Vol.2021-CSEC-95 No.6
Vol.2021-SPT-45 No.6
Vol.2021-EIP-94 No.6
2021/11/8

Mathematical Structure of Finsler Encryption

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

概要：The public-key encryption scheme called **Finsler encryption** introduced by Nagano and Anada at SecITC2020 is investigated about its mathematical structure. In the previous work they stated the scheme based on the linear parallel displacement of vectors on a curve in a Finsler space and exhibited three algorithms of key generation, encryption and decryption in detail. The base idea of Finsler encryption was stated at CSS2019 and at SCIS2020 by the same authors. In this paper, the public key PK is represented as a mapping from $\mathcal{R}^2$ to $\mathcal{R}^9$ and the secret key SK is represented as the inverse mapping of PK.

キーワード：Finsler encryption, public-key encryption, Finsler geometry, differential geometry, linear parallel displacement

1. Introduction

Finsler encryption was defined by Nagano and Anada during from 2019 to 2020(cf.[8],[9],[10]). In the basic, this encryption has the differential geometry, especially, Finsler geometry(cf.[1],[2],[3],[4],[5],[6]). Thus, all items of Finsler encryption are defined on a real and smooth manifold. Further, in differential geometry(Riemaniann geometry), almost all object have symmetric property. On the other hand, one of the most important notions in the public-key encryption is *one direction property*. And encryption has been ever studied on *discrete mathematics* before(cf.[15],[16],[17],[18],[19],[20]).

Finsler geometry is known as geometry that has asymmetric property different from Riemannian geometry(cf.[7],[11],[12],[13],[14]). Especially, the *linear parallel displacement*(cf.[7]) plays a very important role in Finsler encryption. It is a very interesting notion having asymmetric property which the image of a vector obtained by the linear parallel displacement on a curve c is different from the image of the same vector obtained by the linear parallel displacement on the inverse curve c^{-1}. This asymmetric property is used in one direction property in the public-key encryption. Further, in this encryption, almost all items are expressed in continuous and real form because that geodesic and the linear parallel displacement are solutions of simultaneous differential equations. In encryption system, it is not good for using them as it is. Thus we must change them to integer and rational forms by a *quantization* of a parameter easily. Fortunately, there are many methods of quantization.

1 University of Nagasaki, 1-1-1 Manabino, Nagayo Cho, Nishisonogi Gun, Nagasaki Pref., Japan
a) hnagano@sun.ac.jp
b) anada@sun.ac.jp

2. Finsler Encryption

We call new public-key encryption scheme introduced by T. Nagano and H. Anada at SecITC 2020[10] *Finsler Encryption*. In this paper, we discuss about Finsler encryption of §4 in [10], especially.

2.1 Finsler Encryption

Let (x, y) be the coordinate of the base manifold $M = \mathcal{R}^2$ and $(\dot{x}, \dot{y})$ the coordinate of $T_{(x,y)}M$, namely, $x = x^1, y = x^2, \dot{x} = y^1, \dot{y} = y^2$. The Finsler metric $F(x, y, \dot{x}, \dot{y})$ is as follows

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

where all a, b, h_1, h_2 are positive numbers.
According to Recipe in §2 of [10], various objects are obtained. However, in the following representation of them are on the geodesic c only.

Geodesic: straight line

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

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

where the equation of the above straight line is $y = \frac{a}{b} m x$ on M.

Linear parallel displacement: $\Pi_{c_m}(t)$

$$\Pi_{c_m}(t) = \begin{pmatrix} B_1^1 & B_2^1 \\ B_1^2 & B_2^2 \end{pmatrix}, \tag{3}$$

where

$$\begin{aligned}
B_1^1 = & -\frac{1}{\left(a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0 - (b^2h_1 + a^2h_2m^2)t\right)^{3/2}} \times \\
& \Bigl(a^2 \bigl(h_2m^2(t+t_0)\sqrt{a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0} \\
& -b^2 \bigl(\sqrt{a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0 - (b^2h_1 + a^2h_2m^2)t} \\
& +m^2\sqrt{a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0}\bigr)\bigr) \\
& +b^2h_1t_0\sqrt{a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0 - (b^2h_1 + a^2h_2m^2)t}\Bigr),
\end{aligned}$$

$$\begin{aligned}
B_2^1 = & \frac{1}{\left(a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0 - (b^2h_1 + a^2h_2m^2)t\right)^{3/2}} \times \\
& \Bigl(abm \Bigl(b^2 \bigl(-\sqrt{a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0} \\
& +\sqrt{a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0 - (b^2h_1 + a^2h_2m^2)t}\bigr) \\
& + h_2 \bigl(t\sqrt{a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0} \\
& + t_0\sqrt{a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0} \\
& -t_0\sqrt{a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0 - (b^2h_1 + a^2h_2m^2)t}\bigr)\Bigr)\Bigr),
\end{aligned}$$

$$\begin{aligned}
B_1^2 = & \frac{1}{\left(a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0 - (b^2h_1 + a^2h_2m^2)t\right)^{3/2}} \times \\
& \Bigl(abm \Bigl(a^2 \bigl(-\sqrt{a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0} \\
& +\sqrt{a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0 - (b^2h_1 + a^2h_2m^2)t}\bigr) \\
& + h_1 \bigl(t\sqrt{a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0} \\
& + t_0\sqrt{a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0} \\
& -t_0\sqrt{a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0 - (b^2h_1 + a^2h_2m^2)t}\bigr)\Bigr)\Bigr),
\end{aligned}$$

$$\begin{aligned}
B_2^2 = & -\frac{1}{\left(a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0 - (b^2h_1 + a^2h_2m^2)t\right)^{3/2}} \times \\
& \Bigl(-a^2b^2 \bigl(\sqrt{a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0} \\
& +m^2\sqrt{a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0 - (b^2h_1 + a^2h_2m^2)t}\bigr) \\
& + b^2h_1(t+t_0)\sqrt{a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0} \\
& +a^2h_2m^2t_0\sqrt{a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0 - (b^2h_1 + a^2h_2m^2)t}\Bigr).
\end{aligned}$$

Quantization: We change each equation to forms having rational expressions. For new parameters k and t, they are as follows changing.

$$k^2 := a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0 \tag{4}$$

$$t^2 := a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0 - (b^2h_1 + a^2h_2m^2)t. \tag{5}$$

Then as for new parameters k, t, we have components $B_1^1, B_2^1, B_1^2, B_2^2$ of Π

$$\begin{aligned}
B_1^1 = & \frac{1}{\left(h_1b^2 + a^2h_2m^2\right)t^3} \Bigl(\left(h_1b^2 + a^2h_2m^2\right)\left(a^2 - h_1t_0\right)tb^2 + a^2h_2km^2t^2 \\
& +a^2km^2\left(\left(h_1b^2 + a^2h_2m^2\right)\left(b^2 - h_2t_0\right) - h_2k^2\right)\Bigr),
\end{aligned}$$

$$B_2^1 = \frac{abm(k-t)\left(h_2k^2 + h_2tk - \left(h_1b^2 + a^2h_2m^2\right)\left(b^2 - h_2t_0\right)\right)}{\left(h_1b^2 + a^2h_2m^2\right)t^3},$$

$$B_1^2 = \frac{abm(k-t)\left(-h_2m^2a^4 + h_1\left(h_2m^2t_0 - b^2\right)a^2 + h_1\left(h_1t_0b^2 + k(k+t)\right)\right)}{\left(h_1b^2 + a^2h_2m^2\right)t^3},$$

$$\begin{aligned}
B_2^2 = & \frac{1}{\left(h_1b^2 + a^2h_2m^2\right)t^3} \Bigl(h_2m^2\left(kb^2 + m^2\left(b^2 - h_2t_0\right)t\right)a^4 + b^2h_1\Bigl(b^2\left(tm^2 + k\right) \\
& -h_2m^2t_0(k+t)\Bigr)a^2 - b^2h_1k\left(h_1t_0b^2 + k^2 - t^2\right)\Bigr).
\end{aligned}$$

Before obtaining the public key and secret key, we must give a regular matrix $C(\tau)$ as the transformation of $T_p(M)$ and splitting form of the energy of $E(v_1)$. In this paper, we have the same splitting of $E(v_1)$ as [10].

Key Generation: According to [10], we state the outline of its key generation as below.
(1) c: a geodesic, p: start point, q: end point
(2) $v = (v^1, v^2)$: a plaintext (a vector in $\mathcal{R}^2$), $dv = (dv^1, dv^2)$: a positive difference vector ($dv^1 > 0, dv^2 > 0$), $v_0 = v + dv$
(3) $v_1 = C(\tau)v_0$
(4) $v_2 = \Pi_c(t_2)v_1$
(5) $E(v_2) = E(v_1) = E_0 + E_1 + E_2$: a splitting of the energy of v_1
(6) $E(v_1) = \frac{E_0}{f_0} f_0 + \frac{E_1}{f_1 v_0^1} f_1 v_0^1 + \frac{E_2}{f_2 v_0^2} f_2 v_0^2$
(7) $V_3 = \Pi_c(\tau)\ {}^t(\frac{E_1}{f_1 v_0^1}, \frac{E_2}{f_2 v_0^2}) = {}^t(V_3^1, V_3^2)$
(8) $(\frac{E_0}{f_0}, V_3^1, V_3^2)$: a ciphertext
After all, we have a public key $PK = (\frac{E_0}{f_0}, V_3^1, V_3^2)$.

First of all, let $(a, b, h_1, h_2, m, t_0, t_1) = (1, 1, 1, 1, 1, \frac{1}{2}, 1)$ be all parameters.

Case (I) Next, let $C(\tau)$ be

$$C(\tau) = \begin{pmatrix} \tau & -1 \\ 1 & \tau \end{pmatrix}.$$

Then we have the secret key $SK = \{(f_0, f_1, f_2), \Pi_c(\tau), E(v_1)\}$ is as follows.

$$(f_0, f_1, f_2) = (mh_1, at_0h_2, bt_1h_2^2) = (1, \frac{1}{2}, 1),$$

$$\Pi_c(\tau) = \begin{pmatrix} \frac{\tau+1}{2\tau^2} & -\frac{\tau-1}{2\tau^2} \\ -\frac{\tau-1}{2\tau^2} & \frac{\tau+1}{2\tau^2} \end{pmatrix},$$

$$\begin{aligned}
E(v_1) = G(v_1, v_1) = & \frac{1}{8}(3\tau^2 - 2\tau + 3)(v_0^1)^2 + \frac{1}{4}(1 - \tau^2)v_0^1 v_0^2 \\
& + \frac{1}{8}(3\tau^2 + 2\tau + 3)(v_0^2)^2
\end{aligned}$$

and $(\frac{E_0}{f_0}, V_3^1, V_3^2)$ as follows.

$$
\begin{aligned}
\frac{E_0}{f_0} = \frac{1}{64t_2^4} \Big(\Big(& 3(\tau-1)^2 t_2^6 - 8\big(\tau^2+\tau-2\big) t_2^5 - 2((\tau-14)\tau-5)t_2^4 \\
& +16\big(\tau^2+\tau-2\big) t_2^3 + 4(\tau(11\tau-10)+17)t_2^2 + 24(\tau-1)^2\Big) (v_0^1)^2 \\
& + 2(v_0^1)(v_0^2) \Big((t_2(t_2(t_2(3t_2+4)-14)-8)+20)t_2^2 + 12\Big(t_2\Big(2t_2^2 \\
& +t_2-4)+2\Big)\tau t_2^2 - \Big((t_2(t_2(t_2(3t_2+4)-14)-8)+20)t_2^2+24\Big)\tau^2+24\Big) \\
& + (v_0^2)^2 \Big(3(\tau+1)^2 t_2^6 + 8\big(2\tau^2+\tau-1\big) t_2^5 + 2(\tau(5\tau-14)-1)t_2^4 \\
& -16\big(2\tau^2+\tau-1\big) t_2^3 + 4(\tau(17\tau+10)+11)t_2^2 + 24(\tau+1)^2\Big)\Big),
\end{aligned} \tag{6}
$$

$$
\begin{aligned}
V_3^1 = \frac{1}{64\tau^2 t_2^4 (v_0^1)(v_0^2)} \Big(& -2(\tau-1)\Big(\Big(\big(t_2^2-2\big)(t_2(t_2+2)-4)t_2^2 + \big(t_2^6-4t_2^4+8\big)\tau^2 \\
& -2(t_2+2)\big(t_2^2-2\big)\big(t_2^3-t_2^2+t_2-2\big)\tau+8\Big)(v_0^1)^3 + (v_0^1)^2(v_0^2)\Big(3(\tau-1)^2 \\
& (\tau+1)t_2^6 - 4(\tau-1)(3\tau(\tau+2)+5)t_2^5 + 2(\tau(3(1-5\tau)\tau+13)-13)t_2^4 \\
& + 8(\tau-1)(3\tau(\tau+2)+5)t_2^3 + 4(\tau(\tau(13\tau+11)+9)+27)t_2^2 \\
& +24(\tau-1)^2(\tau+1)\Big) - 4(v_0^1)(v_0^2)^2\Big(3(\tau-1)(\tau+1)^2 t_2^6 + (\tau+1)(3(\tau-5)\tau \\
& -4)t_2^5 + (\tau(14-\tau(14\tau+19))+15)t_2^4 - 2(\tau+1)(3(\tau-5)\tau-4)t_2^3 \\
& +2(\tau((\tau-8)\tau-18)-3)t_2^2 + 24(\tau-1)(\tau+1)^2\Big) + (v_0^2)^3(\tau+1) \\
& \Big(7(\tau+1)^2 t_2^6 + 8(\tau+1)(3\tau-1)t_2^5 - 2(\tau(19\tau+34)+21)t_2^4 - 16(\tau+1) \\
& (3\tau-1)t_2^3 + 4(\tau(25\tau+6)+11)t_2^2 + 56(\tau+1)^2\Big)\Big),
\end{aligned} \tag{7}
$$

$$
\begin{aligned}
V_3^2 = \frac{1}{64\tau^2 t_2^4 (v_0^1)(v_0^2)} \Big(& 2(\tau+1)\Big(\Big(\big(t_2^2-2\big)(t_2(t_2+2)-4)t_2^2 + \big(t_2^6-4t_2^4+8\big)\tau^2 \\
& -2(t_2+2)\big(t_2^2-2\big)\big(t_2^3-t_2^2+t_2-2\big)\tau+8\Big)(v_0^1)^3 + (v_0^1)^2(v_0^2)((\tau-1) \\
& (\tau(3\tau-22)+3)t_2^6 - 4(3\tau-5)(\tau(\tau+2)-1)t_2^5 + 2(13-3\tau(\tau(5\tau \\
& -19)+21))t_2^4 + 8(3\tau-5)(\tau(\tau+2)-1)t_2^3 + 4(\tau(\tau(13\tau-7)+37) \\
& -27)t_2^2 + 8(\tau-1)(\tau(3\tau-22)+3)\Big) - 4(v_0^1)(v_0^2)^2\Big((\tau+1)(\tau(3\tau-8)+3)t_2^6 \\
& + (\tau(\tau(3\tau-22)+11)+4)t_2^5 + (\tau(7(3-2\tau)\tau+24)-15)t_2^4 - 2(\tau(\tau(3\tau \\
& -22)+11)+4)t_2^3 + 2(\tau((\tau-18)\tau+12)+3)t_2^2 + 8(\tau+1)(\tau(3\tau-8)+3)\Big) \\
& + (v_0^2)^3(\tau-1)\Big(7(\tau+1)^2 t_2^6 + 8(\tau+1)(3\tau-1)t_2^5 - 2(\tau(19\tau+34)+21)t_2^4 \\
& -16(\tau+1)(3\tau-1)t_2^3 + 4(\tau(25\tau+6)+11)t_2^2 + 56(\tau+1)^2\Big)\Big).
\end{aligned} \tag{8}
$$

Case (II) On the other hand, let $C(\tau)$ be

$$
C(\tau) = \begin{pmatrix} \tau & 1 \\ \tau-1 & 1 \end{pmatrix}.
$$

Then we have the same (f_0, f_1, f_2) and Π_c, however, different $E(v_1)$ and PK as follows:

$$
E(v_1) = G(v_1, v_1) = \frac{1}{8}(4\tau^2-4\tau+3)(v_0^1)^2 + \frac{1}{2}(2\tau-1)v_0^1 v_0^2 + \frac{1}{2}(v_0^2)^2
$$

and $PK = (\frac{E_0}{f_0}, V_3^1, V_3^2)$ is

$$
\begin{aligned}
\frac{E_0}{f_0} = \frac{1}{64t_2^4} \Big(& (v_0^1)^2 \Big(t_2^2\Big(36\tau^2\big(t_2^2+2\big) - 24\tau(t_2(t_2(t_2+2)-2)+4) + t_2(t_2(t_2(3t_2 \\
& +16)+10)-32)+68\Big)+24\Big) - 24t_2^2(v_0^1)(v_0^2)\Big(-3\tau\big(t_2^2+2\big) \\
& +t_2(t_2(t_2+2)-2)+4\Big) + 36\big(t_2^2+2\big)t_2^2(v_0^2)^2\Big),
\end{aligned}
$$

$$
\begin{aligned}
V_3^1 = \frac{1}{64\tau^2 t_2^4 (v_0^1)(v_0^2)} \Big(& 2(\tau-1)(v_0^1)^3\Big(t_2^2\Big(4\tau^2\big(t_2^2-3\big) + \big(2-t_2^2\big)(t_2(t_2+2)-4) \\
& +2\tau(t_2((t_2-3)t_2-2)+10)\Big)-8\Big) + 12(\tau+1)t_2^2\big(t_2^2-10\big)(v_0^2)^3 + 8t_2^2(v_0^1)(v_0^2)^2 \\
& \Big(-30\tau^2-11\tau+4(\tau+1)t_2^3+(3\tau(\tau+1)-2)t_2^2-8(\tau+1)t_2+25\Big) \\
& + (v_0^1)^2(v_0^2)\Big(-56(\tau+1)-7(\tau+1)t_2^6+4(\tau(8\tau+3)-7)t_2^5 \\
& + 2\big(6\tau^3+10\tau^2+\tau+25\big)t_2^4 - 8(\tau(8\tau+3)-7)t_2^3 + 4\Big(\tau\Big(-30\tau^2+2\tau+41\Big) \\
& -35\Big)t_2^2\Big)\Big),
\end{aligned}
$$

$$
\begin{aligned}
V_3^2 = \frac{1}{64\tau^2 t_2^4 (v_0^1)(v_0^2)} \Big(& -2(\tau+1)(v_0^1)^3\Big(t_2^2\Big(4\tau^2\big(t_2^2-3\big) + \big(2-t_2^2\big)(t_2(t_2+2)-4) \\
& +2\tau(t_2((t_2-3)t_2-2)+10)\Big)-8\Big) - 12(\tau-1)t_2^2\big(t_2^2-10\big)(v_0^2)^3 - 8t_2^2(v_0^1)(v_0^2)^2 \\
& \Big((49-30\tau)\tau+4(\tau-1)t_2^3+(3(\tau-1)\tau+2)t_2^2-8\tau t_2+8t_2-25\Big) \\
& + (v_0^1)^2(v_0^2)\Big(56(\tau-1)+7(\tau-1)t_2^6-4(\tau(8\tau-13)+7)t_2^5+2\Big(\tau\Big(-6\tau^2+2\tau \\
& -25\Big)+25\Big)t_2^4 + 8(\tau(8\tau-13)+7)t_2^3 + 4\Big(\tau\Big(30\tau^2-62\tau+71\Big)-35\Big)t_2^2\Big).
\end{aligned}
$$

We can take any regular matrix $C(\tau)$. Whenever applying different $C(\tau)$, we can obtain different $E(v_1)$ and $(\frac{E_0}{f_0}, V_3^1, V_3^2)$ even if the same parameters $(a, b, h_1, h_2, m, t_0, t_1)$. Then we have

Proposition2.1 In the Finsler encryption, even if the parameters $(a, b, h_1, h_2, m, t_0, t_1)$, the quantization and the splitting form of the energy $E(v_1)$ are same, there exist different pairs (SK, PK) of the secret key SK and the public key PK depending on the transformation $C(\tau)$.

Remark2.1 (1) The value t_0 must be chosen a rational number for k to be a rational number.
(2) The methods of quantization are many. For example

$$
\begin{aligned}
(t+1)^2 := {} & a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0 \\
& - (b^2h_1 + a^2h_2m^2)t
\end{aligned} \tag{9}
$$

or

$$
\begin{aligned}
(\frac{1}{t}+1)^2 := {} & a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0 \\
& - (b^2h_1 + a^2h_2m^2)t.
\end{aligned} \tag{10}
$$

(3) If we change the method of quantization, then we have the arranging matrix $\Pi_c(\tau)$ in addition.

2.2 *PK*

In this section, we state the mathematical structure of the pubic key PK of Finsler encryption.
First, in Case (I) of the previous section, we take $(\tau, \beta_0, \beta_1, \beta_2) = (1, \frac{1}{2}, \frac{2}{3}, \frac{3}{4})$. Then we have the public key $PK_{\tau,\beta_0,\beta_1,\beta_2}$ as follows

$$
\begin{aligned}
&\cdot\ (\tau = 1, t_2 = \beta_0 = \frac{1}{2})\\
pk_0 &= \{pk_{00}, pk_{01}, pk_{02}\}\\
&= \left\{ \frac{324(v_0^1)^2 + 48(v_0^1)(v_0^2) + 2071(v_0^2)^2}{64}, \right.\\
&- \frac{468(v_0^1)^2 + 232(v_0^1)(v_0^2) + 4003(v_0^2)^2}{32(v_0^1)},\\
&\left. \frac{44(v_0^1)^2 + 46(v_0^1)(v_0^2) + 499(v_0^2)^2}{16(v_0^2)} \right\},\\
&\cdot\ (\tau = 1, t_2 = \beta_1 = \frac{2}{3})\\
pk_1 &= \{pk_{10}, pk_{11}, pk_{12}\}\\
&= \left\{ \frac{99(v_0^1)^2 + 10(v_0^1)(v_0^2) + 388(v_0^2)^2}{32}, \right.\\
&- \frac{1161(v_0^1)^2 + 498(v_0^1)(v_0^2) + 5858(v_0^2)^2}{144(v_0^1)},\\
&\left. \frac{207(v_0^1)^2 + 204(v_0^1)(v_0^2) + 1327(v_0^2)^2}{144(v_0^2)} \right\},\\
&\cdot\ (\tau = 1, t_2 = \beta_2 = \frac{3}{4})\\
pk_2 &= \{pk_{20}, pk_{21}, pk_{22}\}\\
&= \left\{ \frac{17712(v_0^1)^2 + 1872(v_0^1)(v_0^2) + 57209(v_0^2)^2}{6912}, \right.\\
&- \frac{65232(v_0^1)^2 + 27360(v_0^1)(v_0^2) + 263423(v_0^2)^2}{10368(v_0^1)},\\
&\left. \frac{5616(v_0^1)^2 + 5436(v_0^1)(v_0^2) + 28133(v_0^2)^2}{5184(v_0^2)} \right\}.
\end{aligned}
\tag{11}
$$

The public key $PK_{1,\frac{1}{2},\frac{2}{3},\frac{3}{4}} = (pk_0, pk_1, pk_2)$ is true.

We have the plaintext space $\mathcal{M}$ is a set of lattice points of the first quadrant in $\mathcal{R}^2$. From $PK_{1,\frac{1}{2},\frac{2}{3},\frac{3}{4}}$, we notice that ciphers are rational points in $\mathcal{R}^9$ and the set of the ciphers is a certain subset of $\mathcal{R}^9$.Thus we have the mapping $PK_{1,\frac{1}{2},\frac{2}{3},\frac{3}{4}}$ from $\mathcal{M}$ to $\mathcal{R}^9$. In general, for each $(\tau, \beta_0, \beta_1, \beta_2)$, we can regard the public key $PK_{\tau,\beta_0,\beta_1,\beta_2}$ as the mapping from $\mathcal{M}$ to $\mathcal{R}^9$

$$
\begin{aligned}
&PK_{\tau,\beta_0,\beta_1,\beta_2} : \mathcal{M} \subset \mathcal{R}^2 \ \longrightarrow\ \mathcal{R}^9\\
&\mid v_0 = (v_0^1, v_0^2) \mapsto ct = PK_{\tau,\beta_0,\beta_1,\beta_2}(v_0).
\end{aligned}
\tag{12}
$$

Remark2.2 $PK_{\tau,\beta_0,\beta_1,\beta_2}$ is the mapping from $\mathcal{M}$ to $\mathcal{R}^9$ as the public key, however, as a mapping, on from $\mathcal{R}^2$ to $\mathcal{R}^9$, and excepting axes $v_0^1 = 0$ and $v_0^2 = 0$ it is differentiable with respect to v_0^1 and v_0^2.

2.3 *SK*

First, we put a ciphertext $ct = PK_{\tau,\beta_0,\beta_1,\beta_2}(v_0) = (ct_0, ct_1, ct_2)$, where

$$
\begin{aligned}
ct_0 &= pk_0(v_0) = (ct_{00}, ct_{01}, ct_{02}),\\
ct_1 &= pk_1(v_0) = (ct_{10}, ct_{11}, ct_{12}),\\
ct_2 &= pk_2(v_0) = (ct_{20}, ct_{21}, ct_{22}).
\end{aligned}
\tag{13}
$$

According to the algorithm of the decryption, (v_0^1, v_0^2) is the solution of the following simultaneous linear system of (X, Y)

$$
\begin{cases}
\frac{1}{4}((-ct_{01} + ct_{02} + ct_{11} - ct_{12})\tau + (-ct_{01} - ct_{02} + ct_{11} + ct_{12})\tau^2)X\\
+ \frac{1}{2}((ct_{01} - ct_{02} - ct_{11} + ct_{12})\tau + (-ct_{01} - ct_{02} + ct_{11} + ct_{12})\tau^2)Y\\
= ct_{00} - ct_{10}\\
\frac{1}{4}((-ct_{01} + ct_{02} + ct_{21} - ct_{22})\tau + (-ct_{01} - ct_{02} + ct_{21} + ct_{22})\tau^2)X\\
+ \frac{1}{2}((ct_{01} - ct_{02} - ct_{21} + ct_{22})\tau + (-ct_{01} - ct_{02} + ct_{21} + ct_{22})\tau^2)Y\\
= ct_{00} - ct_{20}.
\end{cases}
\tag{14}
$$

If the following the determinant Det of the above system

$$
Det = \frac{1}{2}(ct_{01}ct_{12} - ct_{01}ct_{22} + ct_{02}ct_{21} - ct_{02}ct_{11} + ct_{11}ct_{22} - ct_{12}ct_{21})\tau^3
\tag{15}
$$

is non-zero, then the answer (X, Y), namely, (v_0^1, v_0^2) is rewrote by

$$
\begin{cases}
v_0^1 = \dfrac{A - B\tau}{(ct_{01}ct_{12} - ct_{01}ct_{22} + ct_{02}ct_{21} - ct_{02}ct_{11} + ct_{11}ct_{22} - ct_{12}ct_{21})\tau^2}\\
v_0^2 = \dfrac{A + B\tau}{2(ct_{01}ct_{12} - ct_{01}ct_{22} + ct_{02}ct_{21} - ct_{02}ct_{11} + ct_{11}ct_{22} - ct_{12}ct_{21})\tau^2},
\end{cases}
\tag{16}
$$

where

$$
\begin{aligned}
A = {} & ct_{01}ct_{10} - ct_{02}ct_{10} - ct_{00}ct_{11} + ct_{00}ct_{12} - ct_{01}ct_{20} + ct_{02}ct_{20}\\
& + ct_{11}ct_{20} - ct_{12}ct_{20} + ct_{00}ct_{21} - ct_{10}ct_{21} - ct_{00}ct_{22} + ct_{10}ct_{22},
\end{aligned}
$$

$$
\begin{aligned}
B = {} & ct_{01}ct_{10} + ct_{02}ct_{10} - ct_{00}ct_{11} - ct_{00}ct_{12} - ct_{01}ct_{20} - ct_{02}ct_{20}\\
& + ct_{11}ct_{20} + ct_{12}ct_{20} + ct_{00}ct_{21} - ct_{10}ct_{21} + ct_{00}ct_{22} - ct_{10}ct_{22}.
\end{aligned}
$$

Proposition2.2 If $(ct_{00}, ct_{01}, ct_{02} \cdots, ct_{20}, ct_{21}, ct_{22})$ is a ciphertext ct of a plaintext $v_0 = (v_0^1, v_0^2)$ and Det of (15) is non-zero, then the simultaneous linear system (14) has unique solution (X, Y) and it is the plaintext $v_0 = (v_0^1, v_0^2)$,namely,

$$
(X, Y) = (v_0^1, v_0^2)
$$

is satisfied.(Decryption of Finsler encryption).

In general, from a point $(ct_{00}, ct_{01}, ct_{02} \cdots, ct_{20}, ct_{21}, ct_{22}) \in \mathcal{R}^9$ and a value $\tau (\neq 0)$, we take the following matrix

$$
ppk_\tau = \begin{pmatrix} \pi_{11} & \pi_{12} \\ \pi_{21} & \pi_{22} \end{pmatrix},
\tag{17}
$$

where

$$
\pi_{11} = \frac{1}{4}((-ct_{01} + ct_{02} + ct_{11} - ct_{12})\tau + (-ct_{01} - ct_{02} + ct_{11} + ct_{12})\tau^2)
$$

$$
\pi_{12} = \frac{1}{2}((ct_{01} - ct_{02} - ct_{11} + ct_{12})\tau + (-ct_{01} - ct_{02} + ct_{11} + ct_{12})\tau^2)
$$

$$
\pi_{21} = \frac{1}{4}((-ct_{01} + ct_{02} + ct_{21} - ct_{22})\tau + (-ct_{01} - ct_{02} + ct_{21} + ct_{22})\tau^2)
$$

$$
\pi_{22} = \frac{1}{2}((ct_{01} - ct_{02} - ct_{21} + ct_{22})\tau + (-ct_{01} - ct_{02} + ct_{21} + ct_{22})\tau^2)
$$

and can consider a linear mapping ppk_τ as following

$$
ppk_\tau : \mathcal{R}^2 \longrightarrow \mathcal{R}^2 | v_0 = (v_0^1, v_0^2) \in \mathcal{R}^2 \mapsto ppk_\tau(v_0) \in \mathcal{R}^2.
\tag{18}
$$

Under the determinant $Det(ppk_\tau) \neq 0$, we can regard

the linear mapping ppk_τ as the mapping $PK_{\tau,\beta_0,\beta_1,\beta_2}$.
($\because$) We consider a projection pr from $\mathcal{R}^9$ to $\mathcal{R}^2$ as follows

$$\begin{aligned} pr :&(ct_{00}, ct_{01}, ct_{02}, ct_{10}, ct_{11}, ct_{12}, ct_{20}, ct_{21}, ct_{22}) \\ &\mapsto (ct_{00} - ct_{10}, ct_{00} - ct_{20}). \end{aligned}$$

Then, for a ciphertext ct, we can commute ppk_τ into $pr \circ PK_{\tau,\beta_0,\beta_1,\beta_2}$, namely,

$$ppk_\tau = pr \circ PK_{\tau,\beta_0,\beta_1,\beta_2} \tag{19}$$

by using the value τ decided by the energy $E(v_1)$(See Appendix).

The projection pr is not injection, in general. Even if $PK_{\tau,\beta_0,\beta_1,\beta_2}$ is injective, ppk_τ is not necessarily injective. However, if $Det(ppk_\tau) \neq 0$, then ppk_τ is regular, namely,

$$\begin{aligned} &ppk_\tau^{-1}(pr(ct)) = ppk_\tau^{-1}(pr(PK_{\tau,\beta_0,\beta_1,\beta_2}(v_0))) \\ &= (ppk_\tau^{-1} \circ pr \circ PK_{\tau,\beta_0,\beta_1,\beta_2})(v_0) = v_0 \quad ((\because) \text{ Proposition 2.2}) \end{aligned}$$

is satisfied, where $pr(ct) = (ct_{00} - ct_{10}, ct_{00} - ct_{20})$. Thus, we have $PK^{-1}_{\tau,\beta_0,\beta_1,\beta_2} = ppk_\tau^{-1} \circ pr$, namely, the secret key $SK_{\tau,\beta_0,\beta_1,\beta_2}$

$$SK_{\tau,\beta_0,\beta_1,\beta_2} = ppk_\tau^{-1} \circ pr \tag{20}$$

satisfies. □

Then we have

Proposition2.3 If the linear mapping ppk_τ of (18) is regular, for a ciphertext ct, the secret key $SK_{\tau,\beta_0,\beta_1,\beta_2}$ satisfies the relation (20). Thus $SK_{\tau,\beta_0,\beta_1,\beta_2}$ is a mapping from $\mathcal{R}^9$ to $\mathcal{R}^2$.

Remark2.3 (1) The general form of ppk_τ depends on Π and (f_0, f_1, f_2).
(2) The equation of τ obtained by $E(v_1)$ is a polynomial equation of a certain degree.
(3) The general form of Π and the degree of $E(v_1)$ with respect to τ depend on the quantization of the parameter t.
(4) The general form of $E(v_1)$ depends on the transformation $C(\tau)$.
(5) When $(\tau, \beta_0, \beta_1, \beta_2) = (4, 1, 2, 3)$,

$$\begin{aligned} Det(ppk_4) = &\frac{1}{2654208 v_0^1 v_0^2}(3v_0^1 - 5v_0^2)(497853(v_0^1)^3 - 1335798(v_0^1)^2(v_0^2) \\ &+ 1552365(v_0^1)(v_0^2)^2 - 415172(v_0^2)^3) \end{aligned}$$

Thus the plaintext $v_0 = (v_0^1, v_0^2)$ that satisfies $3v_0^1 = 5v_0^2$ has $Det(ppk_4) = 0$. There is the ciphertext $ct = PK_{4,1,2,3}(v_0)$, however, the plaintext v_0 is not obtained by the linear mapping ppk_4. Indeed, for any $(\tau, \beta_0, \beta_1, \beta_2)$, the mapping ppk_τ always has non-regular plaintext v_0, where such v_0 is not necessary in the first quadrant of $\mathcal{R}^2$, in general.

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] D.Bao, S.-S. Chern and Z.Shen: *An Introduction to Riemann-Finsler geometry*, 200, Graduate Texts in Math. Springer-Verlag, New York, (2000).
[3] 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).
[4] M. Crampin: Randers spaces with reversible geodesics, Publ. Math.Debrecen, 67(3-4):401-409 (2005).
[5] M. Matsumoto: *Foundations of Finsler geometry and special Finsler spaces.* Kaiseisha Press, Shigaken, 1986.
[6] M. Matsumoto: *Finsler geometry in the 20th-century. In Handbook of Finsler geometry*, Vol. 1, 2, pages 557-966. Kluwer Acad. Publ., Dordrecht, 2003.
[7] T. Nagano, N. Innami, Y. Itokawa and K. Shiohama: Notes on reversibility and branching of geodesics in Finsler spaces, Iasi Ploytechic Inst. Bull.-Mathematics. Theoretical Mechanics. Physics Section, pp.9-28, 2019.
[8] 永野哲也，穴田啓晃: フィンスラー空間の非対称性を用いた公開鍵暗号方式，コンピュータセキュリティシンポジウム 2019 論文集，415-421 (2019).
[9] T. Nagano, H. Anada: One-wayness of Public-Key Encryption Scheme Using Non-symmetry of Finsler Spaces(in Japanese)(Original title: Indistinguishability of Public-Key Encryption Scheme Using Non-symmetry of Finsler Spaces), Proceedings of 2020 Symposium on Cryptography and Information Security, The Institute of Electronics,Information and Communication Engineers, 3A3-1(1-7), (2020).
[10] T.Nagano, H.Anada: Approach to Cryptography from Differential Geometry with Example, Innovative Security Solutions for Information Technology and Communications 2020,Springer Nature, pp.110-129 (2021).
[11] T. Nagano: Notes on the notion of the parallel displacement in Finsler geometry. Tensor (N.S.), 70(3):302-310 (2008).
[12] T. Nagano: On the parallel displacement and parallel vector fields in Finsler geometry, Acta Math. Acad. Paedagog. Nyhazi., 26(2):349-358 (2010).
[13] 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).
[14] 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).
[15] J. Katz and Y. Lindell: *Introduction to Modern Cryptography, Second Edition*, CRC Press, Florida (2014).
[16] 岡本龍明，山本博資: 現代暗号, 産業図書, 東京 (2011).
[17] 岡本龍明: 現代暗号の誕生と発展, 近代科学社, 東京 (2019).
[18] 黒澤　馨: 現代暗号への招待, サイエンス社，東京（2010）.
[19] 黒澤　馨，尾形わかは: 現代暗号の基礎数理, コロナ社，東京（2019）.
[20] 森山大輔，西巻陵，岡本龍明: 公開鍵暗号の数理, 共立出版, 東京 (2011).

付　録

We exhibit the calculation that obtain the value of τ under the following data.

$$(\tau,\beta_0,\beta_1,\beta_2)=(1,\frac{1}{2},\frac{2}{3},\frac{3}{4}),$$
$$v_0=(1516,7084),$$
$$ct=(ct_0,ct_1,ct_2),$$

where

$$ct_0=(ct_{00},ct_{01},ct_{02})=(\frac{6574327027}{4},\frac{-12778117799}{3032},\frac{145661807}{644})$$

$$ct_1=(ct_{10},ct_{11},ct_{12})=(\frac{1237871657}{2},\frac{-18874300661}{13644},\frac{94102555}{1386})$$

$$ct_2=(ct_{20},ct_{21},ct_{22})=(\frac{183233325809}{432},\frac{-853944965495}{982368},\frac{92692874633}{2295216})$$

Start!

Now, from (15), by using ct

$$Det(ppk_\tau)=\frac{5140375407580567\tau^3}{2947104}\neq 0 \text{ (because of } \tau\neq 0)$$

From (16), by using ct, we have a formal solution (v_0^1,v_0^1) as follow

$$\begin{cases} v_0^1=\dfrac{-2(-3921+3163\tau)}{\tau^2}\\ v_0^2=\dfrac{3921+3163\tau}{\tau^2}.\end{cases}$$

Input (v_0^1,v_0^2) to the following energy equation(*).

$$\frac{1}{8}(3\tau^2-2\tau+3)(v_0^1)^2+\frac{1}{4}(1-\tau^2)v_0^1v_0^2+\frac{1}{8}(3\tau^2+2\tau+3)(v_0^2)^2$$
$$=\frac{1}{1952608}(3209270886884104-2167688615345v_0^1\tau$$
$$+4335377230690v_0^2\tau-1946865315933v_0^1\tau^2-3893730631866v_0^2\tau^2).$$

Then we have

$$\frac{1}{8\tau^4}(-292110579+315483660\tau-527209370\tau^2+283265628\tau^3$$
$$+220570661\tau^4)=0.$$

By solving this equation, we obtain $\tau=1$ because that τ is a rational number. □

(*) **About the energy equation.**

From ct_0, we have

$$\Pi_c(\tau)^{-1}\begin{pmatrix}ct_{01}\\ct_{02}\end{pmatrix}=\begin{pmatrix}\frac{1}{2}\tau(1+\tau) & \frac{1}{2}\tau(-1+\tau)\\ \frac{1}{2}\tau(-1+\tau) & \frac{1}{2}\tau(1+\tau)\end{pmatrix}\begin{pmatrix}ct_{01}\\ct_{02}\end{pmatrix}$$
$$=\begin{pmatrix}\frac{1}{2}\tau(1+\tau)ct_{01}+\frac{1}{2}\tau(-1+\tau)ct_{02}\\ \frac{1}{2}\tau(-1+\tau)ct_{01}+\frac{1}{2}\tau(1+\tau)ct_{02}\end{pmatrix}$$
$$=\begin{pmatrix}-\frac{12778117799\tau(1+\tau)}{6064}+\frac{145661807\tau(-1+\tau)}{1288}\\ -\frac{12778117799\tau(-1+\tau)}{6064}+\frac{145661807\tau(1+\tau)}{1288}\end{pmatrix}$$

Thus, we have the energy equation as follows, by using the first component ct_{00} and above 2-dimensional vector,

$$E(v_1)=\Big(\frac{6574327027}{4},-\frac{12778117799\tau(1+\tau)}{6064}+\frac{145661807\tau(-1+\tau)}{1288},$$
$$-\frac{12778117799\tau(-1+\tau)}{6064}+\frac{145661807\tau(1+\tau)}{1288}\Big)\begin{pmatrix}1\\ \frac{1}{2}v_0^1\\ v_0^2\end{pmatrix}.$$

This equation is

$$\frac{1}{8}(3\tau^2-2\tau+3)(v_0^1)^2+\frac{1}{4}(1-\tau^2)v_0^1v_0^2+\frac{1}{8}(3\tau^2+2\tau+3)(v_0^2)^2$$
$$=\frac{1}{1952608}(3209270886884104-2167688615345v_0^1\tau$$
$$+4335377230690v_0^2\tau-1946865315933v_0^1\tau^2-3893730631866v_0^2\tau^2).$$

In addition, from ct_1 and ct_2, we also have the same equation.