Computer Security Symposium 2019
21 - 24 October 2019

フィンスラー空間の非対称性を用いた公開鍵暗号方式

永野 哲也[1,a)]　穴田 啓晃[1,b)]

概要：フィンスラー空間が持つ非対称性に基づく新しい公開鍵暗号方式を提案する．フィンスラー空間は，2 点を結ぶ測地線が向きに依存する．それゆえ，2 点 p と q の距離をその測地線の長さで定めると，p から q への距離と，q から p への距離が異なる．加えて，リーマン空間が平行移動に関し対称性を持つのと異なり，フィンスラー空間は q から p への平行移動が p から q への平行移動の逆写像ではないという有用な性質を持つ．本稿で提案する公開鍵暗号はこの平行移動の非対称性を一方向性の根拠とするよう設計する．

キーワード：公開鍵暗号，フィンスラー空間，線形平行移動，リーマン空間

Public-Key Encryption Scheme Using Non-symmetry of Finsler Spaces

Tetsuya Nagano[1,a)]　Hiroaki Anada[1,b)]

Abstract: We propose a new public key encryption scheme which is based on the non-symmetry in Finsler spaces. In Finsler spaces, the geodesic which links two points depends on the direction. Therefore, when we define the distance of two points p and q by the length of the geodesic, the distance from p to q is different from the distance from q to p. Moreover, as is opposed to the case of Riemannian spaces which have the symmetry in a parallel displacement, Finsler spaces have a useful property that the linear parallel displacement from q to p is not the inverse map of the linear parallel displacement from p to q. In this paper, our public key encryption utilizes the non-symmetry of the parallel displacement.

Keywords: Public-Key Encryption, Finsler space, linear parallel displacement, Riemannian space

1. はじめに

公開鍵暗号の数学構造とその安全性を依拠する計算困難問題は様々に研究されている．代表的なものとして，素因数分解及び離散対数とそれら各々の計算困難問題（[11]），格子，誤り訂正符号，多変数多項式，楕円曲線の同種写像及びハッシュ関数とそれら各々の計算困難問題（[12]）などを挙げることが出来る．これらの数学構造と計算困難問題に基づき，種々の公開鍵暗号方式が研究され設計されてきた（[11], [12]）．

[1] 長崎県立大学情報セキュリティ学科
Department of Information Security, University of Nagasaki
[a)] hnagano@sun.ac.jp
[b)] anada@sun.ac.jp

1.1 本稿の貢献

本稿では，幾何学の構造であるフィンスラー空間（[1], [2], [3], [4], [5]）と，その空間における移動の非対称性に関わる計算問題に着目し，これに基づく新しい公開鍵暗号方式を提案する．フィンスラー空間は，2 点を結ぶ最短曲線，すなわち測地線が向きに依存する．それゆえ，2 点 p と q の距離をその測地線の長さで定めると，p から q への距離と，q から p への距離が異なる．加えて，リーマン空間が平行移動に関し対称性を持つのと異なり，フィンスラー空間は q から p への平行移動が p から q への平行移動の逆写像ではないという有用な性質を持つ．言い換えると，これらの合成写像は恒等写像でなく，従って二つの表現行列の積が単位行列でない．本稿では，この平行移動の

© 2019 Information Processing Society of Japan

非対称性を一方向性の根拠とする狙いで公開鍵暗号方式を設計する．

2. フィンスラー空間

最初に，フィンスラー空間について簡単に述べる (cf.[1], [2], [3], [4], [5])．$\mathcal{R}$ を実数の集合とする．
M を n 次元実可微分多様体とし，TM をその接束とする．TM 上の実数値連続関数 $F : TM \longrightarrow \mathcal{R}$ が以下の 4 条件 ((1), (2), (3), (4)) を満たすとき，M と F の組 (M, F) を n 次元（実）フィンスラー空間といい，F をフィンスラー計量または基本関数という．
$x = (x^1, \cdots, x^n) = (x^i) \in M,\ y = (y^1, \cdots, y^n) = (y^i) \in T_xM,\ (x, y) \in TM$ に対して
(1)(正値性)
$\forall (x, y) \in TM,\ F(x, y) \geq 0$ かつ $F(x, y) = 0 \Leftrightarrow y = 0$
(2)(正斉次性)
$\forall (x, y) \in TM \setminus \{0\}, \forall \lambda > 0, \quad F(x, \lambda y) = \lambda F(x, y)$
(3)(可微分性) $F : TM \setminus \{0\} \longrightarrow \mathcal{R}$（可微分）
(4)(正定値性）計量テンソル $g_{ij}(x, y) := \dfrac{1}{2}\dfrac{\partial^2 F^2}{\partial y^i \partial y^j}$ $(i, j = 1, \cdots, n)$ を成分とする対称行列 $G = (g_{ij}(x, y))$ が正定値
＊本論文では対象は $TM \setminus \{0\}$ 上ですべて可微分とする．

本論文で用いるフィンスラー空間について述べる．
M を 2 次元多様体 $\mathcal{R}^2$ のある開領域とし，基本関数 F を

$$F(x, y, \dot{x}, \dot{y}) = \sqrt{a^2\dot{x}^2 + b^2\dot{y}^2} - h_1 x\dot{x} - h_2 y\dot{y}\ (a, b, h_1, h_2 > 0) \tag{1}$$

とする．ただし，$(x, y) \in M,\ (\dot{x}, \dot{y}) \in T_{(x,y)}M$ とする．
基本関数 F は，接空間上で単位球面（基準面）を定めるが，式 (1) の場合は以下のような 2 次曲線である．

$$\frac{(\dot{x} - \frac{h_1 h_2 xy}{a^2 - h1^2 x^2}\dot{y} - \frac{h_1 x}{a^2 - h_1^2 x^2})^2}{\frac{a^2 b^2}{(a^2 - h_1^2 x^2)(a^2 b^2 - b^2 h_1^2 x^2 - a^2 h_2^2 y^2)}} + \frac{(\dot{y} - \frac{a^2 h_2 y}{b^2 h_1^2 x^2 - a^2(b^2 - h_2^2 y^2)})^2}{\frac{a^2 b^2 (a^2 - h_1^2 x^2)}{b^2 h_1^2 x^2 - a^2(b^2 - h_2^2 y^2)}} = 1 \tag{2}$$

これが $T_{(x,y)}M$ の原点 $(0, 0)$ を内部に含む楕円であるための条件が

$$-\frac{a}{h_1} < x < \frac{a}{h_1},\ -\frac{b\sqrt{a^2 - h_1^2 x^2}}{a h_2} < y < \frac{b\sqrt{a^2 - h_1^2 x^2}}{a h_2} \tag{3}$$

である．よって，フィンスラー空間 (M, F) を，式 (3) を満たす楕円の内部とする．このフィンスラー空間 (M, F) では，F のオイラー・ラグランジュ方程式から直線が測地線であることがわかる．ここで，M の原点を通る直線 (測地線) c_m を t をパラメータとして

$$c_m(t) = (c^1(t), c^2(t)) = \left(\frac{1}{a\sqrt{1 + m^2}}t, \frac{m}{b\sqrt{1 + m^2}}t\right) \tag{4}$$

$$p = c_m(t_0),\ q = c_m(t_1),\ r = c_m(t)$$

とおくと，パラメータ t は，式 (3) から

$$\begin{aligned} -min\{\frac{a^2\sqrt{1 + m^2}}{h_1}, \frac{a^2 b^2\sqrt{1 + m^2}}{\sqrt{a^4 h_2^2 m^2 + b^4 h_1^2}}\} < t \\ < min\{\frac{a^2\sqrt{1 + m^2}}{h_1}, \frac{a^2 b^2\sqrt{1 + m^2}}{\sqrt{a^4 h_2^2 m^2 + b^4 h_1^2}}\} \end{aligned} \tag{5}$$

となる．

3. 線形平行移動

曲線に沿う平行移動を考える ([6], [7], [8], [9], [10])．
$c(t) = (c^1(t), c^2(t))$ を M 上の曲線として，以下の $c(t)$ 上の線形常微分方程式系

$$\frac{dv^i}{dt} + \sum_{r,j} F^i_{rj}(c, \dot{c}) v^r \dot{c}^j = 0, \quad (i = 1, 2) \tag{6}$$

$(\dot{c} := (\dot{c}^1, \dot{c}^2) = (\frac{dc^1}{dt}, \frac{dc^2}{dt}))$ の解 $v(t) = (v^1(t), v^2(t))$ を $c(t)$ 上の平行ベクトル場という．ここで，$\sum$ は断りがない限り 1 から $dimM(= 2)$ まで和をとるものとする．$v(t)$ により定まる始点 $p = c(t_0)$ と終点 $q = c(t_1)$ のそれぞれの接空間 T_pM, T_qM 間の線形写像 Π_c

$$\Pi_c : v(t_0) \in T_pM \ \rightarrow\ v(t_1) \in T_qM \tag{7}$$

を p から q への c に沿う線形平行移動という．
式 (6) の F^i_{rj} は接続係数と呼ばれ以下で定まる．

$$F^i_{rj} := \frac{1}{2}\sum_k g^{ik}\left(\frac{\delta g_{rk}}{\delta x^j} + \frac{\delta g_{kj}}{\delta x^r} - \frac{\delta g_{jr}}{\delta x^k}\right) \quad ((g^{ij}) = (g_{ij})^{-1}) \tag{8}$$

ただし，$\dfrac{\delta}{\delta x^i} := \dfrac{\partial}{\partial x^i} - \sum_k N^k_i \dfrac{\partial}{\partial y^k}$ で N^i_j は非線形接続の係数である．

注意 3.1 (1) 線形平行移動は向きに依存する．
平行ベクトル場 $v(t)$ の逆ベクトル場 $v^{-1}(\tau)(\tau = a + b - t)$ は，必ずしも，逆曲線 $c^{-1}(\tau)$ に沿う平行ベクトル場にならない (平行移動の非対称性)．初期ベクトル v_0 を線形平行移動で p から q まで移動し，続いて，同じ曲線を q から p へ線形平行移動した場合，一般に，v_0 に戻らない．
(2) 曲線に沿う内積の保存・非保存
$v(t) = (v^i(t)), u(t) = (u^i(t))$ を曲線 c に沿う平行ベクトル場とするとき，$< v, u >_{\dot{c}} := g_{ij}(c, \dot{c}) v^i u^j$ を v, u の c に沿う内積という．曲線に沿う内積は, 一般に保存されない．しかし，曲線が測地線ならば保存される． すなわち，測地線上で，内積は一定である．

式 (4) で表される測地線 $c_m(t)$ 上の線形平行移動を求める．
平行ベクトル場 $v(t) = (v^1(t), v^2(t))$ の満たすべき方程式は式 (4), (8) より

$$\sum_j F^1_{1j}\dot{c}^j = \frac{1}{2\left(a^2\left(h_2m^2t-b^2\left(m^2+1\right)\right)+b^2h_1t\right)^2}\times$$
$$\left(a^4h_2m^4\left(h_2t-b^2\right)+a^2b^2h_1\left(3h_2m^2t-b^2\left(3m^2+2\right)\right)\right.$$
$$\left.+2b^4h_1^2t\right) \tag{9}$$

$$\sum_j F^1_{2j}\dot{c}^j = \frac{1}{2\left(a^2\left(h_2m^2t-b^2\left(m^2+1\right)\right)+b^2h_1t\right)^2}\times$$
$$\left(abm\left(b^2h_2\left(h_1t-a^2\left(m^2+2\right)\right)+a^2h_2^2m^2t+b^4h_1\right)\right) \tag{10}$$

$$\sum_j F^2_{1j}\dot{c}^j = \frac{1}{2\left(a^2\left(h_2m^2t-b^2\left(m^2+1\right)\right)+b^2h_1t\right)^2}\times$$
$$\left(abm\left(a^4h_2m^2+h_1t\left(a^2h_2m^2+b^2h_1\right)\right.\right.$$
$$\left.\left.-a^2b^2h_1\left(2m^2+1\right)\right)\right) \tag{11}$$

$$\sum_j F^2_{2j}\dot{c}^j = \frac{1}{2\left(a^2\left(h_2m^2t-b^2\left(m^2+1\right)\right)+b^2h_1t\right)^2}\times$$
$$\left(a^4h_2m^2\left(2h_2m^2t-b^2\left(2m^2+3\right)\right)-a^2b^2h_1\left(b^2-3h_2m^2t\right)\right.$$
$$\left.+b^4h_1^2t\right) \tag{12}$$

であるので，式 (6) を解いて，曲線 $c_m(t)$ 上の点 $p=c_m(t_0)$ から点 $r=c_m(t_0+t)(t\le t_1)$ への線形平行移動 Π_{c_m} は，以下の行列で表される．

$$\Pi_{c_m}(t)=\begin{pmatrix}B^1_1 & B^1_2\\ B^2_1 & B^2_2\end{pmatrix} \tag{13}$$

ただし，

$$B^1_1 = -\frac{1}{\left(a^2\left(b^2\left(m^2+1\right)-h_2m^2(t+t_0)\right)-b^2h_1(t+t_0)\right)^{3/2}}\times$$
$$\left(a^2\left(h_2m^2(t+t_0)\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2t_0\right)-b^2h_1t_0}\right.\right.$$
$$-b^2\left(\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2(t+t_0)\right)-b^2h_1(t+t_0)}\right.$$
$$\left.\left.+m^2\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2t_0\right)-b^2h_1t_0}\right)\right)$$
$$\left.+b^2h_1t_0\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2(t+t_0)\right)-b^2h_1(t+t_0)}\right)$$

$$B^1_2 = \frac{1}{\left(a^2\left(b^2\left(m^2+1\right)-h_2m^2(t+t_0)\right)-b^2h_1(t+t_0)\right)^{3/2}}\times$$
$$\left(abm\left(b^2\left(\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2(t+t_0)\right)-b^2h_1(t+t_0)}\right.\right.\right.$$
$$\left.-\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2t_0\right)-b^2h_1t_0}\right)$$
$$+h_2\left(t\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2t_0\right)-b^2h_1t_0}\right.$$
$$+t_0\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2t_0\right)-b^2h_1t_0}$$
$$\left.\left.\left.-t_0\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2(t+t_0)\right)-b^2h_1(t+t_0)}\right)\right)\right)$$

$$B^2_1 = \frac{1}{\left(a^2\left(b^2\left(m^2+1\right)-h_2m^2(t+t_0)\right)-b^2h_1(t+t_0)\right)^{3/2}}\times$$
$$\left(abm\left(a^2\left(\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2(t+t_0)\right)-b^2h_1(t+t_0)}\right.\right.\right.$$
$$\left.-\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2t_0\right)-b^2h_1t_0}\right)$$
$$+h_1\left(t\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2t_0\right)-b^2h_1t_0}\right.$$
$$+t_0\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2t_0\right)-b^2h_1t_0}$$
$$\left.\left.\left.-t_0\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2(t+t_0)\right)-b^2h_1(t+t_0)}\right)\right)\right)$$

$$B^2_2 = -\frac{1}{\left(a^2\left(b^2\left(m^2+1\right)-h_2m^2(t+t_0)\right)-b^2h_1(t+t_0)\right)^{3/2}}\times$$
$$\left(-a^2b^2\left(m^2\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2(t+t_0)\right)-b^2h_1(t+t_0)}\right.\right.$$
$$\left.+\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2t_0\right)-b^2h_1t_0}\right)$$
$$+h_1(t+t_0)\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2t_0\right)-b^2h_1t_0}$$
$$\left.+a^2h_2m^2t_0\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2(t+t_0)\right)-b^2h_1(t+t_0)}\right)$$

次に，平行ベクトルのエネルギーについて述べる．
$v=(v^1,v^2)$ を平行ベクトルとするとき，その内積，すなわち，

$$E(v) :=< v,v >_{\dot{c}}=\sum_{i,j} g_{ij}(c,\dot{c})v^iv^j = {}^tvGv \tag{14}$$

を，v の c に沿うエネルギーという．
注意 3.1 で述べたように，測地線上では，エネルギー $E(v)$ は一定である．式 (4) の測地線上の G は

$$g_{11} = \frac{1}{a^2b^2\left(m^2+1\right)^2}(b^2m^4a^4+b^2a^4+2b^2m^2a^4$$
$$-(h_2m^4a^4+3b^2h_1m^2a^2+2b^2h_1a^2)t+(b^2h_1^2+b^2h_1^2m^2)t^2)$$
$$g_{12} = -\frac{\left(h_2a^2m+b^2h_1m^3\right)t-\left(h_1h_2m^3+h_1h_2m\right)t^2}{ab\left(m^2+1\right)^2}$$
$$g_{21} = g_{12}$$
$$g_{22} = \frac{1}{a^2b^2\left(m^2+1\right)^2}(a^2m^4b^4+a^2b^4+2a^2m^2b^4$$
$$-(h_1b^4+2a^2h_2m^4b^2+3a^2h_2m^2b^2)t+(a^2h_2^2m^4+a^2h_2^2m^2)t^2)$$

である．
次節で，Π_{c_m} と G を用いて，公開鍵暗号方式を提案する．

4. 公開鍵

前節の Π_{c_m}, G に対して，空間のパラメータ a,b,h_1,h_2 と測地線のパラメータ m,t_0,t_1 を与えることにより，鍵を作成する．はじめに，

$$e := min\{\frac{a^2\sqrt{1+m^2}}{h_1},\frac{a^2b^2\sqrt{1+m^2}}{\sqrt{a^4h_2^2m^2+b^4h_1^2}}\}$$

とおき，

$\widetilde{\mathcal{R}}_+ := \{r\in\mathcal{R}|r$: 整数部分 n_1 桁, 小数部分 n_2 桁の正の 10 進数 $\}$

とする（量子化）．
＜鍵の生成＞
1. $a\in_R\widetilde{\mathcal{R}}_+$, $b\in_R\widetilde{\mathcal{R}}_+$, $h_1\in_R\widetilde{\mathcal{R}}_+$, $h_2\in_R\widetilde{\mathcal{R}}_+$, $m\in_R$

$\widetilde{\mathcal{R}}_+$, $t_1 \in_R \widetilde{\mathcal{R}}_+$, $t_0 \in_R \widetilde{\mathcal{R}}_+$ とする．ただし，$0 < t_1 \leq e$, $0 < t_0 < t_1$ である．

2．**公開鍵 1**$(PK1)$：値 a, b, h_1, m, t_0 を Π_{c_m} に代入

$$PK1 := \Pi_{c_m}(a, b, h_1, m, t_0) \text{ (成分は } h_2, t \text{ の式)}$$

公開鍵 2$(PK2)$：G の t を $t_0 + t$ に変更し，値 a, b, h_1, h_2, m, t_0 を G に代入

$$PK2 := {}^tPK1 \cdot G(a, b, h_1, h_2, m, t_0+t) \cdot PK1 \text{ (成分は } h_2, t \text{ の式)}$$

さらに，$\Delta t := t_1 - t_0$ とおく．秘密鍵 SK と公開鍵 PK を次のとおりにおく．

$$SK := (a, b, h_1, h_2, m, t_0, t_1), \tag{15}$$

$$PK := (PK1, PK2, \Delta t). \tag{16}$$

5. 暗号化と復号

平文：初期ベクトル $v(t_0) = (v_0^1, v_0^2) \in \widetilde{\mathcal{R}}_+^2$

秘密鍵：SK　公開鍵：PK

＜暗号化＞

発信者アリスは$t \in_R \widetilde{\mathcal{R}}_+ (t < \Delta t)$ を指定し，$v(t_0)$ を

$$v(t_0 + t) := PK1(t)v(t_0) \tag{17}$$

と暗号化（$v(t_0+t)$ の成分は，h_2 の式）する．さらに $v(t_0)$ のエネルギーを

$$E(v(t_0)) := {}^tv(t_0)PK2(t)v(t_0) \tag{18}$$

と計算 (値は h_2 の式) して

暗号文：$\{v(t_0 + t),\ E(v(t_0))\}$

を作成する．

＜復号＞

受信者ボブは，形式的平文 $\bar{v}_0 := PK1^{-1}v(t_0 + t)$ とエネルギー $E(v(t_0))$ にそれぞれh_2 の値を与え，エネルギー方程式（t の 2 次方程式）

$${}^t\bar{v}_0 G(a, b, h_1, h_2, m, t_0)\bar{v}_0 = E(v(t_0)) \tag{19}$$

を作成し，これを $0 < t < \Delta t$ の範囲で解いて，t の値を得る．値 t から

$$v(t_0) = PK1^{-1}(t)v(t_0 + t) \tag{20}$$

として，平文 $v(t_0)$ を得る．

6. 暗号文の非可解性

1．エネルギー方程式の非可解性

$PK1$ の逆行列から形式的平文 $\bar{v}_0 := PK1^{-1}v(t_0 + t)$ を求めエネルギーの式に代入しても，得られる t の方程式

$${}^t\bar{v}_0 PK2\bar{v}_0 = E(v(t_0))$$

には未知パラメータ h_2 が含まれるため，数学的に解くことは不可能である．

2．パラメータ (a, b, h_1, h_2, m, t_0) の非決定性

公開鍵 $PK2$ から，G の 4 成分 $g_{11}, g_{12}, g_{21}, g_{22}$ が公開されているが，$g_{12} = g_{21}$ なので独立な値は 3 つであり，含まれる 6 パラメータ a, b, h_1, h_2, m, t_0 を決定することはできない．

さらに，Π_{c_m} が非対称であるため，逆曲線 $c^{-1}(\tau) = c(a + b - \tau)$ に沿う逆ベクトル場 $v^{-1}(\tau) = v(a + b - \tau)$ は平行ベクトル場ではない．すなわち，

$$\Pi_{c_m^{-1}} \circ \Pi_{c_m} \neq I \text{ (恒等変換)}$$

であるので，6 パラメータ a, b, h_1, h_2, m, t_0 に関する情報は得られない．

リーマン空間のように平行移動が対称ならば，逆ベクトル場 $v^{-1}(\tau)$ も平行ベクトル場であるので，その行列 $\Pi_{c_m^{-1}}$ は

$$\Pi_{c_m^{-1}} = \Pi_{c_m}^{-1} \quad \text{すなわち} \quad \Pi_{c_m^{-1}} \circ \Pi_{c_m} = I \text{ (恒等変換)}$$

を満たす．これから，a, b, h_1, h_2, m, t_0 に関する情報が得られる．得られる情報と $PK2$ の成分から 6 パラメータ a, b, h_1, h_2, m, t_0 が決定される．

注意 6.1　上で述べたように，このシステムには，量子化前においてパラメータを決定するアルゴリズムが存在しない．量子化後についても，公開鍵 PK から秘密鍵 SK を復元するアルゴリズムは全数探索以外には無いものと考えられる．それゆえ，写像

$$f : SK \longrightarrow PK$$

は一方向関数と考えられる．

7. 例

パラメータ (a, b, h_1, h_2, m) をランダムに選んだ例を以下に示す．

秘密鍵

$$a = 2,\ b = 3,\ h_1 = 3,\ h_2 = 1,\ m = 2$$

とする．

$$\frac{a^2\sqrt{1+m^2}}{h_1} = \frac{4\sqrt{5}}{3},\ \frac{a^2b^2\sqrt{1+m^2}}{\sqrt{a^4h_2^2m^2 + b^4h_1^2}} = \frac{36\sqrt{5}}{\sqrt{793}}$$

$\frac{4\sqrt{5}}{3} > \frac{36\sqrt{5}}{\sqrt{793}}$ より $e = \frac{36\sqrt{5}}{\sqrt{793}}$

$$t_1 = e = \frac{36\sqrt{5}}{\sqrt{793}} \fallingdotseq 2.85858$$

とする． ここで

$$t_0 = 2(< t_1)$$

をとる．

$$\text{秘密鍵：}\ SK = \left(2,\ 3,\ 3,\ 1,\ 2,\ 2,\ \frac{36\sqrt{5}}{\sqrt{793}}\right)$$

$$\Delta t \fallingdotseq 0.85858$$

公開鍵

4 節の鍵の生成に即して，上記秘密鍵 SK を適用して，公開鍵 PK が以下のように定まる．

$$PK1 = \begin{pmatrix} C_1^1 & C_2^1 \\ C_1^2 & C_2^2 \end{pmatrix}$$

$$C_1^1 = \frac{1}{(-27t-16h_2(t+2)+126)^{3/2}}\left(-2\left(8\sqrt{126-32h_2}h_2(t+2)\right.\right.$$
$$\left.\left.+9\left(\sqrt{-27t-16h_2(t+2)+126}-8\sqrt{126-32h_2}\right)\right)\right)$$
$$C_2^1 = \frac{1}{(-27t-16h_2(t+2)+126)^{3/2}}\left(12\left(h_2\left(\sqrt{126-32h_2}t\right.\right.\right.$$
$$\left.\left.+2\sqrt{126-32h_2}-2\sqrt{-27t-16h_2(t+2)+126}\right)-9\sqrt{126-32h_2}\right.$$
$$\left.\left.+9\sqrt{-27t-16h_2(t+2)+126}\right)\right)$$
$$C_1^2 = \frac{1}{(-27t-16h_2(t+2)+126)^{3/2}}\left(12\left(3\sqrt{126-32h_2}t\right.\right.$$
$$\left.\left.+2\sqrt{126-32h_2}-2\sqrt{-27t-16h_2(t+2)+126}\right)\right)$$
$$C_2^2 = \frac{1}{(-27t-16h_2(t+2)+126)^{3/2}}\times$$
$$\left(-32\sqrt{-16th_2-32h_2-27t+126}h_2-27\sqrt{2}\sqrt{63-16h_2}t\right.$$
$$\left.-18\sqrt{2}\sqrt{63-16h_2}+144\sqrt{-16th_2-32h_2-27t+126}\right)$$

* $PK2$ は最終項に付録として記す．

平文

$v(t_0) = (1254, 2213)$

t の選択

$0 < t < \Delta t \fallingdotseq 0.85858$ から

$$t = \frac{1}{3} \fallingdotseq 0.33333$$

暗号化

$$v(t_0+t) = PK1(1/3)v(t_0)$$
$$= \left(\frac{-1}{(351-112h_2)^{3/2}}\left(12\left(13278\sqrt{351-112h_2}h_2\right.\right.\right.$$
$$-3787\sqrt{378-96h_2}h_2-54108\sqrt{351-112h_2}$$
$$\left.\left.\left.+14607\sqrt{378-96h_2}\right)\right),\right.$$
$$\frac{-1}{(351-112h_2)^{3/2}}\left(212448\sqrt{351-112h_2}h_2\right.$$
$$\left.\left.-865728\sqrt{351-112h_2}+43821\sqrt{378-96h_2}\right)\right)$$

$$E(v(t_0)) = {}^t v(t_0)PK2(1/3)v(t_0)$$
$$= \frac{1}{450(112h_2-351)^3}\left(5179488883442944h_2^3\right.$$
$$-8652833894880\sqrt{6}\sqrt{351-112h_2}\sqrt{63-16h_2}h_2^2$$
$$-58094172204065136h_2^2+215999608780441008h_2$$
$$+43913229766560\sqrt{6}\sqrt{351-112h_2}\sqrt{63-16h_2}h_2$$
$$-35260395871680\sqrt{6}\sqrt{351-112h_2}\sqrt{63-16h_2}$$
$$\left.-265926033515761713\right)$$

$$\text{暗号文：}\ \{v(t_0+t), E(v(t_0))\}$$

復号

$\underline{h_2 = 1 \text{ として}}$，形式的平文 $\bar{v}_0 = PK1^{-1}v(t_0+t)$

$$= \left(\frac{1}{2684687}\left(6\left(\left(335961\sqrt{67398}-419609910\right)t\right.\right.\right.$$
$$\left.\left.-905093\sqrt{717}\sqrt{94-43t}-111987\sqrt{67398}+917286780\right)\right),$$
$$\frac{1}{2684687}\left(3\left(8\left(111987\sqrt{67398}-139869970\right)t\right.\right.$$
$$\left.\left.\left.-387897\sqrt{717}\sqrt{94-43t}-298632\sqrt{67398}+2446098080\right)\right)\right)$$

とエネルギー $E(v(t_0)) = \dfrac{7533088063}{450}$ を用いて，次のエネルギー等式が得られる．

平文のエネルギー等式

$${}^t\bar{v}_0 \cdot G(a,b,h_1,h_2,m,t_0)\cdot\bar{v}_0 = E(v(t_0))\ \ (t \text{ の 2 次方程式})$$

$$G(a,b,h_1,h_2,m,t_0) = \begin{pmatrix} \frac{421}{225} & -\frac{164}{75} \\ -\frac{164}{75} & \frac{2383}{450} \end{pmatrix}\quad \text{から}$$

$$\frac{1}{682595950}\left(80\left(42696344703379-65538152010\sqrt{67398}\right)t^2\right.$$
$$+(13209239940000\sqrt{67398}-14510971413599143)t$$
$$\left.+94\left(168981459480461-40643815200\sqrt{67398}\right)\right) = \frac{7533088063}{450}$$

を解くと

$$t = \frac{1}{3} \fallingdotseq 0.33333,$$
$$t = \frac{-40117206664527109+34384667659200\sqrt{67398}}{-10247122728810960+15729156482400\sqrt{67398}} \fallingdotseq 5.0604$$

$0 < t < \Delta t \fallingdotseq 0.85858$ より $t = \dfrac{1}{3}$ が求める t の値である．よって，形式的平文 $\bar{v}_0$ に $t = \frac{1}{3}$ を代入し，平文 $v(t_0)$ を得る．

$$v(t_0) = (1254, 2213)$$

注意 7.1 公開鍵 PK では，パラメータ h_2 を秘匿したが，秘匿するパラメータは他のパラメータでも，更に複数個でも同様のシステムを作ることができる．

8. むすび

本稿では，幾何学の構造であるフィンスラー空間と，その空間における平行移動の非対称性の計算問題を用い，公開鍵暗号方式を設計した．上述の計算問題の計算量を評価することは今後の課題である．また，一方向安全性を証明可能安全の枠組みにおいて証明することは今後の課題である．

参考文献

[1] T.Aikou and L.Kozma: *Global aspects of Finsler geometry. In Handbook of global analysis*, pages 1-39, 1211. Elsevier Sci. B. V., Amsterdam (2008).

[2] S.-S. Chern and Z.Shen: *Riemann-Finsler geometry*, volume 6 of Nankai Tracts in Mathematics. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ (2005).

[3] M. Crampin: Randers spaces with reversible geodesics, Publ. Math.Debrecen, 67(3-4):401-409 (2005).

[4] M. Matsumoto: *Foundations of Finsler geometry and special Finsler spaces*. Kaiseisha Press, Shigaken, 1986.

[5] M. Matsumoto: *Finsler geometry in the 20th-century. In Handbook of Finsler geometry*, Vol. 1, 2, pages 557-966. Kluwer Acad. Publ., Dordrecht, 2003.

[6] T. Nagano, N. Innami, Y. Itokawa and K. Shiohama: Notes on reversibilty and branching geodesics in Finsler spaces, Iasi Ploytechic Inst. Bull.-Mathematics. Theoretical Mechanics. Physics Section, to appear (2019).

[7] T. Nagano: Notes on the notion of the parallel displacement in Finsler geometry. Tensor (N.S.), 70(3):302-310 (2008).

[8] T. Nagano: On the parallel displacement and parallel vector fields in Finsler geometry, Acta Math. Acad. Paedagog. Nyhazi., 26(2):349-358 (2010).

[9] T. Nagano: A note on linear parallel displacements in Finsler geometry, Journal of the Faculty of Global Communication, University of Nagasaki, 12:195-205 (2011).

[10] T. Nagano: On the quantities W, L, K derived from linear parallel displacements in Finsler geometry, Journal of the Faculty of Global Communication, University of Nagasaki, 14:123-132 (2013).

[11] J. Katz and Y. Lindell: *Introduction to Modern Cryptography, Second Edition*, CRC Press, Florida (2014).

[12] 岡本龍明: 現代暗号の誕生と発展, 近代科学社, 東京 (2019).

付　　録

$PK2$

$$
\begin{pmatrix}
\frac{1}{225(16h_2t+32h_2+27t-126)^3}\left(829440h_2^3t^4+3014656h_2^3t^3+5554176h_2^3t^2+12582912h_2^3t+13795328h_2^3-4924800h_2^2t^4\right.\\
-25473024h_2^2t^3-15012864h_2^2t^2-44679168h_2^2t-154294272h_2^2+7361280h_2t^4+55303632h_2t^3\\
-92880\sqrt{2}\sqrt{63-16h_2}h_2t^3\sqrt{-16h_2t-32h_2-27t+126}+92880\sqrt{2}\sqrt{63-16h_2}t^3\sqrt{-16h_2t-32h_2-27t+126}+24174432h_2t^2\\
-44640\sqrt{2}\sqrt{63-16h_2}h_2t^2\sqrt{-16h_2t-32h_2-27t+126}+44640\sqrt{2}\sqrt{63-16h_2}t^2\sqrt{-16h_2t-32h_2-27t+126}-187788096h_2t\\
+417600\sqrt{2}\sqrt{63-16h_2}h_2t\sqrt{-16h_2t-32h_2-27t+126}-417600\sqrt{2}\sqrt{63-16h_2}t\sqrt{-16h_2t-32h_2-27t+126}\\
+270720\sqrt{2}\sqrt{63-16h_2}h_2\sqrt{-16h_2t-32h_2-27t+126}-270720\sqrt{2}\sqrt{63-16h_2}\sqrt{-16h_2t-32h_2-27t+126}+598870656h_2\\
\left.-3265920t^4+627183t^3-234232722t^2+699758676t-808047576\right)\\
-\frac{1}{75(16h_2t+32h_2+27t-126)^3}\left(2\left(103680h_2^3t^4+376832h_2^3t^3+694272h_2^3t^2+1572864h_2^3t+1724416h_2^3-615600h_2^2t^4\right.\right.\\
-3479968h_2^2t^3+10320\sqrt{2}\sqrt{63-16h_2}h_2^2t^3\sqrt{-16h_2t-32h_2-27t+126}-1174848h_2^2t^2\\
+4960\sqrt{2}\sqrt{63-16h_2}h_2^2t^2\sqrt{-16h_2t-32h_2-27t+126}-4411776h_2^2t-46400\sqrt{2}\sqrt{63-16h_2}h_2^2t\sqrt{-16h_2t-32h_2-27t+126}\\
-30080\sqrt{2}\sqrt{63-16h_2}h_2^2\sqrt{-16h_2t-32h_2-27t+126}-22114304h_2^2+920160h_2t^4+7578594h_2t^3\\
-62565\sqrt{2}\sqrt{63-16h_2}h_2t^3\sqrt{-16h_2t-32h_2-27t+126}+52245\sqrt{2}\sqrt{63-16h_2}t^3\sqrt{-16h_2t-32h_2-27t+126}+4771044h_2t^2\\
-30070\sqrt{2}\sqrt{63-16h_2}h_2t^2\sqrt{-16h_2t-32h_2-27t+126}+25110\sqrt{2}\sqrt{63-16h_2}t^2\sqrt{-16h_2t-32h_2-27t+126}-40664232h_2t\\
+281300\sqrt{2}\sqrt{63-16h_2}h_2t\sqrt{-16h_2t-32h_2-27t+126}-234900\sqrt{2}\sqrt{63-16h_2}t\sqrt{-16h_2t-32h_2-27t+126}\\
+182360\sqrt{2}\sqrt{63-16h_2}h_2\sqrt{-16h_2t-32h_2-27t+126}-152280\sqrt{2}\sqrt{63-16h_2}\sqrt{-16h_2t-32h_2-27t+126}+97125552h_2\\
\left.\left.-408240t^4+2044116t^3-47046744t^2+136970352t-144843552\right)\right)\\
=\quad
-\frac{1}{75(16h_2t+32h_2+27t-126)^3}\left(2\left(103680h_2^3t^4+376832h_2^3t^3+694272h_2^3t^2+1572864h_2^3t+1724416h_2^3-615600h_2^2t^4\right.\right.\\
-3479968h_2^2t^3+10320\sqrt{2}\sqrt{63-16h_2}h_2^2t^3\sqrt{-16h_2t-32h_2-27t+126}-1174848h_2^2t^2\\
+4960\sqrt{2}\sqrt{63-16h_2}h_2^2t^2\sqrt{-16h_2t-32h_2-27t+126}-4411776h_2^2t-46400\sqrt{2}\sqrt{63-16h_2}h_2^2t\sqrt{-16h_2t-32h_2-27t+126}\\
-30080\sqrt{2}\sqrt{63-16h_2}h_2^2\sqrt{-16h_2t-32h_2-27t+126}-22114304h_2^2+920160h_2t^4+7578594h_2t^3\\
-62565\sqrt{2}\sqrt{63-16h_2}h_2t^3\sqrt{-16h_2t-32h_2-27t+126}+52245\sqrt{2}\sqrt{63-16h_2}t^3\sqrt{-16h_2t-32h_2-27t+126}+4771044h_2t^2\\
-30070\sqrt{2}\sqrt{63-16h_2}h_2t^2\sqrt{-16h_2t-32h_2-27t+126}+25110\sqrt{2}\sqrt{63-16h_2}t^2\sqrt{-16h_2t-32h_2-27t+126}-40664232h_2t\\
+281300\sqrt{2}\sqrt{63-16h_2}h_2t\sqrt{-16h_2t-32h_2-27t+126}-234900\sqrt{2}\sqrt{63-16h_2}t\sqrt{-16h_2t-32h_2-27t+126}\\
+182360\sqrt{2}\sqrt{63-16h_2}h_2\sqrt{-16h_2t-32h_2-27t+126}-152280\sqrt{2}\sqrt{63-16h_2}\sqrt{-16h_2t-32h_2-27t+126}+97125552h_2\\
\left.\left.-408240t^4+2044116t^3-47046744t^2+136970352t-144843552\right)\right)\\
\frac{1}{450(16h_2t+32h_2+27t-126)^3}\left(933120h_2^3t^4+8124928h_2^3t^3-4979712h_2^3t^2-4614144h_2^3t+60760064h_2^3-5540400h_2^2t^4\right.\\
-63270432h_2^2t^3+185760\sqrt{2}\sqrt{63-16h_2}h_2^2t^3\sqrt{-16h_2t-32h_2-27t+126}+11965248h_2^2t^2\\
+89280\sqrt{2}\sqrt{63-16h_2}h_2^2t^2\sqrt{-16h_2t-32h_2-27t+126}+319810176h_2^2t-835200\sqrt{2}\sqrt{63-16h_2}h_2^2t\sqrt{-16h_2t-32h_2-27t+126}\\
-541440\sqrt{2}\sqrt{63-16h_2}h_2^2\sqrt{-16h_2t-32h_2-27t+126}-758877696h_2^2+8281440h_2t^4+84681936h_2t^3\\
-1021680\sqrt{2}\sqrt{63-16h_2}h_2t^3\sqrt{-16h_2t-32h_2-27t+126}+835920\sqrt{2}\sqrt{63-16h_2}t^3\sqrt{-16h_2t-32h_2-27t+126}+453167136h_2t^2\\
-491040\sqrt{2}\sqrt{63-16h_2}h_2t^2\sqrt{-16h_2t-32h_2-27t+126}+401760\sqrt{2}\sqrt{63-16h_2}t^2\sqrt{-16h_2t-32h_2-27t+126}-2395718208h_2t\\
+4593600\sqrt{2}\sqrt{63-16h_2}h_2t\sqrt{-16h_2t-32h_2-27t+126}-3758400\sqrt{2}\sqrt{63-16h_2}t\sqrt{-16h_2t-32h_2-27t+126}\\
+2977920\sqrt{2}\sqrt{63-16h_2}h_2\sqrt{-16h_2t-32h_2-27t+126}-2436480\sqrt{2}\sqrt{63-16h_2}\sqrt{-16h_2t-32h_2-27t+126}+3178735488h_2\\
\left.-3674160t^4+159928749t^3-1702691766t^2+4796770428t-4459899528\right)
\end{pmatrix}
$$