中間インスタンスを生成するステップ
を含む、請求項1に記載の方法。

【請求項 4】

前記状態値の前記後続のインスタンスを生成することが、前記状態値の前記中間インス
タンスを回転させることを含み、
前記状態値の前記中間インスタンスが、前記置換ボックス値のビット量に基づくビット
量だけ回転される、請求項3に記載の方法。

【請求項 5】

前記状態値の前記中間インスタンスを生成することが、暗号鍵を、前記回転された置換ボックス値と前記状態値の現在のインスタンスとの前記結合の結果と結合することを含む、請求項4に記載の方法。

【請求項6】

前記状態値の前記現在のインスタンスを決定することが、暗号鍵と前記状態値の以前のインスタンスとを結合すること、または前記状態値の以前のインスタンスを回転することを含む、請求項1に記載の方法。

【請求項7】

前記回転距離の前記決定が、前記状態値の前記現在のインスタンスのビットのサブセットに基づき、前記反復暗号の前記状態値の前記後続のインスタンスを生成することが、暗号鍵を、前記回転された置換ボックス値と前記状態値の前記現在のインスタンスとの前記結合と結合することを含む、請求項1に記載の方法。

【請求項8】

前記回転距離の前記決定が、前記状態値の前記現在のインスタンスからビットのサブセットを選択することと、前記選択されたビットのサブセットに対応する第1の数を決定することと、前記置換ボックス値のビット量に対応する第2の数を決定することと、前記第1の数に前記第2の数を乗算することとを含むか、または前記状態値の前記現在のインスタンスをマスクすることと、前記マスクされた前記状態値の前記現在のインスタンスをシフトすることとを含む、請求項1に記載の方法。

【請求項9】

前記置換ボックス値が全単射である、請求項1に記載の方法。

【請求項10】

前記回転距離の前記決定、前記置換ボックス値の前記回転、および前記回転された置換ボックス値と前記状態値の前記現在のインスタンスとの前記結合が、演算

$s \wedge = \text{ROR}(\text{sbox}, (s \& M1) \ll S1) \& \text{MASK}$ 、および

$s = \text{ROR}(s, R1)$ によって実行され、

ただし、 $\wedge$ はXOR演算であり、RORは右回転演算であり、 $\&$ はAND演算であり、 $\ll$ はビット左シフト演算であり、 s は前記状態値のインスタンスに対応し、 $M1$ は第1のマスク値であり、 MASK は第2のマスク値であり、 $S1$ はシフト値であり、 $R1$ は回転値であり、 sbox は前記置換ボックス値のインスタンスに対応する、請求項1に記載の方法。

【請求項11】

前記回転距離の前記決定、前記置換ボックス値の前記回転、および前記回転された置換ボックス値と前記状態値の前記現在のインスタンスとの前記結合が、演算

$s = \text{ROL}(s, R1)$ 、および

$s \wedge = \text{ROR}(\text{sbox}, (s \& M1) \ll S1) \& \text{MASK}$ によって実行され、

ただし、 $\wedge$ はXOR演算であり、ROLは左回転演算であり、RORは右回転演算であり、 $\&$ はAND演算であり、 $\ll$ はビット左シフト演算であり、 s は前記状態値のインスタンスに対応し、 $M1$ は第1のマスク値であり、 MASK は第2のマスク値であり、 $R1$ は回転値であり、 $S1$ はシフト値であり、 sbox は前記置換ボックス値のインスタンスに対応する、請求項1に記載の方法。

【請求項12】

前記回転距離の前記決定、前記置換ボックス値の前記回転、および前記回転された置換ボックス値と前記状態値の前記現在のインスタンスとの前記結合が、演算

$s \wedge = \text{ROR}(\text{sbox}, (s \& M1) \ll S1)$ 、および

$s = \text{ROR}(s, R1)$ によって実行され、

ただし、 $\wedge$ はXOR演算であり、RORは右回転演算であり、 $\&$ はAND演算であり、 $\ll$ はビット左シフト演算であり、sは前記状態値のインスタンスに対応し、M1はマスク値であり、S1はシフト値であり、R1は回転値であり、sboxは前記置換ボックス値のインスタンスに対応する、請求項1に記載の方法。

【請求項13】

前記回転距離の前記決定、前記置換ボックス値の前記回転、および前記回転された置換ボックス値と前記状態値の前記現在のインスタンスとの前記結合が、演算

$s = \text{ROL}(s, R1)$ 、
 $\text{shift} = (\text{tinv} \gg ((\text{state} \& M1) \ll S1)) \ll S2$ 、および
 $s \wedge= \text{ROR}(\text{sbox}, \text{shift})$ によって実行され、

ただし、 $\wedge$ はXOR演算であり、ROLは左回転演算であり、RORは右回転演算であり、 $\&$ はAND演算であり、 $\ll$ はビット左シフト演算であり、 $\gg$ はビット右シフト演算であり、sは前記状態値のインスタンスに対応し、M1はマスク値であり、S1は第1のシフト値であり、S2は第2のシフト値であり、R1は第1の回転値であり、shiftは第2の回転値であり、tinvは逆置換ボックス値であり、sboxは前記置換ボックス値のインスタンスに対応する、請求項1に記載の方法。

【請求項14】

反復暗号を用いて暗号信号を生成するための装置であって、

第1の信号を受信するための手段と、

前記第1の信号から、前記反復暗号の状態値の現在のインスタンスを決定するための手段と、

前記状態値の前記現在のインスタンスを用いて、回転距離を決定するための手段と、

前記回転距離だけ、置換ボックス値を回転させるための手段と、

前記回転された置換ボックス値と前記状態値の前記現在のインスタンスとを結合するための手段と、

前記回転された置換ボックス値と前記状態値の前記現在のインスタンスとの前記結合を用いて、前記反復暗号の前記状態の後続のインスタンスを生成するための手段とを備える装置。

【請求項15】

コンピュータ実行可能コードを記録するコンピュータ可読記録媒体であって、

第1の信号を受信すること、

前記第1の信号から、反復暗号の状態値の現在のインスタンスを決定すること、

前記状態値の前記現在のインスタンスを用いて、回転距離を決定すること、

前記回転距離だけ、置換ボックス値を回転させること、

前記回転された置換ボックス値と前記状態値の前記現在のインスタンスとを結合すること、および

前記回転された置換ボックス値と前記状態値の前記現在のインスタンスとの前記結合を用いて、前記反復暗号の前記状態の後続のインスタンスを生成することを行うためのコードを含む、コンピュータ可読記録媒体。