2次元フィンスラー空間の例と暗号システムへの試み

永野哲也　(長崎県立大学)*

概　　要

2次元フィンスラー空間の具体例を3つ提示し、その中の1つを用いて公開鍵暗号の可能性と具体例を示した。

はじめに

一般に、フィンスラー空間は種々の非対称性を持つ。フィンスラー空間では、幾何的対象に向きを込めて扱う。例えば、点pとqを結ぶ曲線cは、pからqへ向かうか、逆にqからpへ向かうかの2つ存在する。よって、同じ像を持つ曲線でもpからqへ向かう曲線の長さ（弧長）と、qからpへ向かう弧長が異なる。また2点間の最短曲線として測地線というものがあるが、2点p,qを結ぶ測地線は像がそもそも一般に異なる。第1節で2点を結ぶ測地線の像が異なる例、一致する例、片側だけ一致する例の3つを示す。第2節で例その2を用いて、公開鍵暗号の具体例を示す。

1. 2次元フィンスラー空間の具体例

$M \subset \mathcal{R}^2$, (x,y): $\mathcal{R}^2$の座標系, $(\dot{x},\dot{y})$: $T_{(x,y)}M$の座標系, $(x,y,\dot{x},\dot{y})$: TMの座標系

例　その1　基本関数: $F(x,y,\dot{x},\dot{y}) = \sqrt{\dot{x}^2+\dot{y}^2} - y\dot{x}$　(図1参照)

単位球面（基準面）: $\dfrac{(\dot{x}-\dfrac{y}{1-y^2})^2}{\dfrac{1}{(1-y^2)^2}} + \dfrac{\dot{y}^2}{\dfrac{1}{1-y^2}} = 1 \quad \mathrm{on} T_{(x,y)}M$

$M = \{(x,y) | -1 < y < 1\}$

測地線:

$$\begin{cases} x(t) &= a\cos t + b\sin t + c_1 \\ y(t) &= b\cos t - a\sin t + c_2, \quad (a^2+b^2=1) \end{cases} \tag{1}$$

$$i.e.\ \ (x-c_1)^2 + (y-c_2)^2 = 1$$

例　その2　基本関数: $F(x,y,\dot{x},\dot{y}) = \sqrt{\dot{x}^2+\dot{y}^2} - y\dot{y}$　(図2参照)

単位球面（基準面）: $\dfrac{\dot{x}^2}{\dfrac{1}{1-y^2}} + \dfrac{(\dot{y}-\dfrac{y}{1-y^2})^2}{\dfrac{1}{(1-y^2)^2}} = 1 \quad \mathrm{on} T_{(x,y)}M$

$M = \{(x,y) | -1 < y < 1\}$

測地線:

$$\begin{cases} x(t) &= at + b \\ y(t) &= ct + d, \quad (a^2+c^2=1) \end{cases} \tag{2}$$

$$i.e.\ \ c(x-b) - a(y-d) = 0$$

* 本講演は、平成30年度長崎県立大学学長裁量研究費「フィンスラー空間の非対称性を応用した新公開鍵暗号の具体例の構成」に基づく発表である。

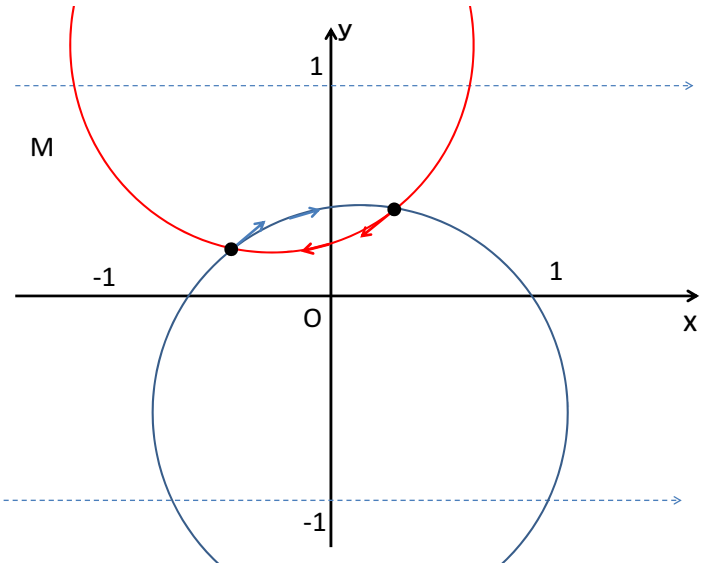

図 1: 測地線の像が異なるフィンスラー空間

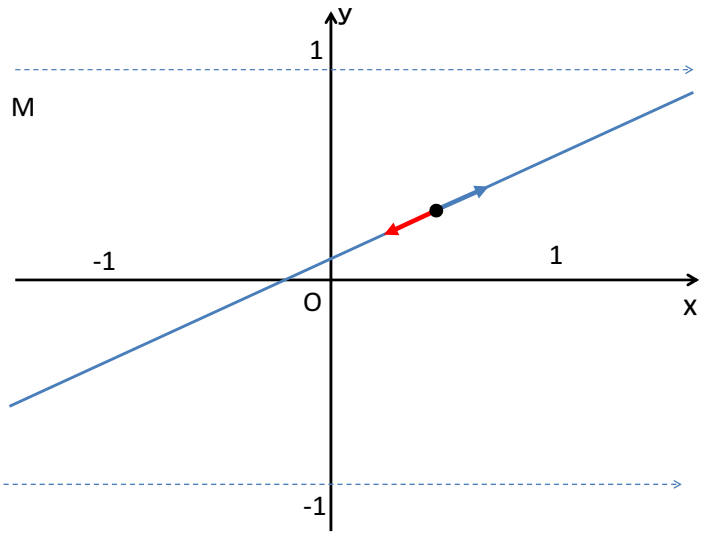

図 2: 測地線の像が一致するフィンスラー空間

例　その３　基本関数: $F(x,y,\dot{x},\dot{y}) = \sqrt{\dot{x}^2+\dot{y}^2} - e(y)\dot{x}$ (図３参照)

$$e(y) = \begin{cases} e^{-\frac{1}{y}} & (y>0) \\ 0 & (y \le 0) \end{cases}$$

(関数$e(y)$は、$y=0$でC^∞-級につながっている)

$M = \mathcal{R}^2$

測地線:

(I) $y \le 0$の場合

$$F(x,y,\dot{x},\dot{y}) = \sqrt{\dot{x}^2+\dot{y}^2}$$

可逆直線(方程式は擬似パラメータtの一次式)

(II) $y > 0$の場合

$$F(x,y,\dot{x},\dot{y}) = \sqrt{\dot{x}^2+\dot{y}^2} - e^{-\frac{1}{y}}\dot{x}$$

$$\begin{cases} \dot{x} = \dfrac{dx}{dt} &= e^{-\frac{1}{y}} + a \ (a: \text{定数}) \\ \dot{y} = \dfrac{dy}{dt} &= \pm\sqrt{1-(e^{-\frac{1}{y}}+a)^2} \end{cases}$$

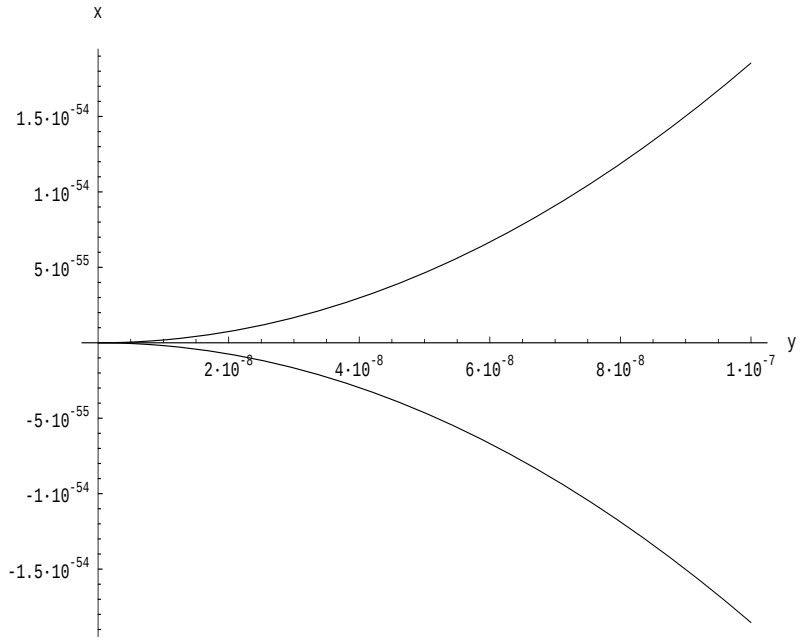

図 3: 測地線の像が片側だけ一致するフィンスラー空間

2. 暗号システムへの試み

フィンスラー空間がもつ別の非対称に、平行移動の非対称というものがある。

＜線形平行移動＞

$F\Gamma = (N^i_j(x,y), F^i_{rj}(x,y), C^i_{rj}(x,y))$：あるフィンスラー接続

$c(t) = (c^i(t))$：曲線,　　$v(t) = (v^i(t))$：cに沿うベクトル場

$$v: c\text{に沿う平行ベクトル場} \iff \frac{dv^i}{dt} + F^i_{rj}(c,\dot{c})v^r\dot{c}^j = 0 \qquad (3)$$

線形平行移動：始点と終点における接空間の線形写像 (図 4 参照)

＊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、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。ただし、測地線に沿う内積は、一定になる。

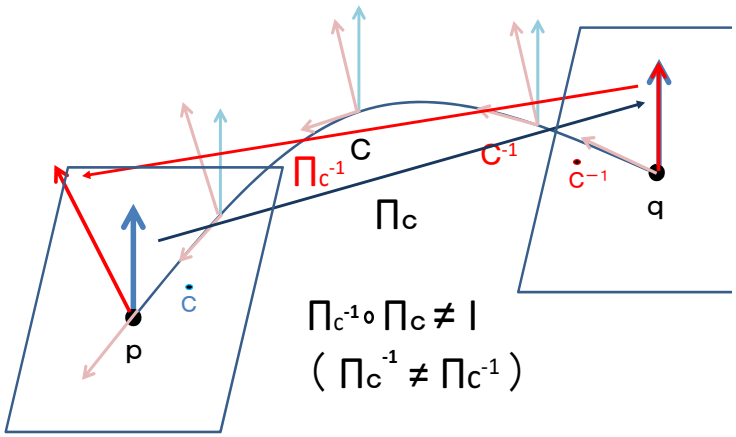

図 4: 非対称な平行移動

例その 2 のフィンスラー空間を用いて、平行移動の非対称性から次をマスターキーとする公開鍵暗号を提案した。

$$\Pi_{c_m}(t) = \begin{pmatrix} \dfrac{\sqrt{1-m^2(-1+t+t_0)}-m^2(-1+t+t_0)\sqrt{1-m^2(-1+t_0)}}{(1-m^2(-1+t+t_0))^{\frac{3}{2}}} & \dfrac{m(-1+t+t_0)\sqrt{1-m^2(-1+t_0)}-m(-1+t_0)\sqrt{1-m^2(-1+t+t_0)}}{(1-m^2(-1+t+t_0))^{\frac{3}{2}}} \\ \dfrac{m\sqrt{1-m^2(-1+t+t_0)}-m\sqrt{1-m^2(-1+t_0)}}{(1-m^2(-1+t+t_0))^{\frac{3}{2}}} & \dfrac{\sqrt{1-m^2(-1+t_0)}-m^2(-1+t_0)\sqrt{1-m^2(-1+t+t_0)}}{(1-m^2(-1+t+t_0))^{\frac{3}{2}}} \end{pmatrix} \tag{4}$$

$$E(v(t)) = \frac{1}{(1+m^2)^2}\left(((1+m^2)^2 - m^4(t+t_0))(v^1)^2 - 2m(t+t_0)v^1v^2 \right. \\ \left. +(1+m^2(-1+(t+t_0))(-2+m^2(-1+(t+t_0))+(t+t_0)))(v^2)^2\right) \tag{5}$$

＜秘密鍵・公開鍵＞

秘密鍵：$m=3, t_0=\frac{1}{2}$

公開鍵１：

$$PK1 = \begin{pmatrix} \frac{1}{1-9\left(t-\frac{1}{2}\right)} - \frac{3m\sqrt{\frac{11}{2}}\left(t-\frac{1}{2}\right)}{\left(1-9\left(t-\frac{1}{2}\right)\right)^{3/2}} & \frac{m\sqrt{1-9\left(t-\frac{1}{2}\right)}-m\sqrt{\frac{11}{2}}+6\sqrt{\frac{11}{2}}t}{2\left(1-9\left(t-\frac{1}{2}\right)\right)^{3/2}} \\ \frac{m}{1-9\left(t-\frac{1}{2}\right)} - \frac{3\sqrt{\frac{11}{2}}}{\left(1-9\left(t-\frac{1}{2}\right)\right)^{3/2}} & \frac{\sqrt{\frac{11}{2}}}{\left(1-9\left(t-\frac{1}{2}\right)\right)^{3/2}} - \frac{3m}{2\left(9\left(t-\frac{1}{2}\right)-1\right)} \end{pmatrix}$$

公開鍵２：

$$PK2 = \frac{1}{100}\left(\frac{119}{2}(v_0^1)^2 - 3v_0^1v_0^2 + 28(v_0^2)^2\right)$$

数値実験

平文 $v(t_0) = (1023, 2301)$

秘密鍵：$m=3, t_0=\frac{1}{2}$

公開鍵１ $PK1 = \begin{pmatrix} \frac{1}{1-9\left(t-\frac{1}{2}\right)} - \frac{3m\sqrt{\frac{11}{2}}\left(t-\frac{1}{2}\right)}{\left(1-9\left(t-\frac{1}{2}\right)\right)^{3/2}} & \frac{m\sqrt{1-9\left(t-\frac{1}{2}\right)}-m\sqrt{\frac{11}{2}}+6\sqrt{\frac{11}{2}}t}{2\left(1-9\left(t-\frac{1}{2}\right)\right)^{3/2}} \\ \frac{m}{1-9\left(t-\frac{1}{2}\right)} - \frac{3\sqrt{\frac{11}{2}}}{\left(1-9\left(t-\frac{1}{2}\right)\right)^{3/2}} & \frac{\sqrt{\frac{11}{2}}}{\left(1-9\left(t-\frac{1}{2}\right)\right)^{3/2}} - \frac{3m}{2\left(9\left(t-\frac{1}{2}\right)-1\right)} \end{pmatrix}$

公開鍵２ $PK2 = \frac{1}{100}\left(\frac{119}{2}(v_0^1)^2 - 3v_0^1v_0^2 + 28(v_0^2)^2\right)$

$t=\frac{1}{4}$　として、暗号文 $\left\{PK1(\frac{1}{4})v(t_0), PK2(v(t_0))\right\}$ を作成。

$v(t) = PK1(\frac{1}{4})v(t_0) = \left(\frac{3}{169}\left(\left(19942-511\sqrt{286}\right)m + 2301\sqrt{286} + 17732\right), -\frac{6}{169}\left(512\sqrt{286} - 38779m\right)\right)$

$PK2(v(t_0)) = \frac{406911069}{200}$

次に、受信者が t の値を求めるための計算。$m=3, t_0=\frac{1}{2}$ から

$PK2(v(t)) = \frac{108t\left(15\left(1046866981-9163776\sqrt{286}\right)t+118365440\sqrt{286}-19221457233\right)+99\left(6429090587-22909440\sqrt{286}\right)}{109850}$

方程式 $PK2(v(t)) = PK2(v(t_0))$ を解くと

方程式の解：$t=\frac{1}{4}, \frac{19\left(17684480\sqrt{286}-3220148643\right)}{60\left(9163776\sqrt{286}-1046866981\right)}$　（t の範囲から、$t=\frac{1}{4}$ のみが求める解）

$m=3, t_0=\frac{1}{2}, t=\frac{1}{4}$ から

$$PK1(1/4) = \begin{pmatrix} \frac{4}{13} + \frac{9\sqrt{\frac{22}{13}}}{13} & \frac{8\left(\frac{3\sqrt{\frac{11}{2}}}{4} + \frac{3}{2}\left(-\sqrt{\frac{11}{2}} + \frac{\sqrt{13}}{2}\right)\right)}{13\sqrt{13}} \\ \frac{12}{13} - \frac{12\sqrt{\frac{22}{13}}}{13} & \frac{18}{13} + \frac{4\sqrt{\frac{22}{13}}}{13} \end{pmatrix}$$

$$v(1/4) = \left(\frac{3}{169} \left(17732 + 2301\sqrt{286} + 3 \left(19942 - 511\sqrt{286} \right) \right), -\frac{6}{169} \left(512\sqrt{286} - 116337 \right) \right)$$

$$\therefore \quad \text{平文}\, v(t_0) = PK1^{-1}(1/4)v(1/4) = (1023, 2301)$$

となる。

このシステムが暗号としてどの程度の強度を持つかの評価は、今後の研究課題である。

参考文献

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

[2] N. Innami, T. Nagano, and K. Shiohama. : *Geodesics in a Finsler surface with one-parameter group of motions*, Publ. Math. Debrecen, 89(1-2):137-160, 2016.

[3] N. Innami, Y.Itokawa, T. Nagano, and K. Shiohama. : *Parallel axiom and the 2-nd order differentiability of Busemann functions*, Publ. Math. Debrecen, 91(3-4):403-425, 2017.

[4] 永野哲也：逆線形平行移動を与える曲線の存在について, 2018 年日本数学会年度会幾何学分科会講演アブストラクト. p1 − 2, 東京大学, 3 月 18 日, 2018.