論　文

Affine線形暗号と照合可能暗号について

木原眞紀

甲南大学 知能情報学部
兵庫県神戸市東灘区岡本８－９－１, 658-8501

(受理日 2024 年 11 月 25 日)

概 要

照合可能暗号と呼ばれる暗号化したまま 2 つの平文の距離を導出可能な暗号系のクラスが 2019 年に木原，入山によって提案されている．いくつかの暗号系が照合可能暗号に属することはわかっているが，照合可能暗号に属する暗号系の十分条件や必要条件，照合可能暗号で扱うことができる距離関数の条件など，照合可能暗号に関する数学的な性質や構造がわかっていない．本論文では，照合可能暗号の数学的性質の解明を目的として，リー距離と Affine 線系性をもつ暗号系に対して，照合可能暗号の十分条件を与える．

キーワード：Affine 線形暗号，照合可能暗号，秘密計算

1　はじめに

従来の暗号化技術ではデータを暗号化して保護した場合，これらのデータを解析や比較するために計算などの処理を行う場合，1 度復号して元の平文の状態に戻す必要がある．これにより，暗号化したにも関わらず，漏えいリスクが発生する．

この漏えいリスクへの解決策の 1 つとして，秘密計算と呼ばれる，暗号化したまま何らかの計算を行う技術がある．秘密計算技術は，いくつかの技術の総称であり，各技術によってどのような計算ができるか異なるため，ここでは「何らかの計算」と表記した．

例えば，秘密計算技術の 1 つに準同型暗号と呼ばれる技術がある．これは暗号化関数が準同型写像であるような暗号系の総称であり，この準同型性を利用し暗号化したまま加法または乗法の算術演算が可能な秘密計算技術である．乗法に関する準同型暗号として，RSA 暗号 [1] や ElGamal 暗号 [2]，加法に関する準同型暗号として Paillier 暗号 [3] や Elgamal 暗号に若干の修正を加えた modified-ElGamal 暗号が挙げられる．また，暗号化したまま加法と乗法の両方の演算が可能な準同型暗号として，完全準同型暗号についても [4] を皮切りに多くの研究がなされている．

そのほかにも，秘密情報を何らかのグループのメンバーで分散して保持する秘密分散技術 [5, 6] や，自身の入力値を秘匿したまま複数人の参加者で計算を行う秘匿マルチパーティ計算技術 [7, 8, 9] なども秘密計算を実現する技術である．

こういった秘密計算技術の中の 1 つに，2019 年に提案された照合可能暗号と呼ばれる暗号系のクラスがある [10]．照合可能暗号は，暗号化したまま 2 つのデータ間の距離を導出することができる暗号系のクラスであり，いくつかの暗号系がこのクラスに属していることがわかっている [10, 11, 12, 13, 14]．しかし，照合可能暗号クラスに属する暗号系の条件や，照合可能暗号で扱うことができる距離関数の条件など，照合可能暗号の数学的な性質や代数構造などについては未だ明らかでない．

本論文では，照合可能暗号の数学的性質の解明を目的として，距離関数をリー距離に固定した上で Affine 線形性をもつ暗号系が照合可能暗号に属することを示す．

2 数学的準備

本章では，数学的準備として本論文で扱う演算や集合について定義する．その後，暗号系，距離関数について定義する．

- n: 正の整数 ($n > 1$)
- m: 正の整数
- $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z} = \{0, 1, \cdots, n-1\}$
- $X^m := \{(x_1, \cdots, x_m) \mid x_i \in X, i \in \{1, \cdots, m\}\}$: 集合 X の m 個の直積集合
- $\mathbb{R}_+ := [0, \infty)$
- $|X|$: 集合 X の濃度 (または基数ともよぶ)

Definition 2.1 ($\mathbb{Z}_n^m$ 上の加法)**.** 任意の $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}_n^m$ に対して，$\boldsymbol{a} = (a_1, \cdots, a_m)$, $\boldsymbol{b} = (b_1, \cdots, b_m), a_i, b_i \in \mathbb{Z}_n (i = 1, \cdots, m)$ とする．$\mathbb{Z}_n^m$ 上の加法を次のように定める．

$$\begin{aligned} \boldsymbol{a} + \boldsymbol{b} \mod n &:= (a_1 + b_1 \mod n, \cdots, a_m + b_m \mod n), \\ \boldsymbol{a} - \boldsymbol{b} \mod n &:= (a_1 - b_1 \mod n, \cdots, a_m - b_m \mod n). \end{aligned}$$

ここで，$-b_i$ は $b_i \in \mathbb{Z}_n$ の加法逆元であり，$-b_i \in \mathbb{Z}_n$ である．

本論文では $\mathbb{R}^m$ や $\mathbb{C}^m$ 上の通常の意味のベクトルの加法と区別するために，$[\mathrm{mod} n]$ をつけて表記することとする．

Remark 2.2. 定義 *2.1* の加法が $\mathbb{Z}_n^m$ 上で閉じていることは明らかであるので，$(\mathbb{Z}_n^m, +)$ は代数系である．さらに，$(\mathbb{Z}_n^m, +)$ が加法可換群であることも明らかである．

2.1 暗号系

Definition 2.3 (暗号系 [15])**.** 暗号化方式または暗号系とは，*5* 成分からなる組 $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ であり，次の性質をもつとする．

1. $\mathcal{P}$ は集合であり平文空間という．その元を平文とよぶ.
2. $\mathcal{C}$ は集合であり暗号文空間という．その元を暗号文とよぶ.
3. $\mathcal{K}$ は集合であり鍵空間という．その元を鍵とよぶ.
4. $\mathcal{E} = \{E_k \mid k \in \mathcal{K}\}$ は関数 $E_k : \mathcal{P} \to \mathcal{C}$ の族である．その元を暗号化関数という.
5. $\mathcal{D} = \{D_k \mid k \in \mathcal{K}\}$ は関数 $D_k : \mathcal{C} \to \mathcal{P}$ の族である．その元を復号化関数という.
6. 任意の $e \in \mathcal{K}$ に対し，すべての $p \in \mathcal{P}$ に対して等式

$$D_d(E_e(p)) = p$$

が成立するような $d \in \mathcal{K}$ が存在する.

本論文で扱う暗号を暗号系の形で表現して紹介する.

Example 2.1 (Shift 暗号)**.** *Shift* 暗号系 $C_{shift} = (\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ は以下で定める集合により与えられる.

- $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$
- $\mathcal{E} = \{E_k \mid E_k(p) = p + k \mod 26, k \in \mathcal{K}\}$
- $\mathcal{D} = \{D_k \mid D_k(c) = c - k \mod 26, k \in \mathcal{K}\}$.

Example 2.2 (Affine 暗号 [15])**.** *Affine* 暗号系 $C_{affine} = (\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ は以下で定める集合により与えられる.

- $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$
- $\mathcal{K} = \mathbb{Z}_n^2 \times \mathbb{Z}_n^2\{(e, d) \mid e = (a, b) \in \mathbb{Z}_n^2, d = (a', b) \in \mathbb{Z}_n^2, aa' \equiv 1 \mod n\}$
- $\mathcal{E} = \{E_e \mid E_e(p) = ax + b \mod n, e = (a, b) \in \mathcal{K}\}$
- $\mathcal{D} = \{D_d \mid D_d(c) = a'(c - b) \mod 26, d = (a', b) \in \mathcal{K}\}$.

Example 2.3 (Vernam 暗号)**.** *Vernam* 暗号系 $C_{vernam} = (\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ は以下で定める集合により与えられる.

- $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_2^m$
- $\mathcal{E} = \{E_{\boldsymbol{k}} \mid E_{\boldsymbol{k}}(\boldsymbol{p}) = \boldsymbol{p} + \boldsymbol{k} \mod 2, \boldsymbol{k} \in \mathcal{K}\}$
- $\mathcal{D} = \{D_{\boldsymbol{k}} \mid D_{\boldsymbol{k}}(\boldsymbol{c}) = \boldsymbol{c} + \boldsymbol{k} \mod 2, \boldsymbol{k} \in \mathcal{K}\}$.

ここで，任意の鍵 $\boldsymbol{k} \in \mathcal{K}$ は一様分布に従って選ばれる.

例 2.1–例 2.3 は後に定める Affine 線形暗号により表現できる．以降，Affine 線形暗号を定義するまで，適宜 [15] から抜粋しながら定義していく．

R は (乗法) 単位元 1 をもつ可換環であるとする．例えば，n を自然数として，$R = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ をとる．R 上の $\ell \times m$ 行列とは，ℓ 行 m 列の長方形に数を並べて括弧で括った

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ a_{2,1} & a_{1,2} & \cdots & a_{2,m} \\ \vdots & \vdots & \cdots & \vdots \\ a_{\ell,1} & a_{\ell,2} & \cdots & a_{\ell,m} \end{pmatrix}$$

のことであり，これを

$$A = (a_{i,j})$$

とも表す．R 上の全ての $\ell \times m$ 行列全体を $\mathcal{M}_{\ell,m}(R)$ と表すことにする．

Definition 2.4 (行列のベクトルと積)**.** $A = (a_{i,j}) \in \mathcal{M}_{\ell,m}(R), \boldsymbol{v} \in R^m$ に対して，積 $A\boldsymbol{v}$ はベクトル $\boldsymbol{w} = (w_1, \cdots, w_\ell)$ で定義される．ここで，

$$w_i = \sum_{j=1}^{m} a_{i,j} v_j, \quad 1 \leq i \leq \ell$$

であるとする．

Definition 2.5 (行列の和と積)**.** $n \in \mathbb{N}$ とし $A, B \in \mathcal{M}_{\ell,m}(R), A = (a_{i,j}), B = (b_{i,j})$ に対し，

A と B の和 $A + B = (a_{i,j} + b_{i,j})$

A と B の積 $AB = (c_{i,j}), c_{i,j} = \sum_{h=1}^{m} a_{i,h} b_{h,j}$

と定める．

Definition 2.6 (行列式)**.** 行列 $A = (a_{i,j}) \in \mathcal{M}_{m,m}(R)$ の行列式 $\det A$ は次のように定める．

- $m = 1$ のとき：$A = (a)$ より $\det A = a$
- $m > 1$ のとき：$i, j \in \{1, \cdots, m\}$ に対して，A の i 行と j 列を取り除いた $m-1$ 次行列を $A_{i,j}$ と表す．i を固定すると，A の行列式は

  $$\det A = \sum_{j=1}^{m} (-1)^{i+j} a_{i,j} \det A_{i,j}$$

  となる．この値は i の選び方によらず，あらゆる j について，

  $$\det A = \sum_{i=1}^{m} (-1)^{i+j} a_{i,j} \det A_{i,j}$$

  となる．

Definition 2.7 (逆行列)**.** 行列 $A = (a_{i,j}) \in \mathcal{M}_{m,m}(R)$ は，$\det A$ が R で単位元であるときにのみ乗法に関して逆元を持つ．

- $m = 1$ のとき：$A = (a)$ であり，(a^{-1}) が A の逆元となる．
- $m > 1$ のとき：定義 *2.6* における $A_{i,j}$ の定義を用いて，A の余因子行列は $m \times m$ 行列であり，

$$\mathrm{adj}A = ((-1)^{i+j} \det A_{i,j})$$

と定義される．A の逆元は，

$$A^{-1} = (\det A)^{-1}\mathrm{adj}A$$

となる．

Definition 2.8. $A = (a_{i,j}), B = (b_{i,j}) \in \mathcal{M}_{m,m}(\mathbb{Z})$ とし，$n \in \mathbb{N}$ とする．このとき，$1 \leq i, j \leq m$ に対して，$a_{i,j} \equiv b_{i,j} \mod n$ が成り立つとき，$A \equiv B \mod n$ と表す．

証明は省略するが，合同式 $AA' \equiv E_n \mod n$ の解 A' については次の命題がある．

Proposition 2.9. m を $m > 1$ を満たす自然数とする．$A \in \mathcal{M}_{m,m}(\mathbb{Z})$ に対して，$\det A$ が n と互いに素であるときに限り，

$$AA' \equiv E_m \mod n$$

が解 A' をもつ．かつ，a が $a \cdot \det A \equiv 1 \mod n$ を満たす整数ならば，

$$A' = a \cdot \mathrm{adj}A \mod n$$

であり，この解は n を法として一意的である．

Definition 2.10 (Affine 線形)**.** 任意の $\boldsymbol{v} \in R^m$ に対して，

$$f(\boldsymbol{v}) = A\boldsymbol{v} + \boldsymbol{b}$$

である行列 $A \in \mathcal{M}_{\ell,m}(\mathbb{R})$ とベクトル $\boldsymbol{b} \in R^\ell$ が存在するとき，写像 $f : R^m \to R^\ell$ を *Affine* 線形写像という．

Remark 2.11. $\boldsymbol{b} = \boldsymbol{0}$ のとき *Affine* 線形写像 f は線形写像と呼ばれる．

Affine 線形写像 $f : \mathbb{Z}_n^m \to \mathbb{Z}_n^\ell$ は次のように定められる．

Definition 2.12 ($\mathbb{Z}_n^m$ 上の Affine 線形)**.** 任意の $\boldsymbol{v} \in \mathbb{Z}_n^m$ に対して，

$$f(\boldsymbol{v}) = A\boldsymbol{v} + \boldsymbol{b} \mod n$$

である行列 $A \in \mathcal{M}_{\ell,m}(\mathbb{Z}_n)$ とベクトル $\boldsymbol{b} \in \mathbb{Z}_n^\ell$ が存在するとき，写像 $f : \mathbb{Z}_n^m \to \mathbb{Z}_n^\ell$ を *Affine* 線形写像という．

Remark 2.13. $\boldsymbol{b} \equiv \boldsymbol{0} \mod n$ のとき *Affine* 線形写像 f は線形写像と呼ばれる．

Theorem 2.14. 定義 *2.10* の *Affine* 線形写像は，$\ell = m$ であり，かつ $\det A$ が R の単位元であるときに限り全単射である．同様に，定義 *2.12* の *Affine* 線形写像は，$\ell = m$ であり，かつ $\det A$ が n と互いに素であるときに限り全単射である．

Definition 2.15 (ブロック暗号)**.** ブロック暗号とは，平文空間と暗号文空間が Σ^m である暗号系のことである．ここで，Σ^m はアルファベット σ 上の長さ n の全ての語の集合である．ブロック長とは n は自然数である．

Lemma 2.16. ブロック暗号の暗号化関数は置換である．

Definition 2.17 (Affine 線形暗号)**.** ブロック長 m のブロック暗号の平文空間 $\mathcal{P}$ および暗号文空間 $\mathcal{C}$ を $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n^m$ とする．このブロック暗号の全ての暗号化鍵 $e = (A, \boldsymbol{b}) \in \mathcal{M}_{m,m}(\mathbb{Z}_n) \times \mathbb{Z}^m$ に対して暗号化関数 $E_e : \mathcal{P} \to \mathcal{C}$ が *Affine* 線形であれば，この暗号は *Affine* 線形であるという．

より詳しく見ると，任意のブロック暗号の暗号化関数 E_e は補題 2.16 により E_e は全単射である．さらに，定理 2.14 により $\det A$ は n と互いに素である．暗号化鍵 $e = (A, \boldsymbol{b}) \in \mathcal{M}_{m,m}(\mathbb{Z}_n) \times \mathbb{Z}^m$ によって暗号化関数 E は

$$E_e : \mathbb{Z}_n^m \to \mathbb{Z}_n^m \quad A\boldsymbol{p} + \boldsymbol{b} \mod n$$

と一意に定まる．同様に復号化関数は，

$$D_d : \mathbb{Z}_n^m \to \mathbb{Z}_n^m \quad A'(\boldsymbol{c} - \boldsymbol{b}) \mod n$$

となる．ここで，$A' = (a'\mathrm{adj}A) \mod n, a' = (\det A)^{-1}$ とする．共通鍵は $k = (A, \boldsymbol{b})$ として考える (復号鍵を $d = (A', \boldsymbol{b})$ としても良いが，暗号化鍵から多項式時間で一意に導出できるため，暗号化鍵・復号鍵のどちらも秘密にする必要があるため，結局秘密鍵暗号である)．

Affine 線形暗号の例を 2 つ挙げる．

Example 2.4 (Vigenère 暗号 [15])**.** *Vigenère* 暗号系 $C_{vig} = (\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ は以下で定める集合により与えられる．

- $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n^m$
- $\mathcal{E} = \{E_{\boldsymbol{k}} \mid E_{\boldsymbol{k}}(\boldsymbol{p}) = \boldsymbol{p} + \boldsymbol{k} \mod n, k \in \mathcal{K}\}$
- $\mathcal{D} = \{D_{\boldsymbol{k}} \mid D_{\boldsymbol{k}}(\boldsymbol{c}) = \boldsymbol{c} - \boldsymbol{k} \mod n, k \in \mathcal{K}\}$.

Remark 2.18. *Vigenère* 暗号における法 n は英語アルファベットの個数 *26* で表されることも多いが，より一般的には任意のアルファベットで考えられるため，n のままで表記する．

Example 2.5 (Hill 暗号 [15])**.** *Hill* 暗号系 $C_{hill} = (\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ は以下で定める集合により与えられる．

- $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n^m$
- $\mathcal{K} = \{A \in \mathcal{M}_{m,m}(\mathbb{Z}_n) \mid \gcd(\det A, n) = 1\}$
- $\mathcal{E} = \{E_K \mid E_K(\boldsymbol{p}) = K\boldsymbol{p} \mod n, K \in \mathcal{K}\}$
- $\mathcal{D} = \{D_K \mid D_K(\boldsymbol{c}) = K'\boldsymbol{c} \mod n, K \in \mathcal{K}, K' = ((\det K)^{-1}\mathrm{adj}A) \mod n\}$

2.2 距離関数

ここでは，距離関数を定義し，本論文で扱う距離関数について紹介する．

Definition 2.19 (距離関数)**.** X を集合とし，$x, y, z \in X$ とする．以下の性質を満たす関数 $V : X \times X \to \mathbb{R}_+$ を距離関数とよぶ.

1. $V(x, y) = 0 \Leftrightarrow x = y$
2. $V(x, y) = V(y, x)$
3. $V(x, z) \leq V(x, y) + V(y, z)$

一般には距離関数を d と表記することが多いが，本論文では定義 2.3 における条件 6 の式に復号鍵に d を使っているため，混乱を避けるため距離関数を V で表す.

Example 2.6 (ハミング距離)**.** $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}_2^m$ 間の距離 $V_{Hamming} : \{0,1\}^m \times \{0,1\}^m \to \mathbb{R}_+$ を次のように定め，これをハミング距離とよぶ.

$$V_{Hamming}(\boldsymbol{a}, \boldsymbol{b}) := |\{i \in \{1, \cdots, m \mid a_i \neq b_i\}\}|$$

ただし，$\boldsymbol{a} = (a_1, a_2, \cdots, a_m), \boldsymbol{b} = (b_1, b_2, \cdots, b_m) \in \{0,1\}^m$ である．

ハミング距離は 2 つのバイナリ列 $\boldsymbol{a}, \boldsymbol{b}$ における異なるビットの数であり，任意の i で $a_i = b_i$ ならばそのビットについては数えられず，逆に $a_i \neq b_i$ ならば，そのビットはカウントされる．a_i, b_i は 0 か 1 しか取らないことに注意してこれを言い換えると，i 番目の成分の比較結果は $a_i + b_i \mod 2$ で表現することができ，全ての i でで和を取ればハミング距離は以下のように書き換えることができる．

$$\begin{aligned} V_{Hamming}(\boldsymbol{a}, \boldsymbol{b}) &= |\{i \in \{1, 2, \cdots, m\} \mid a_i \neq b_i\}| \\ &= (a_1 + b_1 \mod 2) + \cdots + (a_m + b_m \mod 2) \\ &= \sum_{i=1}^{m} a_i + b_i \mod 2 \end{aligned}$$

すなわち，ハミング距離は，バイナリ列 $\boldsymbol{a}, \boldsymbol{b}$ の和 $\boldsymbol{a} + \boldsymbol{b}$ の成分和で表現できる．

Definition 2.20 (リー距離)**.** $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}_n^m$ 間の距離 $V_{Lee} : \mathbb{Z}_n^m \times \mathbb{Z}_n^m \to \mathbb{R}_+$ を次のように定め，これをリー距離とよぶ.

$$V_{Lee}(\boldsymbol{a}, \boldsymbol{b}) := \sum_{i=1}^{m} \min(|a_i - b_i|, n - |a_i - b_i|)$$

ただし，$\boldsymbol{a} = (a_1, a_2, \cdots, a_m), \boldsymbol{b} = (b_1, b_2, \cdots, b_m) \in \mathbb{Z}_n^m$ である．

3 照合可能暗号のサブクラスについて

本章では，照合可能暗号の定義をした後，照合可能暗号のサブクラスの構成法について考察する．

$V : \mathcal{P} \times \mathcal{P} \to \mathbb{R}_+$ を平文空間上の距離関数とする．

Definition 3.1 (照合可能暗号 [10, 11])**.** 距離関数 V と *2* つの暗号系
$C_1 = (\mathcal{P}, \mathcal{C}, \mathcal{K}^{(1)}, \mathcal{E}^{(1)}, \mathcal{D}^{(1)}), C_2 = (\mathcal{P}, \mathcal{C}, \mathcal{K}^{(2)}, \mathcal{E}^{(2)}, \mathcal{D}^{(2)})$ が与えられているとき，次の条件を満たす $(\mathcal{E}^{(1)}, \mathcal{E}(2))$ を照合可能暗号とよぶ：
任意の $(k_1, k_2) \in \mathcal{K}^{(1)} \times \mathcal{K}^{(2)}$ に対し，ある *2* つの写像 $F : \mathcal{C} \times \mathcal{C} \to \mathcal{C}, G_{k_1,k_2} : \mathcal{C} \to \mathbb{R}_+$ が存在し，すべての平文 $p_1, p_2 \in \mathcal{P}$ に対し次が成り立つ．

$$G_{k_1,k_2}(F(E^{(1)}_{k_1}(p_1), E^{(2)}_{k_2}(p_2))) = V(p_1, p_2).$$

ここで，$E^{(i)} \in \mathcal{E}^{(i)} (i = 1, 2)$ である．

[10] では，例 2.3 などが照合可能暗号クラスに属することを示しており，[11] では，例 2.1, 例 2.3 がもつ性質などを抽出した加法可換群からなる暗号系が照合可能暗号クラスに属することを示している．本論文では，[11] で不十分であったサブクラスに関する議論，特に加法可換群からなる暗号系に関する議論を Affine 線形暗号まで拡張し，サブクラスを構成していく．

Theorem 3.2. *Affine* 線形暗号系は照合可能暗号クラスに属する．すなわち，*Affine* 線形暗号系は暗号化したままリー距離を導出することができる暗号系である．

Proof. 例 2.17 より，Affine 線形暗号系 $C_{alc} = (\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ は次のように暗号系の形で表現できる．

- $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n^m$
- $\mathcal{K} = \mathcal{M}_{m,m}(\mathbb{Z}_n) \times \mathbb{Z}^m$
- $\mathcal{E} = \{E_k : \mathbb{Z}_n^m \to \mathbb{Z}_n^m \mid E_k(\boldsymbol{p}) = A\boldsymbol{p} + \boldsymbol{b} \mod n, k = (A, \boldsymbol{b}) \in \mathcal{K}, \gcd(\det A, n) = 1\}$
- $\mathcal{D} = \{D_k : \mathbb{Z}_n^m \to \mathbb{Z}_n^m \mid D_k(\boldsymbol{c}) = (\det A)^{-1}\mathrm{adj}A(\boldsymbol{c} - \boldsymbol{b}) \mod n, k = (A, \boldsymbol{b}) \in \mathcal{K}\}$

簡単のため，$A' = (\det A)^{-1}\mathrm{adj}A, A' = (a'_{i,j})$ と表すことにする．

$C_1 = C_2 = C_{alc}, V = V_{Lee}$ とする．任意の鍵 $k_1 = (A, \boldsymbol{b}_1), k_2 = (A, \boldsymbol{b}_2)$ をとって，すべての平文 $\boldsymbol{p}_1, \boldsymbol{p}_2 \in \mathcal{P}$ をそれぞれ暗号化したものを $\boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathcal{C}$ とすると，

$$\boldsymbol{c}_1 = A\boldsymbol{p}_1 + \boldsymbol{b}_1 \mod n, \quad \boldsymbol{c}_2 = A\boldsymbol{p}_2 + \boldsymbol{b}_2 \mod n$$

である．ここで，写像 F, G を

$$F(\boldsymbol{c}_1, \boldsymbol{c}_2) := \boldsymbol{c}_1 - \boldsymbol{c}_2 \mod n$$
$$G_{k_1,k_2}(\boldsymbol{c}) := \sum_{i=1}^{m} \min(|v_i|, n - |v_i|)$$
$$(\boldsymbol{v} = A'(\boldsymbol{c} - \boldsymbol{b}) \mod n, \boldsymbol{b} = \boldsymbol{b}_1 - \boldsymbol{b}_2 \mod n \in \mathbb{Z}_n^m)$$

とすれば，主張は真となる．実際,

$$\begin{aligned}\boldsymbol{c} = F(\boldsymbol{c}_1, \boldsymbol{c}_2) &= \boldsymbol{c}_1 - \boldsymbol{c}_2 \mod n \\ &= A\boldsymbol{p}_1 + \boldsymbol{b}_1 - (A\boldsymbol{p}_2 + \boldsymbol{b}_2) \mod n \\ &= A(\boldsymbol{p}_1 - \boldsymbol{p}_2) + (\boldsymbol{b}_1 - \boldsymbol{b}_2) \mod n\end{aligned}$$

とすると,

$$\begin{aligned}\boldsymbol{v} &= A'(\boldsymbol{c} - \boldsymbol{b}) \mod n \\ &= A'(A(\boldsymbol{p}_1 - \boldsymbol{p}_2) + (\boldsymbol{b}_1 - \boldsymbol{b}_2) - (\boldsymbol{b}_1 - \boldsymbol{b}_2)) \mod n \\ &= A'(A(\boldsymbol{p}_1 - \boldsymbol{p}_2)) \mod n \\ &= \boldsymbol{p}_1 - \boldsymbol{p}_2 \mod n\end{aligned}$$

であるので,

$$G_{k_1,k_2}(F(\boldsymbol{c}_1, \boldsymbol{c}_2)) = \sum_{i=1}^{m} \min(|v_i|,\, n - |v_i|)$$

において，すべての i で v_i は $p_{1,i} - p_{2,i}$($\boldsymbol{p}_1$ と $\boldsymbol{p}_2$ の第 i 成分の差) の形をしているので，結局 $\boldsymbol{p}_1$ と $\boldsymbol{p}_2$ 間のリー距離と一致する．

Affine 線形暗号系自体が 1 つの固有の暗号ではなく，Affine 線形性をもつ暗号化関数をもつ暗号系のクラスであるので，結局，Affine 線形暗号系はリー距離を取得可能な照合可能暗号のサブクラスであるといえる． □

Remark 3.3. A は暗号文 $\boldsymbol{c}_1, \boldsymbol{c}_2$ で共通でなければこの定理は成立しないが，$\boldsymbol{b}_1, \boldsymbol{b}_2$ は異なるものであっても構わない．

この定理からいくつかの暗号系単体が照合可能暗号クラスとなる事実を容易に導くことができる．系として，以下のものがある．

Corollary 3.4. 例 *2.1* の *Shift* 暗号系は照合可能暗号クラスに属する．

Proof. Affine 線形暗号において，$m = 1, n = 26$ とすれば，Shift 暗号と一致する． □

Corollary 3.5. 例 *2.2* の *Affine* 暗号系は照合可能暗号クラスに属する．

Proof. Affine 線形暗号において，$m = 1, n = 26$ とすれば，Affine 暗号と一致する． □

Corollary 3.6. 例 *2.3* の *Vernam* 暗号系は照合可能暗号クラスに属する．

Proof. リー距離は $n = 2$ のとき，ハミング距離と一致することと，$\mathbb{Z}_2$ におけるマイナス元は自分自身と一致する，すなわち $a \in \mathbb{Z}_2$ に対して，$-a = a$ であることに注意すれば，Affine 線形暗号において $n = 2, A = E_m$ とすることで，Vernam 暗号と一致する． □

Corollary 3.7. 例 *2.4* の *Vigenère* 暗号系は照合可能暗号クラスに属する．

Proof. Affine 線形暗号の鍵 m 次正方行列 A を，$A = E_m$ として取れば Vigenère 暗号と一致する． □

[12, 13] では，本論文の定理が示される前に，例 2.4 で紹介した Vigenère 暗号が照合可能暗号クラスに属することを示しているが，系 3.7 と一致するため，証明は省略する．

Corollary 3.8. 例 *2.5* の *Hill* 暗号系は照合可能暗号クラスに属する．

Proof. Affine 線形暗号の鍵 m 次元ベクトル $\boldsymbol{b}$ を，$\boldsymbol{b} = \mathbf{0}$ として取れば Hill 暗号と一致する． □

次に，[14] では，リー距離の定義域を $\mathbb{Z}_n^m$ から $\mathbb{Z}_n$ 成分をもつ m 次全行列環 $\mathcal{M}_{m,m}(\mathbb{Z}_n)$ に拡張し，照合可能暗号クラスに属するかどうかを議論している．以下では，[14] の結果を適宜修正し，いくつかの主張を行う．

Definition 3.9 (全行列環上のリー距離)**.** $A, B \in \mathcal{M}_{m,m}(\mathbb{Z}_n)$ 間の写像 $V_{MLee} : \mathcal{M}_{m,m}(\mathbb{Z}_n) \times \mathcal{M}_{m,m}(\mathbb{Z}_n) \to \mathbb{R}_+$ を次のように定め，これを行列環上のリー距離とよぶ.

$$V_{MLee}(A, B) := \sum_{i=1}^{m} \sum_{j=1}^{m} \min(|a_{i,j} - b_{i,j}|,\, n - |a_{i,j} - b_{i,j}|)$$

ただし，$A = (a_{i,j}), B = (b_{i,j}) \in \mathcal{M}_{m,m}(\mathbb{Z}_n)$ である．

Lemma 3.10. 定義 *3.9* の写像 $V_{MLee} : \mathcal{M}_{m,m}(\mathbb{Z}_n) \times \mathcal{M}_{m,m}(\mathbb{Z}_n) \to \mathbb{R}_+$ は距離の公理を満たす.

Proof. 定義 3.9 における写像 V_{MLee} が定義 2.19 の 3 条件を満たすかどうか確かめる．
任意の $A = (a_{i,j}), B = (b_{i,j}) \in \mathcal{M}_{m,m}(\mathbb{Z}_n)$ に対して，$A = {}^t(\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m), B = {}^t(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_m)$ とも表せるとすると，

$$V_{MLee}(A, B) = \sum_{i=1}^{m} \sum_{j=1}^{m} \min(|a_{i,j} - b_{i,j}|,\, n - |a_{i,j} - b_{i,j}| = \sum_{i=1}^{m} V_{Lee}(\boldsymbol{a}_i, \boldsymbol{b}_i)$$

と書き換えられることに注意する．

1. $V_{MLee}(A, B) = 0 \Leftrightarrow A = B$ を示す.
   $V_{MLee}(A, B)$ は行列 A, B の第 i 行ベクトル $\boldsymbol{a}_i, \boldsymbol{b}_i$ に対して，リー距離を取ってから全ての i で和を取ったものであることがわかる．ゆえに，リー距離の性質から $V_{MLee}(A, B) = 0$ ならば，すべての i で $\boldsymbol{a}_i = \boldsymbol{b}_i$ が成り立つ．よって，$A = B$ が言える．逆に，$A = B$ であるとすると，各行ベクトル $\boldsymbol{a}_i, \boldsymbol{b}_i (i \in \{1, \cdots, m\})$ は等しい．したがって，リー距離の性質から $V_{Lee}(\boldsymbol{a}_i, \boldsymbol{b}_i) = 0$ であり，これを i に対して和を取ると，$V_{MLee}(A, B) = 0$ が言える．
2. $V_{MLee}(A, B) = V_{MLee}(B, A)$ を示す.

すべての i に対して，$V_{Lee}(\boldsymbol{a}_i, \boldsymbol{b}_i) = V_{Lee}(\boldsymbol{b}_i, \boldsymbol{a}_i)$ であるので，

$$\begin{aligned} V_{MLee}(A,B) &= \sum_{i=1}^{m}\sum_{j=1}^{m} \min(|a_{i,j}-b_{i,j}|,\, n-|a_{i,j}-b_{i,j}| \\ &= \sum_{i=1}^{m} V_{Lee}(\boldsymbol{a}_i, \boldsymbol{b}_i) \\ &= \sum_{i=1}^{m} V_{Lee}(\boldsymbol{b}_i, \boldsymbol{a}_i) \\ &= \sum_{i=1}^{m}\sum_{j=1}^{m} \min(|b_{i,j}-a_{i,j}|,\, n-|b_{i,j}-a_{i,j}| \\ &= V_{MLee}(B,A). \end{aligned}$$

3. $V_{MLee}(A,C) \leq V_{MLee}(A,B)+V_{MLee}(B,C)$，すなわち，$V_{MLee}(A,B)+V_{MLee}(B,C)-V_{MLee}(A,C) \geq 0$ を示せば良い．

   任意の $A = {}^t(\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m), B = {}^t(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_m), C = {}^t(\boldsymbol{c}_1, \cdots, \boldsymbol{c}_m) \in \mathcal{M}_{m,m}(\mathbb{Z}_n)$ とする．各 $i \in \{1, \cdots, m\}$ に対して，$V_{Lee}(\boldsymbol{a}_i, \boldsymbol{b}_i) + V_{Lee}(\boldsymbol{b}_i, \boldsymbol{c}_i) - V_{Lee}(\boldsymbol{a}_i, \boldsymbol{c}_i) \geq 0$ に注意すると，

$$\begin{aligned} &V_{MLee}(A,B) + V_{MLee}(B,C) - V_{MLee}(A,C) \\ &\quad = \sum_{i=1}^{m} V_{Lee}(\boldsymbol{a}_i, \boldsymbol{b}_i) + \sum_{i=1}^{m} V_{Lee}(\boldsymbol{b}_i, \boldsymbol{c}_i) - \sum_{i=1}^{m} V_{Lee}(\boldsymbol{a}_i, \boldsymbol{c}_i) \\ &\quad = \sum_{i=1}^{m} \{V_{Lee}(\boldsymbol{a}_i, \boldsymbol{b}_i) + V_{Lee}(\boldsymbol{b}_i, \boldsymbol{c}_i) - V_{Lee}(\boldsymbol{a}_i, \boldsymbol{c}_i)\} \geq 0 \end{aligned}$$

距離の公理における 3 つの条件を満たしたので，V_{MLee} は距離関数である． □

Lemma 3.11. 任意の $V \in \mathcal{M}_{m,m}(\mathbb{Z}_n)$ に対し，$f(V) = AV + B \mod n$ を満たす行列 $A, B \in \mathcal{M}_{m,m}(\mathbb{Z}_n)$ が存在するとき，写像 $f : \mathcal{M}_{m,m}(\mathbb{Z}_n) \to \mathcal{M}_{m,m}(\mathbb{Z}_n)$ は *Affine* 線形である．

Proof. 定義より明らかであるが，Affine 線形写像は線形部分 AV と平行移動部分 $+B$ に分けられるので，それらについて考えると，

- 線形部分 AV：任意の $V_1, V_2 \in \mathcal{M}_{m,m}(\mathbb{Z}_n), \lambda \in \mathbb{Z}_n$ に対して，

  $$A(V_1 + V_2) = AV_1 + AV_2, \quad A(\lambda V) = \lambda(AV)$$

  が成り立つ．

- 平行移動部分 $+B$：定数行列 B を加えていることから，平行移動とみなすことができる．

となるので，写像 $f : \mathcal{M}_{m,m}(\mathbb{Z}_n) \to \mathcal{M}_{m,m}(\mathbb{Z}_n), f(V) = AV + B \mod n$ は Affine 線形である． □

Theorem 3.12. 定理 *3.2* は全行列環上に拡張できる．すなわち，全行列環 $\mathcal{M}_{m,m}(\mathbb{Z}_n)$ 上の *Affine* 線形暗号系は全行列環上のリー距離を取得可能であり，照合可能暗号クラスに属する．

Proof. 例2.17のAffine線形暗号系をm次全行列環$\mathcal{M}_{m,m}(\mathbb{Z}_n)$上で再構成すると，$C_{malc} = (\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$は次のように暗号系の形で表現できる．

- $\mathcal{P} = \mathcal{C} = \mathcal{M}_{m,m}(\mathbb{Z}_n)$
- $\mathcal{K} = \mathcal{M}_{m,m}(\mathbb{Z}_n) \times \mathcal{M}_{m,m}(\mathbb{Z}_n)$
- $\mathcal{E} = \{E_K :| E_K(P) = AP + B \mod n, K = (A, B) \in \mathcal{K}, \gcd(\det A, n) = 1\}$
- $\mathcal{D} = \{D_K \mid D_K(C) = (\det A)^{-1}\mathrm{adj}A(C - B) \mod n, K = (A, B) \in \mathcal{K}\}$

簡単のため，$A' = (\det A)^{-1}\mathrm{adj}A, A' = (a'_{i,j})$と表すことにする．

$C_1 = C_2 = C_{malc}, V = V_{MLee}$とする．任意の鍵$K_1 = (A, B_1), K_2 = (A, B_2)$をとって，すべての平文$P_1, P_2 \in \mathcal{P}$をそれぞれ暗号化したものを$C_1, C_2 \in \mathcal{C}$とすると，

$$C_1 = AP_1 + B_1 \mod n, \quad C_2 = AP_2 + B_2 \mod n$$

である．ここで，写像F, Gを

$$\begin{aligned} F(C_1, C_2) &:= C_1 - C_2 \mod n \\ G_{K_1,K_2}(C) &:= \sum_{i=1}^{m}\sum_{j=1}^{m} \min(|v_{i,j}|, n - |v_{i,j}|) \\ &\quad (V = A'(C - B) \mod n, B = B_1 - B_2 \mod n \in \mathcal{M}_{m,m}(\mathbb{Z}_n)) \end{aligned}$$

とすれば，主張は真となる．実際，

$$\begin{aligned} C = F(C_1, C_2) &= C_1 - C_2 \mod n \\ &= AP_1 + B_1 - (AP_2 + B_2) \mod n \\ &= A(P_1 - P_2) + (B_1 - B_2) \mod n \end{aligned}$$

とすると，

$$\begin{aligned} V &= A'(C - B) \mod n \\ &= A'(A(P_1 - P_2) + (B_1 - B_2) \mod n - (B_1 - B_2)) \mod n \\ &= A'(A(P_1 - P_2)) \mod n \\ &= (P_1 - P_2) \mod n \end{aligned}$$

であるので，

$$G_{K_1,K_2}(C) = \sum_{i=1}^{m}\sum_{j=1}^{m} \min(|v_{i,j}|, n - |v_{i,j}|))$$

において，すべてのi, jで$v_{i,j}$は$p_{i,j} - p_{i,j}$(P_1とP_2のi行j列の成分の差)の形をしているので，結局P_1とP_2間の全行列環上のリー距離と一致する．よって，m次全行列環$\mathcal{M}_{m,m}(\mathbb{Z}_n)$上のAffine線形暗号も照合可能暗号クラスに属する． □

4 おわりに

本論文では，照合可能暗号と Affine 線形暗号の関係について，距離関数をリー距離に固定したとき，暗号系と照合可能暗号に関する十分条件を示した．これにより，Affine 線形性をもつ暗号系であれば，暗号化したままリー距離を取得できる，という性質を与えることができる．また，言い換えれば，照合可能暗号の性質として，少なくとも 1 つ Affine 線形性をもつ暗号系を認めるという数学的な性質がわかった．しかし，照合可能暗号クラスの中には Affine 線形性を有さない暗号系も存在するので，今回の結果で必要条件を与えられるわけではない．その他の照合可能暗号に属する暗号系との共通点や，それらも包含するような十分条件の導出も今後試みる．

今回の結果と以前の結果 ([10, 11, 13] など) の発見の共通事項として，照合可能暗号クラスに属する暗号系に関する証明では，与える距離関数は乗算を必要としないもの，すなわち加法のみで構成されている距離関数しか照合可能暗号で扱うことができることがわかっていない．今後の調査では，乗法と加法からなる距離関数，例えばユークリッド距離などが照合可能暗号で扱うことができるか否かなど，距離関数に関する判定条件の導出が必要となる．

さらに，照合可能暗号に属しているか議論されていない暗号，例えば，準同型性をもつ暗号系との関係なども今回の定理では考慮できていないので，後の論文にて，これらについて議論を深め，可能であれば照合可能暗号で扱うことができる暗号系・距離関数の必要十分条件の導出を行いたい．

本論文の結果による工学的効果としては，照合可能暗号をもとにした認証への応用を行うことで，多要素認証の実現や多段階認証のユーザー負担の軽減などが可能性として考えられる．その他にも m 個のデータを一度に比較することができる秘密計算の実現に貢献できると考えられる．

謝辞

照合可能暗号に関する研究は，著者が東京理科大学博士課程在籍時からの研究であり，博士課程・助教時代の指導教員である東京理科大学入山聖史教授には大変多くの助言をいただいた．また，研究成果の一部は入山教授研究室に在籍していた修士課程の学生の小野寺さん，大久保さんの貢献も大きく，それらの研究成果を発展させたものである．

参考文献

[1] RL. Rivest, A. Shamir and L. Adelman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no.2, pp. 120–126, 1978.

[2] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” *IEEE transactions on information theory*, vol. 31, no. 4, pp.469-472, 1985.

[3] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in *Proc. International conference on the theory and applications of cryptographic techniques*, pp. 223-238, 1999.

[4] C. Gentry, “Fully homomorphic encryption using ideal lattices,” in *Proc. the 41st annual ACM symposium on Theory of computing*, pp.169-178, 2009.

[5] A. Shamir, “How to share a secret,” *Communications of the ACM*, vol.22, no. 11, pp. 612-613, 1979.

[6] GR. Blakley, “Safeguarding cryptographic keys,” in *Proc. Managing requirements knowledge, international workshop on*, pp. 313–317, 1979.

[7] R. Canetti, U. Feige, O. Goldreich and M. Naor, “Adaptively secure multi-party computation,” in *Proc. the 28th annual ACM symposium on Theory of computing*, pp. 639–648, 1996.

[8] AC. Yao, “Protocols for secure computations,” in *Proc. 23rd annual symposium on foundations of computer science*, pp. 160-164, 1982.

[9] ACC. Yao, “How to generate and exchange secrets,” in *Proc.27th annual symposium on foundations of computer science*, pp. 162-167, 1986.

[10] M. Kihara and S. Iriyama, “New Authentication Algorithm Based on Verifiable Encryption with Digital Identity,” *Cryptography*, vol. 3, no. 3, pp.1–18, 2019.

[11] M. Kihara and S. Iriyama, “Security and Performance of Single Sign-On Based on One-Time Pad Algorithm,” *Cryptography*, vol. 4 no.2, pp. 1–29, 2020.

[12] T. Onodera, M. Kihara and S. Iriyama, “Note on New Subclass of Verifiable Encryption,” in *poster presented at The Virtual QBIC Workshop 2022*, 2022.

[13] 木原眞紀, 入山聖史. “照合可能暗号を用いた多要素認証についての一考察,” 信学技報, vol. 123, no. 14, pp. 1-5, 2023.

[14] C. Okubo, M. Kihara and S. Iriyama, “Note on A Subclass of Verifiable Encryption over Linear Space,” in *poster presented at The Hybrid QBIC Workshop 2023*, 2023.

[15] J. A. ブーフマン，林芳樹． 暗号理論入門 原書第 *3* 版 暗号アルゴリズム，署名と検証，その数学的基礎. 丸善出版株式会社, 2012.