Computer Security Symposium 2017
23 - 25 October 2017

# ブロック暗号 SHipher の 選択平文解読と既知平文解読

藤山　雄輔*　金子　敏信*　五十嵐　保隆*

**概要**：SHipher は 2014 年に Xiali Hei,Binheng Song によって提案されたブロック長($(3l-1)$ビット　$l$は正の整数)の共通鍵ブロック暗号である．秘密鍵から鍵となる行列を生成し，行列化した平文と乗算演算を行うことにより暗号文を得る仕様になっている．

鍵生成の仕様上，秘密鍵と等価な鍵が複数存在するので，秘密鍵を一意に特定することは不可能である．しかし，条件を満たした平文と暗号文の対を 4 通り用意することで秘密鍵と等価な鍵行列を特定することが可能であり，この鍵行列を用いることで任意の暗号文の復号が可能となる．

本稿では，実際に鍵行列を特定し，暗号文を復号できることを示した．

**キーワード**：ブロック暗号，SHipher

## 1. はじめに

SHipher は，2014 年に Xiali Hei,Binheng Song によって提案された任意のブロック長$(3l-1)$及び秘密鍵長$2m*(3l-1)$ビットを持つ共通鍵ブロック暗号($l,m$は正の整数)である．秘密鍵から暗号化を行う際に使用する鍵となる行列を生成し，同じく行列化を行った平文と乗算演算を行うことにより暗号文を得る仕様となっている．

鍵生成の仕様上，秘密鍵には等価な鍵が複数存在するため秘密鍵を特定することは不可能である．しかし，条件を満たした平文と暗号文の対を 4 通り用意することで秘密鍵より生成された鍵行列と等価な鍵行列を特定することが可能であり，この鍵行列を用いることで任意の暗号文の復号が可能となる．

本稿では，実際にこの鍵行列を特定し，暗号文を復号できることを示した．

## 2. SHipher の全体構造

SHipher は秘密鍵及び平文の行列化，生成された秘密鍵及び平文の行列による乗算演算，暗号文の生成及び出力の 3 段階で構成されている．平文のブロック長は$(3l-1)$ビット，鍵長は$2m*(3l-1)$ビットである．図 1,2 に SHipher の暗号化過程と復号過程を示し，その詳細は節 2.1 から節 2.5 に示す．

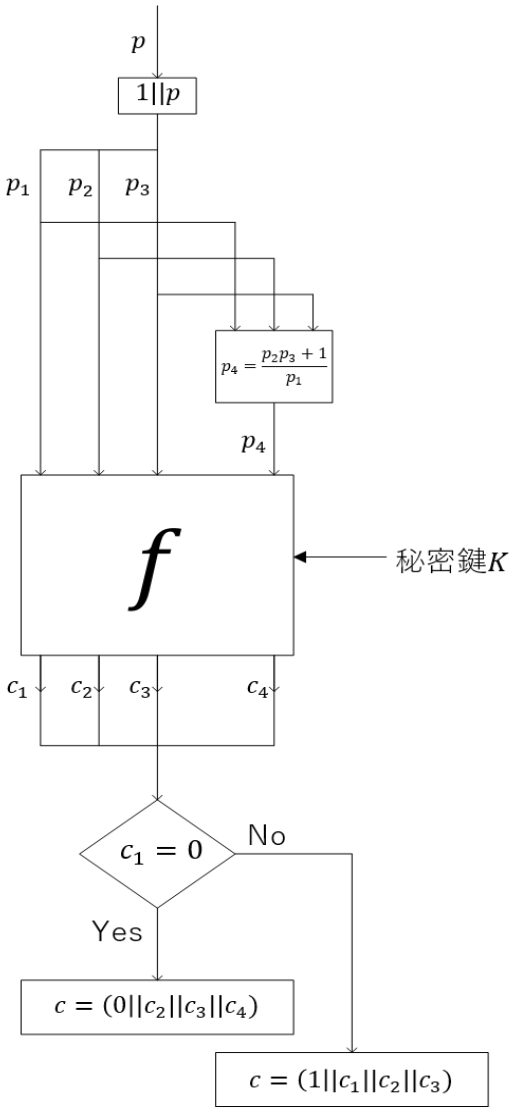


図 1　全体構造（暗号化過程）

* 東京理科大学大学院理工学研究科電気工学専攻

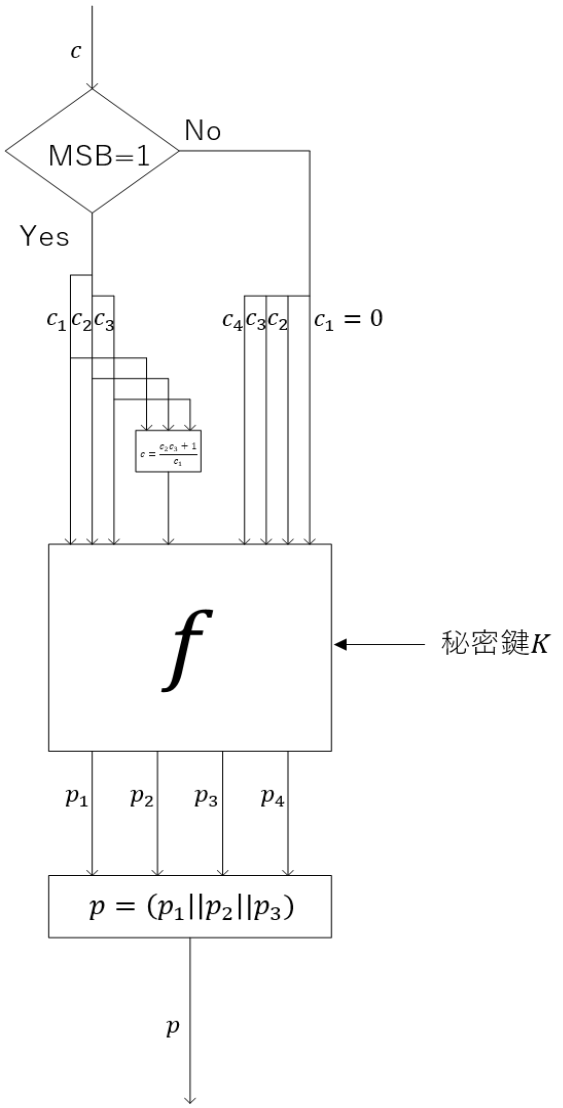


図２　全体構造（復号化過程）

### 2.1 平文の行列化

$(3l-1)$ビットの平文$p$を行列$\boldsymbol{M_p}$に変換する．

ｉ．平文$p$の最上位ビット（MSB）に 1 を結合

$$1||p \tag{1}$$

ⅱ．結合して$3l$ビットとなった $1||p$を 3 等分し，$p_4$を(3)式のように生成

$$1||p = (p_1, p_2, p_3) \tag{2}$$

$$p_4 = \frac{p_2 p_3 + 1}{p_1} \mod q \tag{3}$$

ただし，$p_1 \neq 0$であり，$q$は$(l+1)$ビットの素数に設定する．

ⅲ．(2),(3)式を用いて，行列$\boldsymbol{M_p}$を生成する．行列式が 1 となるように$p_4$を設定しているため，$\boldsymbol{M_p}$は必ず逆行列を持つ．

$$\boldsymbol{M_p} = \begin{bmatrix} p_1 & p_2 \\ p_3 & p_4 (= \dfrac{p_2 p_3 + 1}{p_1}) \end{bmatrix} \mod q \tag{4}$$

### 2.2 鍵生成

秘密鍵$K$より暗号化に用いる鍵行列$\boldsymbol{H_1}$,$\boldsymbol{H_2}$を生成する．

ｉ．秘密鍵$K$の生成

長さ$3l-1$ビットの値$a_{i_j}$をランダムに$2m$個選択し（$j = 0,1,\ldots 2m-1$），秘密鍵$K$を(5)式とする．

$$K = a_{i_0}||a_{i_1}|| \ \ldots ||a_{i_{2m}-1} \tag{5}$$

ⅱ．鍵行列$H_1$，$H_2$の生成

$(3l-1)$ビットの値$a_{i_j}$を節 2.1 平文の行列化の手順ｉからⅲにおいて$p = a_{i_j}$とみなし，生成された$\boldsymbol{M_p}$を$\boldsymbol{M_{a_{i_j}}}$とする．

生成された行列$\boldsymbol{M_{a_{i_j}}}$を次式(6)，(7)に代入し，行列の積を計算することで鍵行列$\boldsymbol{H_1}$，$\boldsymbol{H_2}$を生成する．また，(4)式と同様に鍵行列$\boldsymbol{H_1}$，$\boldsymbol{H_2}$の行列式は 1 となり，必ず逆行列を持つ．

$$\begin{aligned} \boldsymbol{H_1} &= \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \\ &= \boldsymbol{M_{a_{i_{m-1}}}} \times \boldsymbol{M_{a_{i_{m-2}}}} \times \ldots\ldots \times \boldsymbol{M_{a_{i_1}}} \times \boldsymbol{M_{a_{i_0}}} \\ &\mod q \end{aligned} \tag{6}$$

$$\begin{aligned} \boldsymbol{H_2} &= \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} \\ &= \boldsymbol{M_{a_{i_{2m-1}}}} \times \boldsymbol{M_{a_{i_{2m-2}}}} \times \ldots\ldots \times \boldsymbol{M_{a_{i_{m+1}}}} \times \boldsymbol{M_{a_{i_m}}} \\ &\mod q \end{aligned} \tag{7}$$

### 2.3 暗号化

鍵行列$\boldsymbol{H_1}$,$\boldsymbol{H_2}$を用いて暗号文$\boldsymbol{c}$を生成する．

ｉ．暗号文行列$\boldsymbol{M_c}$の生成

$$\boldsymbol{M_c} = \boldsymbol{H_1} \times \boldsymbol{M_p} \times \boldsymbol{H_2}$$

$$\begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \begin{bmatrix} p_1 & p_2 \\ p_3 & p_4 \end{bmatrix} \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} \mod q \tag{8}$$

(8)式から分かるように$\boldsymbol{M_c}$の行列式も 1 である．尚，平文と暗号文を行列ではなくベクトルで表現すると，(8)式は次式で書き表すことができる．

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix} = \boldsymbol{H} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{bmatrix}$$

$$\boldsymbol{H} = \begin{bmatrix} a_1b_1 & a_1b_3 & a_2b_1 & a_2b_3 \\ a_1b_2 & a_1b_4 & a_2b_2 & a_2b_4 \\ a_3b_1 & a_3b_3 & a_4b_1 & a_4b_3 \\ a_3b_2 & a_3b_4 & a_4b_2 & a_4b_4 \end{bmatrix} \quad (9)$$

ii. 暗号文$c$の生成

$$c = (c_1 \| c_2 \| c_3 \| c_4) \quad (10)$$

### 2.4 出力

暗号文$c$の出力は（11），（12）式の 2 通りとなる．

$\mathrm{c}_1 \neq 0$の場合　$c = (1 \| c_1 \| c_2 \| c_3)$　(11)

$\mathrm{c}_1 = 0$の場合　$c = (0 \| c_2 \| c_3 \| c_4)$　(12)

暗号文の復号は節 2.5 に示すように暗号化の逆演算を行うため，暗号文をすべて（11）式のように出力すると，$\mathrm{c}_1$が 0 の場合に$\mathrm{c}_4$を生成することが出来ない．従って，$\mathrm{c}_1$の値により出力時の暗号文を変化させる．この時，暗号文を区別するために MSB にそれぞれ 1 か 0 の冗長ビットを加える．

### 2.5 復号

鍵行列$\boldsymbol{H_1}$,$\boldsymbol{H_2}$の逆行列を用いて暗号文を復号し平文を得る．ただし，$\mathrm{c}_1 \neq 0$の場合 $\mathrm{c}_4 = \frac{c_2c_3+1}{c_1} \mod \mathrm{q}$

i. 平文行列$\boldsymbol{M_p}$の復元

$$\boldsymbol{M_p} = \begin{bmatrix} p_1 & p_2 \\ p_3 & p_4 \end{bmatrix} = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}^{-1} \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}^{-1} \quad (13)$$

mod q

ii. 平文の復元

$$p = (p_1 \| p_2 \| p_3) \quad (14)$$

## 3. 選択平文解読と機知平文解読

### 3.1 解読手法の手順

SHipher は秘密鍵，平文を共に行列に変換し暗号化変換を行う．鍵生成の性質上，秘密鍵$K$を特定することは不可能である．しかし，秘密鍵$K$より生成された鍵行列$\boldsymbol{H_1}$,$\boldsymbol{H_2}$と等価な(9)式の鍵行列$\boldsymbol{H}$を特定することができる．この鍵行列$\boldsymbol{H}$を用いることで、秘密鍵$K$を特定することができなくても暗号文の復号が可能である．実際には鍵行列$\boldsymbol{H}$は平文と暗号文のベクトルの対を 4 通り用意することで特定することが可能である．

i. (1)式に示された$(3l-1)$ビットの平文$p^i$ $(i = 1,2,3,4)$を 4 通り用意し、(2),(3)式を用いて 4 通りの$(p_1^i, p_2^i, p_3^i, p_4^i)$を導出する．そして，次式に従い平文行列$\boldsymbol{P}$を生成する．

$$\boldsymbol{P} = \begin{bmatrix} p_1^1 & p_1^2 & p_1^3 & p_1^4 \\ p_2^1 & p_2^2 & p_2^3 & p_2^4 \\ p_3^1 & p_3^2 & p_3^3 & p_3^4 \\ p_4^1 & p_4^2 & p_4^3 & p_4^4 \end{bmatrix} \quad (15)$$

mod q

ii. 4 通りの平文$p^i$に対応する暗号文$c^i$を入手し(11),(12)式に従い$(c_1^i, c_2^i, c_3^i, c_4^i)$を導出し，次式に従い暗号文行列$\boldsymbol{C}$を生成する．

$$\boldsymbol{C} = \begin{bmatrix} \mathrm{c}_1^1 & \mathrm{c}_1^2 & \mathrm{c}_1^3 & \mathrm{c}_1^4 \\ \mathrm{c}_2^1 & \mathrm{c}_2^2 & \mathrm{c}_2^3 & \mathrm{c}_2^4 \\ \mathrm{c}_3^1 & \mathrm{c}_3^2 & \mathrm{c}_3^3 & \mathrm{c}_3^4 \\ \mathrm{c}_4^1 & \mathrm{c}_4^2 & \mathrm{c}_4^3 & \mathrm{c}_4^4 \end{bmatrix} \quad (16)$$

mod q

iii. (9)式より平文行列$\boldsymbol{P}$と暗号文行列$\boldsymbol{C}$の関係は次式で表すことができる．

$$\boldsymbol{C} = \boldsymbol{H} \times \boldsymbol{P} \quad \mod \mathrm{q} \quad (17)$$

iv. (17)式を$\boldsymbol{H}$について解く．

$$\begin{bmatrix} a_1b_1 & a_1b_3 & a_2b_1 & a_2b_3 \\ a_1b_2 & a_1b_4 & a_2b_2 & a_2b_4 \\ a_3b_1 & a_3b_3 & a_4b_1 & a_4b_3 \\ a_3b_2 & a_3b_4 & a_4b_2 & a_4b_4 \end{bmatrix} = \begin{bmatrix} \mathrm{c}_1^1 & \mathrm{c}_1^2 & \mathrm{c}_1^3 & \mathrm{c}_1^4 \\ \mathrm{c}_2^1 & \mathrm{c}_2^2 & \mathrm{c}_2^3 & \mathrm{c}_2^4 \\ \mathrm{c}_3^1 & \mathrm{c}_3^2 & \mathrm{c}_3^3 & \mathrm{c}_3^4 \\ \mathrm{c}_4^1 & \mathrm{c}_4^2 & \mathrm{c}_4^3 & \mathrm{c}_4^4 \end{bmatrix} \begin{bmatrix} p_1^1 & p_1^2 & p_1^3 & p_1^4 \\ p_2^1 & p_2^2 & p_2^3 & p_2^4 \\ p_3^1 & p_3^2 & p_3^3 & p_3^4 \\ p_4^1 & p_4^2 & p_4^3 & p_4^4 \end{bmatrix}^{-1} \quad (18)$$

mod q

$$\boldsymbol{H} = \boldsymbol{C} \times \boldsymbol{P^{-1}} \quad (19)$$

(18)式から分かるように，平文行列$\boldsymbol{P}$は逆行列$\boldsymbol{P^{-1}}$を持たなければならないという制約条件が生じる．$\boldsymbol{H}$はそのままでは平文を暗号文に変換することはできるが，暗号文を平文に復号することはできない．$\boldsymbol{H}$の行列式は次式のように表すことができるため、$\boldsymbol{H}$は常に逆行列を持つ．

$$det(\boldsymbol{H}) = det(\boldsymbol{H_1})^2 \times det(\boldsymbol{H_2})^2 = 1 \qquad (20)$$

従って，$\boldsymbol{H}$の逆行列を用いることで任意の暗号文から平文に復号することが可能である，

等価鍵の解読という意味では，ここまでの手順で十分に目的を果たしている．これ以降ではさらに鍵行列$\boldsymbol{H_1}$，$\boldsymbol{H_2}$の候補を絞り込むことができることを示す．

鍵行列$\boldsymbol{H}$から$\boldsymbol{H_1}$,$\boldsymbol{H_2}$の各要素を絞り込む．特定した鍵行列$\boldsymbol{H}$の要素を$h^i_j$(i,j=1,2,3,4)とし鍵行列$\boldsymbol{H}$を(21)式のように表し$\boldsymbol{H_1}$,$\boldsymbol{H_2}$の各要素について解く．

$$\boldsymbol{H} = \begin{bmatrix} h_1^1 & h_1^2 & h_1^3 & h_1^4 \\ h_2^1 & h_2^2 & h_2^3 & h_2^4 \\ h_3^1 & h_3^2 & h_3^3 & h_3^4 \\ h_4^1 & h_4^2 & h_4^3 & h_4^4 \end{bmatrix} \qquad (21)$$

mod q

(9)式と(21)式より次式が得られる．

$$\begin{aligned} a_1\boldsymbol{H_2} &= \begin{bmatrix} h_1^1 & h_2^1 \\ h_1^2 & h_2^2 \end{bmatrix}, a_2\boldsymbol{H_2} = \begin{bmatrix} h_1^3 & h_2^3 \\ h_1^4 & h_2^4 \end{bmatrix} \\ a_3\boldsymbol{H_2} &= \begin{bmatrix} h_3^1 & h_4^1 \\ h_3^2 & h_4^2 \end{bmatrix}, a_4\boldsymbol{H_2} = \begin{bmatrix} h_3^3 & h_4^3 \\ h_3^4 & h_4^4 \end{bmatrix} \\ b_1\boldsymbol{H_1} &= \begin{bmatrix} h_1^1 & h_1^3 \\ h_3^1 & h_3^3 \end{bmatrix}, b_2\boldsymbol{H_1} = \begin{bmatrix} h_2^1 & h_2^3 \\ h_4^1 & h_4^3 \end{bmatrix} \\ b_3\boldsymbol{H_1} &= \begin{bmatrix} h_1^2 & h_1^4 \\ h_3^2 & h_3^4 \end{bmatrix}, b_4\boldsymbol{H_1} = \begin{bmatrix} h_2^2 & h_2^4 \\ h_4^2 & h_4^4 \end{bmatrix} \end{aligned} \qquad (22)$$

$\boldsymbol{H_1}$と$\boldsymbol{H_2}$の行列式は 1 であるので，(22)式の両辺の行列式を考えると次式が得られる．

$$\begin{aligned} a_1^2 &= h_1^1h_2^2 - h_2^1h_1^2, a_2^2 = h_1^3h_2^4 - h_2^3h_1^4 \\ a_3^2 &= h_3^1h_4^2 - h_3^2h_4^1, a_4^2 = h_3^3h_4^4 - h_4^3h_3^4 \\ b_1^2 &= h_1^1h_3^3 - h_1^3h_3^1, b_2^2 = h_2^1h_4^3 - h_2^3h_4^1 \\ b_3^2 &= h_1^2h_3^4 - h_3^2h_1^4, b_4^2 = h_2^2h_4^4 - h_4^2h_1^2 \end{aligned} \qquad (23)$$

$det(\boldsymbol{H_1}) = 1$であるため，(6)式より$a_1, a_2, a_3, a_4$ のうち少なくとも 2 つは非零となる． $a_1 \neq 0$ とすると，(23)式より次式が得られる．

$$a_1 = \pm\sqrt{h_1^1h_2^2 - h_2^1h_1^2} \quad (2\text{ 通り}) \qquad (24)$$

ゆえに(22)式の第 1 番目の式より次式が得られる．

$$\boldsymbol{H_2} = \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} = \frac{1}{a_1}\begin{bmatrix} h_1^1 & h_2^1 \\ h_1^2 & h_2^2 \end{bmatrix} \qquad (25)$$

(24)式より，$\boldsymbol{H_2}$の候補を 2 通りに絞り込むことができる．同様に$det(\boldsymbol{H_2}) = 1$なので(7)式より$b_1, b_2, b_3, b_4$ のうち少なくとも 2 つは非零となる． $b_1 \neq 0$ とすると，(22)式の第 5 番目の式より次式が得られる．

$$\boldsymbol{H_1} = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} = \frac{1}{b_1}\begin{bmatrix} h_1^1 & h_3^1 \\ h_1^3 & h_3^3 \end{bmatrix} \qquad (26)$$

(26)式より，$\boldsymbol{H_1}$の候補も 2 通りに絞り込むことができる．総当たりでは$\boldsymbol{H_1}$と$\boldsymbol{H_2}$はそれぞれ$2^{3l-1}$通りあり$(\boldsymbol{H_1}, \boldsymbol{H_2})$の組み合わせは$2^{2(3l-1)}$通りあるが，この組み合わせを 2 通りに絞り込むことができることを示した．

### 3.2 平文の制約条件

平文行列$P$が逆行列を持つという制約条件の下，選択平文解読及び既知平文解読について調査を行う．

#### 3.2.1 選択平文解読

制約条件を満たすように平文を選択する．行列$\boldsymbol{P}$を生成する際, 4 通りの平文を(27)式のように選択することで行列$\boldsymbol{P}$は常に逆行列を持つ．結果，(18)式を解くことで鍵行列$\boldsymbol{H}$の特定が可能となる．(2)式より，$p_1$の MSB は 1 であるが，MSB 以外のビット値は任意である．

$$\boldsymbol{P} = \begin{bmatrix} p_1 & p_1 & p_1 & p_1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ \frac{1}{p_1} & \frac{1}{p_1} & \frac{1}{p_1} & \frac{2}{p_1} \end{bmatrix} \qquad (27)$$

mod q

### 3.3 既知平文解読

ランダムに取得した既知平文による解読の場合，平文行列$\boldsymbol{P}$が逆行列を持つ保証はない．ここでは，既知平文解読の際に平文行列$\boldsymbol{P}$が逆行列を持つ確率（解読成功率）を考察するために既知平文により生成された平文行列$\boldsymbol{P}$が制約条件を満たすか調べるための実験を行った．ランダムに取得した 4 通りの既知平文が互いに独立であるかを既知平文のビット長$l$を変化させ調査する．

さらに比較・考察のために各要素のビット長が$l$である任意の4×4行列を$\boldsymbol{V}$と定め，行列$\boldsymbol{V}$が逆行列を持つ確率を解析する．

行列の各要素は任意の値をとるとする4×4行列$\boldsymbol{V}$を(28)式とする．

$$\boldsymbol{V}=\begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ c_1 & c_2 & c_3 & c_4 \\ d_1 & d_2 & d_3 & d_4 \end{bmatrix} \tag{28}$$

行列$\boldsymbol{V}$が逆行列を持つ確率$prob$は(29)式のように書くことができる．

$$prob = \frac{(2^{4l}-1)}{2^{4l}}\cdot\frac{(2^{4l}-2^{l})}{2^{4l}}\cdot\frac{(2^{4l}-2^{2l})}{2^{4l}}\cdot\frac{(2^{4l}-2^{3l})}{2^{4l}} \tag{29}$$

(29)式の右辺第一項は行列$\boldsymbol{V}$の 1 列目の要素が全て 0 となる場合以外の確率，第二項は 2 列目が 1 列目の整数倍でない確率，第三項は 3 列目が 1 列目と 2 列目の線形結合ではない確率，第四項は 4 列目が他 3 列の線形結合ではない確率をそれぞれ表している．

(29)式により求めた行列$\boldsymbol{V}$が逆行列を持つ確率は各要素のビット長での理論値となる．

計算機を用いて行列$\boldsymbol{P}$，$\boldsymbol{V}$の各要素のビット長$l$を変化させたときの逆行列を持つ確率を調査し，(29)式より求まる行列$\boldsymbol{V}$の逆行列を持つ確率の理論値と比較した．

計算機実験では，4×4行列$\boldsymbol{P}$，$\boldsymbol{V}$が逆行列を持たなかった場合，つまりそれぞれの行列の行列式が 0 となった場合の数をカウントする．このカウントが 100 となった時点の総試行回数からそれぞれの行列が逆行列を持つ確率を算出した．

表 1 にそれぞれの比較の結果を示す．また表 2 に実験を 100 回繰り返した時の総試行回数の平均値を示す．図 3 は表 1,表 2 に示されたデータをグラフ化したものである．

表 1　行列$\boldsymbol{P}$，$\boldsymbol{V}$が逆行列を持つ確率の理論値と実験値との比較

| | 理論値[%] | 実験値[%] | |
|---|---|---|---|
| ビット長 | 行列$V$ | 行列$V$ | 行列$P$ |
| 1 | 30.7617 | 33.4796 | 9.8205 |
| 2 | 68.9435 | 77.5356 | 61.8393 |
| 3 | 85.9435 | 90.7347 | 88.2585 |
| 4 | 93.3595 | 95.3224 | 95.1151 |
| 5 | 96.7773 | 97.8421 | 97.8289 |
| 6 | 98.4130 | 98.8714 | 98.8766 |
| 7 | 99.2126 | 99.4545 | 99.4473 |
| 8 | 99.6078 | 99.7249 | 99.7264 |
| 9 | 99.8043 | 99.8650 | 99.8657 |
| 10 | 99.9022 | 99.9319 | 99.9322 |
| 11 | 99.9511 | 99.9657 | 99.9662 |
| 12 | 99.9755 | 99.9830 | 99.9829 |
| 13 | 99.9877 | 99.9914 | 99.9913 |
| 14 | 99.9938 | 99.9956 | 99.9957 |
| 15 | 99.9969 | 99.9978 | 99.9978 |

表 1 から行列$\boldsymbol{P}$が逆行列を持つ確率は各要素のビット長が大きくなるにつれ(29)式に漸近することが分かる．

表 2　計算機実験の平均総試行回数

| | 平均総試行回数 | |
|---|---|---|
| ビット長 | 行列$V$ | 行列$P$ |
| 1 | 150.33 | 110.89 |
| 2 | 445.15 | 262.05 |
| 3 | 1079.3 | 851.68 |
| 4 | 2137.88 | 2047.14 |
| 5 | 4634.2 | 4606.17 |
| 6 | 8861.2 | 8902.17 |
| 7 | 18335.12 | 18095.96 |
| 8 | 36361.09 | 36552.05 |
| 9 | 74090.99 | 74470.78 |
| 10 | 146906.14 | 147621.15 |
| 11 | 291565.36 | 295927.44 |
| 12 | 588465.43 | 586082.62 |
| 13 | 1173979.93 | 1161423.75 |
| 14 | 2290679.31 | 2344957.56 |
| 15 | 4710618.33 | 4663559.94 |

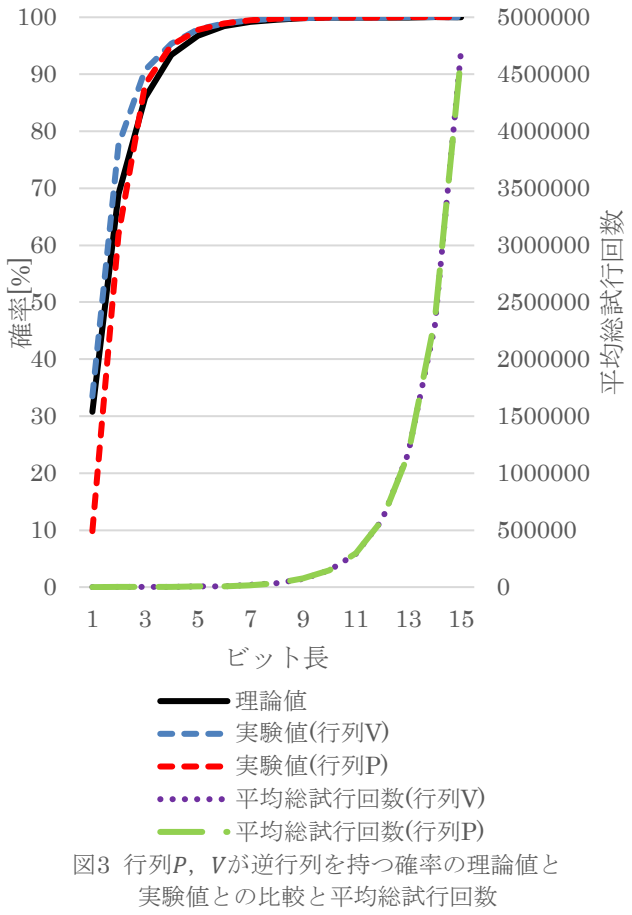


図3　行列$P$，$V$が逆行列を持つ確率の理論値と実験値との比較と平均総試行回数

## 4.　結論

秘密鍵を特定することは不可能であるが，秘密鍵と等価な鍵行列は特定することができ，暗号の解読が可能である．

選択平文の場合，(27)式のように 4 通りの平文を選ぶことで解読が可能となる．既知平文の場合，$l \geq 7$ならば，4 通りの平文のみで解読できる確率は 99%以上である．また，鍵行列$\boldsymbol{H_1}$，$\boldsymbol{H_2}$は$2^{2(3l-1)}$通りあるがこれを 2 通りに絞り込むことができることを示した．

## 参考文献

[1]　Xiali.Hei, Binheng.Song, “SHipher；Families of Block Ciphers based on SubSet-Sum Problem”, https://eprint.iacr.org/2014/103.pdf