Finsler Encryption[⋆]

Tetsuya Nagano[1] and Hiroaki Anada[2]

University of Nagasaki, Nagasaki 851-2195, Japan
hnagano@sun.ac.jp
Aomori University, Tokyo 134-0087, Japan
anada@aomori-u.ac.jp

Abstract. Inspired by previous work with the first example proposed at SecITC 2020, we give a general description of Finsler encryption that is based on a Finsler space, which uses a kind of a differentiable geometry on a smooth manifold, with appropriate quantization as the security parameter. Key generation, encryption and decryption algorithms are introduced in detail, and a further example is presented. Then we analyse security properties of Finsler encryption. First, as the dimension (as another security parameter) increases, the length of the secret key also increases, and hence the computational hardness becomes stronger. Second, we prove indistinguishability against chosen-plaintext attacks.

Keywords: Finsler geometry · Differential geometry · Linear parallel displacement problem · Underdetermined systems of equations · Mapping-decomposition problem

1 Introduction

Finsler encryption is a new cryptographic system that has recently been studied. In previous work[10] proposed at SecITC 2020, an example was given in the case of dimension 2. To capture the intuition, we first state the outline of this system briefly. First of all, we choose a Finsler space with the asymmetric property (See Appendix (2)). Next, the geodesics and the linear parallel displacement must be decided. Both of these are defined by certain differential equations system. And the equation of the energy of a vector is calculated. The key generation is performed using linear parallel displacement of vectors and preserved norms. The obtained key is an $n+1$-dimensional vector consisting of rational expressions with several parameters as components. The n is the dimension of Finsler space. The encryption algorithm generates the ciphertext by calculating several sums of vectors obtained by substituting several given parameter values. On the other hand, the decryption algorithm is performed based on the value of parameter τ obtained from a system of simultaneous linear equations with unknown plaintext components and homogeneous quadratic equations involving the squared

[⋆] This work was supported by Institute of Mathematics for Industry, Joint Usage/Research Center in Kyushu University. (FY2022 Workshop(II) "CRISMATH2022" (2022c006).).

norms of vectors. In the next section, we will present a detailed explanation of the Finsler space used to generate Finsler encryption and its key generation, encryption and decryption. In the following section, we will explain in detail the strength of Finsler encryption, but the intuitive outline is as follows.

If an attacker attempts to decrypt a ciphertext that is encrypted with a public key, he must solve a system of underdetermined equations. This is because, by setting k to be greater than or equal to $n+1$, the number of unknown variables becomes greater than the number of equations that can be obtained from the ciphertext and the public key. Generally, solutions to underdetermined systems of equations can only be obtained in the form that includes unknown constants, which we call "the property of **SUS**". Therefore, determining one plaintext from countless solutions is impossible. Next, finding a "linear parallel displacement" is an assumably computationally hard problem, which we call the Linear Parallel Displacement problem (**LPD problem**). We emphasize that the problem arises from the structure of asymmetric Finsler spaces, and currently no algorithm to solve it known. The last one is the difficulty of solving the composite mapping problem, which we call **Mapping-decomposition problem**. That is, the energy expression is a product of five regular matrices. It is difficult to decompose the energy function, which is a product of five regular matrices, to obtain the five regular matrices.

In this paper, we formalize Finsler encryption in the case of general dimension n. Then we study the strength of our Finsler encryption. Note that we implicitly use the general theory on Finsler geometry and linear parallel displacement, that can be seen in previous publications.

2 Preliminaries

2.1 Public-Key Encryption

A public-key encryption scheme PKE consists three probabilistic polynomial-time (PPT) algorithms; $\mathsf{PKE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$.
• $\mathsf{KeyGen}(1^\lambda) \to (\mathbf{PK}, \mathbf{SK})$. On input the security parameter 1^λ, this PPT algorithm generates a secret key $\mathbf{SK}$ and the corresponding public key $\mathbf{PK}$. It returns $(\mathbf{PK}, \mathbf{SK})$.
• $\mathsf{Enc}(\mathbf{PK}, m) \to ct$. On input the public key $\mathbf{PK}$ and a message m, this PPT algorithm generates a ciphertext ct. It returns ct.
• $\mathsf{Dec}(\mathbf{SK}, ct) \to \hat{m}$. On input the secret key $\mathbf{SK}$ and a ciphertext ct, this deterministic polynomial-time algorithm generates a decrypted message $\hat{m}$. It returns $\hat{m}$.

Correctness should hold for PKE. That is; for any 1^λ and any m,

$$\Pr[m = \hat{m} \mid \mathsf{KeyGen}(1^\lambda) \to (\mathbf{SK}, \mathbf{PK}); \mathsf{Enc}(\mathbf{PK}, m) \to ct; \mathsf{Dec}(\mathbf{SK}, ct) \to \hat{m}] = 1.$$

(cf. [19–21])

2.2 IND-CPA Security of PKE

We prove here the security of indistinguishability against chosen-plaintext attacks is defined by the following experimental algorithm $\mathsf{Exp}^{\text{ind-cpa}}_{\mathsf{PKE},\mathbf{A}}$, where $\mathbf{A}$ is any given PPT algorithm.

```
$\mathsf{Exp}^{\text{ind-cpa}}_{\mathsf{PKE},\mathbf{A}}(1^\lambda)$
  $(\mathbf{SK}, \mathbf{PK}) \leftarrow \mathsf{KeyGen}(1^\lambda));\ (m_0, m_1) \leftarrow \mathbf{A}(\mathbf{PK})$
  $b \in_R \{0,1\};\ ct \leftarrow \mathsf{Enc}(\mathbf{PK}, m_b);\ b' \leftarrow \mathbf{A}(ct)$
  If $b = b'$ then return 1 else return 0
```

The advantage of $\mathbf{A}$ over PKE is defined as

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{PKE},\mathbf{A}}(\lambda) \overset{\text{def}}{=} |\Pr[\mathsf{Exp}^{\text{ind-cpa}}_{\mathsf{PKE},\mathbf{A}}(1^\lambda) = 1] - (1/2)|.$$

PKE is said to be IND-CPA secure if, for any PPT algorithm $\mathbf{A}$, $\mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{PKE},\mathbf{A}}(\lambda)$ is negligible in λ(cf. [18, 19]).

3 Finsler encryption

3.1 Finsler space

Generally, Finsler space (M, F) over the set of real numbers $\mathbb{R}$ is defined as a pair consisting of a smooth n-dimensional manifold M and a scalar function F on its tangent bundle TM([1–6]). Let $x = (x^1, \cdots, x^n)$ be the coordinate of the base manifold M and $y = (y^1, \cdots, y^n)$ the coordinate of a tangent vector y on T_xM. $F = F(x, y)$ is called the Finsler metric or the fundamental function and plays role giving the norm $||y||$ of a tangent vector y. The Finsler metric $F(x, y)$ determines everything in the space. The metric tensor $g_{ij}(x, y)$ which is very important quantity is calculated from $F(x, y)$ as follows:

$$g_{ij}(x, y) := \frac{1}{2}\frac{\partial^2 F^2}{\partial y^i \partial y^j},$$

$$||y||_x = F(x, y) = \sqrt{\sum_{i,j} g_{ij}(x, y) y^i y^j},\ (i, j = 1, \cdots, n).$$

We use the asymmetric property of linear parallel displacement of tangent vectors to construct a new public key encryption.

Necessary objects(See Appendix (2),(3),(4))
(1) Metric tensor field $g_{ij}(x, y)$,
(2) Nonlinear connection $N^i_j(x, y)$,
(3) Horizontal connection $F^i_{rj}(x, y)$,
(where the indices $i, j, r = 1, 2, \cdots, n = dimM$)
(4) Geodesic $c = c(t)$

(5) Linear parallel displacement (LPD) $\mathit{\Pi}_c$ on c is constructed by the solution of the following differential equations:

$$(\star)\quad \frac{dv^i}{dt} + \sum_{j,r} F^i_{jr}(c,\dot{c})v^j\dot{c}^r = 0 \quad (\dot{c}^r = \frac{dc^r}{dt}),$$

and we call the linear map $\mathit{\Pi}_c :\ v(t_0) \in T_pM \ \longrightarrow\ v(t_1) \in T_qM$ a **linear parallel displacement** along $c([7, 14–17])$.
(6) The energy $E(v)$ of a vector $v = (v^1, \cdots, v^n)$ on c:

$$E(v) := \sum_{i,j} g_{ij}(c,\dot{c})v^iv^j$$

Example.
We introduce 2-dimensional Finsler space as follows (i.e. the case $n = 2$)(cf. [8–10]):

$$M := \mathbb{R}^2$$

$(\star\star)$ $F(x, y, \dot{x}, \dot{y}) = \sqrt{a^2\dot{x}^2 + b^2\dot{y}^2} - h_1x\dot{x} - h_2y\dot{y}$ $(a, b, h_1, h_2 :$ positive constant),

where (x, y) is the coordinate of the base manifold M, and $(\dot{x}, \dot{y})$ is the coordinate of $T_{(x,y)}M$, namely, $x = x^1, y = x^2, \dot{x} = y^1, \dot{y} = y^2$.

Geodesics in this Finsler space are any straight lines. So we choose a geodesic as follows

$$c_m(t) = (c^1(t), c^2(t)) = (\frac{1}{a\sqrt{1+m^2}}t, \frac{m}{b\sqrt{1+m^2}}t)\ (y = \frac{am}{b}x).$$

And the linear transformation $C(\tau)$ on $T_pM(p :$ start point) is

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

Then we have 7 parameters $(a, b, h_1, h_2, m, t_0, t_1)$, where t_0, t_1 mean the start point and the end point of the linear parallel displacement on the geodesic c, respectively. In this case the linear parallel displacement $\mathit{\Pi}_{c_m}(t)$ is the solution of $(\star)$ as follows

$$\mathit{\Pi}_{c_m}(t) = \begin{pmatrix} B^1_1 & B^1_2 \\ B^2_1 & B^2_2 \end{pmatrix} \quad \text{(See Appendix (5))},$$

and the energy equation $E(v_1)$ is

$$E(v_1) := < v_1, v_1 >_{\dot{c}} = \sum_{i,j} g_{ij}(c,\dot{c})v^i_1v^j_1 = \ {}^tv_1Gv_1,$$

where $G = \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix}$,

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

However, the components $B_1^1, B_2^1, B_1^2, B_2^2$ are expressed by rationalization as follows:

Rationalization of Forms: For new parameters l and τ or t_2, they are changing as follows:.

$$\begin{aligned}
l^2 &:= a^2b^2(1+m^2) - (b^2h_1 + a^2h_2m^2)t_0, \\
\tau^2(\text{or } t_2^2) &:= l^2 - (b^2h_1 + a^2h_2m^2)t,
\end{aligned}$$

where l must be elected as t_0 is a rational number. The methods of Rationalization, however, are many(See §3.5, 2).

3.2 KeyGen, Enc and Dec of Finsler Encryption

The description hereafter is under the assumption that a real number is approximately represented with a rational number that is a ratio of the form (a λ-bit integer)/(a λ-bit integer). Our Finsler encryption scheme FE consists of three polynomial-time (in λ) algorithms KeyGen, Enc and Dec(cf. [11–13]).

$\mathsf{KeyGen}(1^\lambda)$
Step1. $c(t)$: a geodesic, $p(t_0)$: start point, $q(t_1)$: end point
Step2. v: a vector in $\mathbb{Z}_+^n$(a plaintext), dv: a positive difference vector , $v_0 = (v_0^i) = v + dv$
Step3. $v_1 = C(\tau)v_0$ ($C(\tau)$ is a regular matrix)
Step4. $v_2 = \mathit{\Pi}_c(t_2)v_1$ ($\mathit{\Pi}_c(t_2)$ is the matrix of LPD)
Step5.$E(v_1) = E(v_2) = \sum_{i=0}^n E_i$ where $E_1, \ldots, E_n \in_R \mathbb{Q}[v_0, \tau, t_2], E_0 := E(v_1) - \sum_{i=1}^n E_i$ (because $E(v_1)$ is preserved by LPD)
Step6.$E(v_1) = E(v_2) = \sum_{i=0}^n \frac{E_i}{f_iv_0^i} f_iv_0^i$ where $f_0, \ldots, f_n \in_R \mathbb{Q}_+$; $v_0^0 = 1$
Step 7. $V_3 = \mathit{\Pi}_c(\tau)\ {}^t(\frac{E_1}{f_1v_0^1}, \cdots, \frac{E_n}{f_nv_0^n}) = {}^t(V_3^1, \cdots, V_3^n)$
Step 8. $(\frac{E_0}{f_0}, V_3^1, \cdots, V_3^n)$: an encryption key
$\mathbf{PK} := (\frac{E_0}{f_0}, V_3^1, \cdots, V_3^n)$, $\mathbf{SK} := \{(f_0, \cdots, f_n), \mathit{\Pi}_c(t_2), E(v_1)\}$
Return $(\mathbf{PK}, \mathbf{SK})$.

Note that, for the above **PK** and **SK**, the set of plaintexts should be $\mathbb{Z}_+^n$ and the set of ciphertexts should be a certain subset Cy of $\mathbb{Q}^{(n+1)^2}$.

Next, we obtain the ciphertext ct of a plaintext $v = (v^i)$ by using $1+(n+1)k$ parameters, where $k > n$ as follows:

```
$\mathsf{Enc}(\mathbf{PK}, v)$   $//\mathbf{PK} = (\frac{E_0}{f_0}, V_3^1, \cdots, V_3^n)$
Step1. $k$: Choose a natural number $k$ which is above $n$.
Step2. $\alpha,\ \beta_1, \cdots, \beta_{(n+1)k}$: Each other different rational numbers
Step3. $\{v, \tau \leftarrow \alpha, t_2 \leftarrow \beta_1\}\ \rightarrow\ e_1 = \frac{1}{k}(\frac{E_0}{f_0}, v_3^1, \cdots, v_3^n)$
$\vdots$                              $\vdots$
$\{v, \tau \leftarrow \alpha, t_2 \leftarrow \beta_{(n+1)k}\}\ \rightarrow\ e_{(n+1)k} = \frac{1}{k}(\frac{E_0}{f_0}, v_3^1, \cdots, v_3^n)$
Step4. $ct_1 := \sum_{i=1}^{k} e_i,\ ct_2 := \sum_{i=k+1}^{2k} e_i,\ \cdots,\ ct_{n+1} := \sum_{i=nk+1}^{(n+1)k} e_i$
Step5. $ct = \{ct_1, \cdots, ct_{n+1}\}$: a ciphertext
Return $ct$.
```

Finally, we can decrypt ct and recover the plaintext v by using the secret key $\mathbf{SK} = \{(f_0, \cdots, f_n), \mathit{\Pi}_c(t_2), E(v_1)\}$ as follows:

```
$\mathsf{Dec}(\mathbf{SK}, ct)$   $//\mathbf{SK} := \{(f_0, \cdots, f_n), \mathit{\Pi}_c(t_2), E(v_1)\}$
Step1. $(f_0, f_1, \cdots, f_n) \rightarrow\ sx := (f_0, f_1X_1, \cdots, f_nX_n)$
Step2. $\bar{ct}_1 := (ct_1[[1]], \mathit{\Pi}_c^{-1}(\tau)\ {}^t(ct_1[[2]], \cdots, ct_1[[n+1]]))$
$\vdots$            $\vdots$                    $\vdots$
$\bar{ct}_{n+1} := (ct_{n+1}[[1]], \mathit{\Pi}_c^{-1}(\tau)\ {}^t(ct_{n+1}[[2]], \cdots, ct_{n+1}[[n+1]]))$
Step3. $EX_1 :=< sx, \bar{ct}_1 >, \cdots, EX_{n+1} :=< sx, \bar{ct}_{n+1} >$
Step4.
    $(I)\ \begin{cases} EX_1 &= EX_{n+1} \\ \ \vdots & \vdots\ \vdots \\ EX_n &= EX_{n+1} \end{cases}$
    (System of simultaneous linear equations with $X_1, \cdots, X_n$)
Step5. $\bar{X}_1, \cdots, \bar{X}_n$: formal solution of simultaneous linear equations $(I)$ with unknown $\tau$
Step6. $EX_1|_{X_1 \leftarrow \bar{X}_1, \cdots, X_n \leftarrow \bar{X}_n} - E(v_1)|_{v_0^1 \leftarrow \bar{X}_1, \cdots, v_0^n \leftarrow \bar{X}_n} = 0$
(algebraic equation of $\tau$)
Step7. Solve the **rational number solution** $\tau = \alpha$ and substitute them for $\bar{X}_1, \cdots, \bar{X}_n$
    $v_0 = (v_0^1, \cdots, v_0^n) = (\bar{X}_1|_{\tau \leftarrow \alpha}, \cdots, \bar{X}_n|_{\tau \leftarrow \alpha})$
Step8. Finally, obtain the plaintext $v$ as follows
    $v = v_0 - dv.$
Return $v$.
```

Example
In the Finsler space ($\star\star$) in p.4, we put $(a, b, h_1, h_2, m, t_0, t_1) = (1, 1, 1, 1, 1, \frac{1}{2}, 1)$, then

SK:

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

$$\Pi_{c_m}(\tau) = \begin{pmatrix} \frac{\tau+1}{2\tau^2} & -\frac{\tau-1}{2\tau^2} \\ -\frac{\tau-1}{2\tau^2} & \frac{\tau+1}{2\tau^2} \end{pmatrix}.$$

$$\begin{aligned} E(v_1) = G(v_1, v_1) = {}^tv_2Gv_2 = {}^tv_1\,{}^t\Pi_cG\Pi_cv_1 = {}^tv_0\,{}^tC\,{}^t\Pi_cG\Pi_cCv_0 \\ = \frac{1}{8}(3\tau^2 - 2\tau + 3)(v_0^1)^2 + \frac{1}{4}(1 - \tau^2)v_0^1v_0^2 + \frac{1}{8}(3\tau^2 + 2\tau + 3)(v_0^2)^2 \end{aligned}$$

PK:

$$\mathbf{PK} = (\frac{E_0}{f_0}, V_3^1, V_3^2) \text{ (See Appendix (6)).}$$

From $E(v_1) = (\frac{E_0}{f_0})f_0 + (\frac{E_1}{f_1v_0^1})f_1v_0^1 + (\frac{E_2}{f_2v_0^2})f_2v_0^2 \to V = (\frac{E_1}{f_1v_0^1}, \frac{E_2}{f_2v_0^2})$, $(V_3^1, V_3^2) = V_3 = \Pi_c(\tau)V$. Then, **PK** is obtained.

4 Security Analysis

4.1 Strength of SK

In this section, the strength of each secret key $(f_0, \cdots, f_n)$, $\Pi_c(t_2)$ and $E(v_1)$ is stated about the security from a viewpoint of a calculation amount.

1. $(f_0, \cdots, f_n)$: **Each component is arbitrary rational number.**
2. $\Pi_c(t_2)$: The regular matrix $\Pi_c(t_2)$ is derived from a certain simultaneous differential equations. The differential equations are made by the Finsler metric function F. Therefore nobody knows the equations without F(**LPD problem**, see Appendix (1)). Further, in general, the linear parallel displacement of a Finsler space satisfying asymmetric property is asymmetric, namely,

$$\Pi_c^{-1} \neq \Pi_{c^{-1}}$$

is satisfied. This means that any informations of Π_c^{-1} used in the algorithm of decryption are not obtained from $\Pi_{c^{-1}}$, where c^{-1} is the inverse curve of c. Π_c is an one-way function(cf.[8, 9]).
3. $E(v_1)$: The energy of the vector v_1. This equation is directly affected by the matrix $C(\tau)$. If you replace $C(\tau)$ for the following matrix

$$\begin{pmatrix} \tau & 1 \\ \tau - 1 & 1 \end{pmatrix},$$

then the expression of $E(v_1)$ is changed as follows

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

Therefore nobody knows three coefficients $\frac{1}{8}(4\tau^2 - 4\tau + 3)$, $\frac{1}{2}(2\tau - 1)$ and $\frac{1}{2}$ without recognition of $C(\tau)$. $C(\tau)$ is completely arbitrary regular matrix.
On the other hand, the matrix E is composed by three regular matrixes $C(\tau), \mathit{\Pi}_c(\tau)$ and G, namely,

$$E = {}^tC\ {}^t\mathit{\Pi}_c G \mathit{\Pi}_c C,\ (E(v_1) = {}^tv_0 E v_0),$$

where G is called the Finsler metric tensor field. If E can be decomposed, then the attacker can get $C(\tau), \mathit{\Pi}_c(\tau)$ and G. Then the attacker can decrypt any ciphertext. However, to decompose E to 5-pieces regular matrix ${}^tC$, ${}^t\mathit{\Pi}_c, G, \mathit{\Pi}_c, C$ is computationally hard under the assumption of Mapping-Decomposition Problem(cf.[12, 13]).

4.2 Strength of PK

In the encryption algorithm, the ciphertext ct is made from $(1+(n+1)k)$ parameters β_i at Step3. Each component $ct_i (i = 1, \cdots, n+1)$ of $ct = \{ct_1, \cdots, ct_{n+1}\}$ is made by k-pieces parameters β_j $(j = (i-1)k + 1, \cdots, ik)$. Thus, algebraic equations made by the public key **PK** and ct have the property that the number of its unknown variables is more than ones of equations. For example, in the former case $\mathbf{PK} = (\frac{E_0}{f_0}, V_3^1, V_3^2)$, if $k = 2$, we have the following equation:
If a ciphertext $ct = (ct_1, ct_2, ct_3) = (ct_{11}, ct_{12}, ct_{13}, ct_{21}, ct_{22}, ct_{23}, ct_{31}, ct_{32}, ct_{33})$,
$ct_1 = (ct_{11}, ct_{12}, ct_{13}) \leftarrow \frac{1}{2}(\frac{E_1}{f_0}, V_3^1, V_3^2)|_{t_2 \leftarrow \beta_1} + \frac{1}{2}(\frac{E_1}{f_0}, V_3^1, V_3^2)|_{t_2 \leftarrow \beta_2}$
$ct_2 = (ct_{21}, ct_{22}, ct_{23}) \leftarrow \frac{1}{2}(\frac{E_1}{f_0}, V_3^1, V_3^2)|_{t_2 \leftarrow \beta_3} + \frac{1}{2}(\frac{E_1}{f_0}, V_3^1, V_3^2)|_{t_2 \leftarrow \beta_4}$
$ct_3 = (ct_{31}, ct_{32}, ct_{33}) \leftarrow \frac{1}{2}(\frac{E_1}{f_0}, V_3^1, V_3^2)|_{t_2 \leftarrow \beta_5} + \frac{1}{2}(\frac{E_1}{f_0}, V_3^1, V_3^2)|_{t_2 \leftarrow \beta_6}$
for example, from ct_1, we have following three equations
$ct_{11} = \frac{1}{2}\frac{E_1}{f_0}|_{t_2 \leftarrow \beta_1} + \frac{1}{2}\frac{E_1}{f_0}|_{t_2 \leftarrow \beta_2}$, $ct_{12} = \frac{1}{2}V_3^1|_{t_2 \leftarrow \beta_1} + \frac{1}{2}V_3^1|_{t_2 \leftarrow \beta_2}$, $ct_{13} = \frac{1}{2}V_3^2|_{t_2 \leftarrow \beta_1} + \frac{1}{2}V_3^2|_{t_2 \leftarrow \beta_2}$.
From ct_2,
$ct_{21} = \frac{1}{2}\frac{E_1}{f_0}|_{t_2 \leftarrow \beta_3} + \frac{1}{2}\frac{E_1}{f_0}|_{t_2 \leftarrow \beta_4}$, $ct_{22} = \frac{1}{2}V_3^1|_{t_2 \leftarrow \beta_3} + \frac{1}{2}V_3^1|_{t_2 \leftarrow \beta_4}$, $ct_{23} = \frac{1}{2}V_3^2|_{t_2 \leftarrow \beta_3} + \frac{1}{2}V_3^2|_{t_2 \leftarrow \beta_4}$
From ct_3,
$ct_{31} = \frac{1}{2}\frac{E_1}{f_0}|_{t_2 \leftarrow \beta_5} + \frac{1}{2}\frac{E_1}{f_0}|_{t_2 \leftarrow \beta_6}$, $ct_{32} = \frac{1}{2}V_3^1|_{t_2 \leftarrow \beta_5} + \frac{1}{2}V_3^1|_{t_2 \leftarrow \beta_6}$, $ct_{33} = \frac{1}{2}V_3^2|_{t_2 \leftarrow \beta_5} + \frac{1}{2}V_3^2|_{t_2 \leftarrow \beta_6}$

Thus, in total, we have 9-pieces unknown variables $v_0^1, v_0^2, \tau, \beta_1, \cdots, \beta_6$ and 9-pieces equations. Here k is known, however. In general, for ct_{11}, the attacker must solve the following equation.

$$\frac{1}{k}\frac{E_1}{f_0}|_{t_2 \leftarrow \beta_1} + \cdots + \frac{1}{k}\frac{E_1}{f_0}|_{t_2 \leftarrow \beta_k} = ct_{11}$$

is satisfied. Namely, let $(v_0^1, v_0^2, \tau, k, t_{21}, \cdots, t_{2k})$ be unknown variables, then the attacker must solve the following equation with $(4+k)$-pieces unknowm variables

$$\begin{aligned}
&\frac{1}{64kt_{21}^4}\times \\
&\Big(t_{21}^6\left(3\tau^2(v_0^1)^2-6\tau(v_0^1)^2+3(v_0^1)^2-6\tau^2v_0^1v_0^2+6v_0^1v_0^2+3\tau^2(v_0^2)^2\right.\\
&\quad\left.+6\tau(v_0^2)^2+3(v_0^2)^2\right)\\
&+t_{21}^5\left(-8\tau^2(v_0^1)^2-8\tau(v_0^1)^2+16(v_0^1)^2-8\tau^2v_0^1v_0^2+48\tau v_0^1v_0^2\right.\\
&\quad\left.+8v_0^1v_0^2+16\tau^2(v_0^2)^2+8\tau(v_0^2)^2-8(v_0^2)^2\right)\\
&+t_{21}^4\left(-2\tau^2(v_0^1)^2+28\tau(v_0^1)^2+10(v_0^1)^2+28\tau^2v_0^1v_0^2+24\tau v_0^1v_0^2\right.\\
&\quad\left.-28v_0^1v_0^2+10\tau^2(v_0^2)^2-28\tau(v_0^2)^2-2(v_0^2)^2\right)\\
&+t_{21}^3\left(16\tau^2(v_0^1)^2+16\tau(v_0^1)^2-32(v_0^1)^2+16\tau^2v_0^1v_0^2-96\tau v_0^1v_0^2\right.\\
&\quad\left.-16v_0^1v_0^2-32\tau^2(v_0^2)^2-16\tau(v_0^2)^2+16(v_0^2)^2\right)\\
&+t_{21}^2\left(44\tau^2(v_0^1)^2-40\tau(v_0^1)^2+68(v_0^1)^2-40\tau^2v_0^1v_0^2+48\tau v_0^1v_0^2\right.\\
&\quad\left.+40v_0^1v_0^2+68\tau^2(v_0^2)^2+40\tau(v_0^2)^2+44(v_0^2)^2\right)\\
&+24\tau^2(v_0^1)^2-48\tau(v_0^1)^2+24(v_0^1)^2-48\tau^2v_0^1v_0^2+48v_0^1v_0^2\\
&\quad+24\tau^2(v_0^2)^2+48\tau(v_0^2)^2+24(v_0^2)^2\Big)+\\
&\quad+\cdots\cdots(\text{sum of k-terms})\cdots\cdots+\\
&+\frac{1}{64kt_{2k}^4}\times \\
&\Big(t_{2k}^6\left(3\tau^2(v_0^1)^2-6\tau(v_0^1)^2+3(v_0^1)^2-6\tau^2v_0^1v_0^2+6v_0^1v_0^2+3\tau^2(v_0^2)^2\right.\\
&\quad\left.+6\tau(v_0^2)^2+3(v_0^2)^2\right)\\
&+t_{2k}^5\left(-8\tau^2(v_0^1)^2-8\tau(v_0^1)^2+16(v_0^1)^2-8\tau^2v_0^1v_0^2+48\tau v_0^1v_0^2\right.\\
&\quad\left.+8v_0^1v_0^2+16\tau^2(v_0^2)^2+8\tau(v_0^2)^2-8(v_0^2)^2\right)\\
&+t_{2k}^4\left(-2\tau^2(v_0^1)^2+28\tau(v_0^1)^2+10(v_0^1)^2+28\tau^2v_0^1v_0^2+24\tau v_0^1v_0^2\right.\\
&\quad\left.-28v_0^1v_0^2+10\tau^2(v_0^2)^2-28\tau(v_0^2)^2-2(v_0^2)^2\right)\\
&+t_{2k}^3\left(16\tau^2(v_0^1)^2+16\tau(v_0^1)^2-32(v_0^1)^2+16\tau^2v_0^1v_0^2-96\tau v_0^1v_0^2\right.\\
&\quad\left.-16v_0^1v_0^2-32\tau^2(v_0^2)^2-16\tau(v_0^2)^2+16(v_0^2)^2\right)\\
&+t_{2k}^2\left(44\tau^2(v_0^1)^2-40\tau(v_0^1)^2+68(v_0^1)^2-40\tau^2v_0^1v_0^2+48\tau v_0^1v_0^2\right.\\
&\quad\left.+40v_0^1v_0^2+68\tau^2(v_0^2)^2+40\tau(v_0^2)^2+44(v_0^2)^2\right)\\
&+24\tau^2(v_0^1)^2-48\tau(v_0^1)^2+24(v_0^1)^2-48\tau^2v_0^1v_0^2+48v_0^1v_0^2\\
&\quad+24\tau^2(v_0^2)^2+48\tau(v_0^2)^2+24(v_0^2)^2\Big)\\
&=ct_{11}.
\end{aligned}$$

Further, from ct_{12} and ct_{13},

$$\frac{1}{k}V_3^1|_{t_2\leftarrow\beta_1}+\cdots+\frac{1}{k}V_3^1|_{t_2\leftarrow\beta_k}=ct_{12},$$

$$\frac{1}{k}V_3^2|_{t_2 \leftarrow \beta_1} + \cdots + \frac{1}{k}V_3^2|_{t_2 \leftarrow \beta_k} = ct_{13}$$

are satisfied. After all, $(4+k)$-pieces $(v_0^1, v_0^2, \tau, k, t_{21}, \cdots, t_{2k})$ are unknown variables. Next, from $ct_2 = (ct_{21}, ct_{22}, ct_{23})$, according to the same manner, we have $(4+k)$-pieces $(v_0^1, v_0^2, \tau, k, t_{2(k+1)}, \cdots, t_{2(2k)})$ unknown variables and, further from $ct_3 = (ct_{31}, ct_{32}, ct_{33})$, we have $(4+k)$-pieces $(v_0^1, v_0^2, \tau, k, t_{2(2k+1)}, \cdots, t_{2(3k)})$ unknown variables. Totally, we have $(4+3k)$-pieces $(v_0^1, v_0^2, \tau, k, t_1, \cdots, t_{2(3k)})$ unknown variables. $3k \geq 6$ is true if $k \geq 2$, so unknown variables number satisfies $4 + 3k \geq 10$ if $k \geq 2$. The other side, equation's number is 9, obviously. This means that the simultaneous equations made by 9-pieces algebraic equations are not able to be solved because these are underdetermined on rational numbers (**SUS problem**). In general, if an n-dimensional vector v is a plaintext, then the unknown variables are $n + 2 + (n+1)k$-pieces because the components of v is n-pieces and other parameters are $(2+3k)$-pieces $\left\{k, \tau, \beta_1, \cdots, \beta_{(n+1)k}\right\}$. Therefore the equation's number is $(n+1)^2$ and if $k \geq n+1$ is satisfied then $n + 2 + (n+1)k > (n+1)^2$ is true(Underdetermined system)([13]).

4.3 Length of SK

Finally, we remark the length of the secret key $\mathbf{SK} = \{(f_0, \cdots, f_n), \mathit{\Pi}_c(\tau), E(v_1)\}$. The length depend on the dimension n.
$(f_0, \cdots, f_n)$: $n+1$-pieces arbitrary rational numbers.

$$\mathit{\Pi}_c(\tau) = \begin{pmatrix} \dfrac{a_{11}(\tau)}{b_{11}(\tau)} & \cdots & \dfrac{a_{1n}(\tau)}{b_{1n}(\tau)} \\ \vdots & \ddots & \vdots \\ \dfrac{a_{n1}(\tau)}{b_{n1}(\tau)} & \cdots & \dfrac{a_{nn}(\tau)}{b_{nn}(\tau)} \end{pmatrix}$$

$$E(v_1) = \sum_{i=1}^{n} \frac{a_i(\tau)}{b_i(\tau)}(v_0^i)^2 + \sum_{i<j, i=1,\cdots,n-1, j=2,\cdots,n} \frac{c_{ij}(\tau)}{d_{ij}(\tau)} v_0^i v_0^j,$$

where $a_{ij}(\tau)$ and $b_{ij}(\tau)$ are polynomials of τ of degree p and q and $a_i(\tau), b_i(\tau), c_{ij}(\tau)$ and $d_{ij}(\tau)$ are polynomials of τ of degree r, s, t and w. Therefore all of integer as coefficients of all polynomial $a_{ij}, b_{ij}, a_i, b_i, c_{ij}, d_{ij}$ is $2n + (p+1)n^2 + (q+1)n^2 + rn + sn + t\ {}_nC_2 + w\ {}_nC_2 \approx \alpha n^2 + \beta n + \gamma (\alpha, \beta, \gamma : \text{certain natural numbers})$. Thus we can recognize that *the length of the secret key increases linearly to square of the dimension n* (i.e. $\mathcal{O}(n^2)$).

4.4 IND-CPA Security

We prove here the IND-CPA security of FE under the LPD assumption.

To construct the public key **PK** and the secret key **SK** of FE needs some parameters. In the case of the example of Appendix, the values $(a, b, h_1, h_2, m, t_0, t_1, \alpha, f_0, f_1, f_2)$ and the matrix $C(\alpha), \mathit{\Pi}_c(\alpha)$ are needed. In addition the energy form $E(v_1)$ is also needed. Especially, for **PK**, certain methods of rationalization and splitting are essentially needed. The values $(a, b, h_1, h_2, m, t_0, t_1, \alpha, f_0, f_1, f_2, C(\alpha))$ and the method of splitting of $E(v_1)$ decides **PK**, and the values $(a, b, h_1, h_2, m, t_0, t_1, \alpha)$ and the method of rationalization of t_2 decides $\mathit{\Pi}_c(\alpha)$.

Here, we state the LPD assumption([8–10]).

Computational problem of linear parallel displacement (LPD Problem)
Suppose that each variable is quantized with λ-bit uniformly. (Note that λ is the security parameter.) Let (M, F) be a Finsler space and p, q be points on M. For a geodesic c from p to q, the problem is stated as the computational problem to find values of the parameters of linear parallel displacement along c from T_pM to T_qM, where T_pM, T_qM are tangent spaces at p, q respectively. Formally,

- **Input:** (p, q, c)
- **Output:** A matrix $\mathit{\Pi}_c(\alpha)$ of linear parallel displacement along c from T_pM to T_qM.

LPD Assumption
For a fixed Finsler space with $H^i_j \neq 0$(See Appendix (2)), there exists no polynomial time algorithm to solve a random instance of LPD problem.

We will prove the following theorem.

Theorem 41 *FE has the IND-CPA security under LPD assumption.*

Propositions for Theorem. First we consider the following problem;
Problem Let $\mathit{\Pi}_c(\alpha)$ and $\mathit{\Pi}_c(\alpha')$ be the matrices of the linear parallel displacement made by the values $(a, b, h_1, h_2, m, t_0, t_1, \alpha)$ and $(a, b, h_1, h_2, m, t_0, t_1, \alpha')$, respectively. Then we distinguish $\mathit{\Pi}_c(\alpha)$ and $\mathit{\Pi}_c(\alpha')$, where the method of rationalization is unknown and $(a, b, h_1, h_2, m, t_0, t_1)$ are same values.

We can state the two matrices in the Problem are indistinguishable under LPD assumption.

Proposition 41 *The two matrices in the above Problem are indistinguishable under LPD assumption.*

Proof We assume that the two matrices in Problem are capable of being identified. This assumption means that m-pieces matrices $\mathit{\Pi}_c(\alpha_1), \cdots, \mathit{\Pi}_c(\alpha_m)$ which are correspondent to the different m values $\alpha_1, \cdots, \alpha_m$ are distinguishable.
Now, we have no information of the method of the rationalization of t_2. Then the general form of $\mathit{\Pi}_c(\alpha)$ is put by

$$\mathit{\Pi}_c(\alpha) = \begin{pmatrix} \frac{a_{11}(\alpha)}{b_{11}(\alpha)} & \frac{a_{12}(\alpha)}{b_{12}(\alpha)} \\ \frac{a_{21}(\alpha)}{b_{21}(\alpha)} & \frac{a_{22}(\alpha)}{b_{22}(\alpha)} \end{pmatrix},$$

where the forms $a_{11}(\alpha), a_{12}(\alpha), a_{21}(\alpha), a_{22}(\alpha), b_{11}(\alpha), b_{12}(\alpha), b_{21}(\alpha), b_{22}(\alpha)$ are polynomials with respect to unknown value α. If the amount of unknown coefficients of α of all forms $a_{ij}(\alpha), b_{ij}(\alpha)(i,j=1,2)$ are m, then all coefficients are solvable under informations of distinguished m-pieces matrices $\Pi_c(\alpha_1), \cdots, \Pi_c(\alpha_m)$. Namely, the general form of $\Pi_c(\alpha)$ is obtained. That means that LPD assumption is broken. Therefore this proposition's assertion is true. □

Further, we have the following proposition.

Proposition 42 *In FE, if parameter values $(a, b, h_1, h_2, m, t_0, t_1, f_0, f_1, f_2, \alpha)$ and the values of entries of the matrix of linear parallel displacement $\Pi_c(\alpha)$ are known, then any ciphertext $ct = \{ct_1, ct_2, ct_3\}$ is solvable. Namely, to decrypt any ciphertext is no need of $E(v_1)$.*

Proof Let $ct_1 = (ct_{11}, ct_{12}, ct_{13}), ct_2 = (ct_{21}, ct_{22}, ct_{23}), ct_3 = (ct_{31}, ct_{32}, ct_{33})$ be the components of the ciphertext ct, where all $ct_{ij}(i,j=1,2)$ are rational numbers.
First, respectively, we can obtain $\overline{ct}_{12}, \overline{ct}_{13}, \overline{ct}_{22}, \overline{ct}_{23}, \overline{ct}_{32}, \overline{ct}_{33}$ from ct_1, ct_2, ct_3 and $\Pi_c(\alpha)$ as follows;
$$\begin{pmatrix}\overline{ct}_{12}\\ \overline{ct}_{13}\end{pmatrix} = \Pi_c^{-1}(\alpha)\begin{pmatrix}ct_{12}\\ ct_{13}\end{pmatrix}, \begin{pmatrix}\overline{ct}_{22}\\ \overline{ct}_{23}\end{pmatrix} = \Pi_c^{-1}(\alpha)\begin{pmatrix}ct_{22}\\ ct_{23}\end{pmatrix}, \begin{pmatrix}\overline{ct}_{32}\\ \overline{ct}_{33}\end{pmatrix} = \Pi_c^{-1}(\alpha)\begin{pmatrix}ct_{32}\\ ct_{33}\end{pmatrix}.$$
Next, we can construct the following simultaneous linear equations of X_1, X_2;

$$\begin{cases} ct_{11}f_0 + \overline{ct}_{12}f_1X_1 + \overline{ct}_{13}f_2X_2 = ct_{31}f_0 + \overline{ct}_{32}f_1X_1 + \overline{ct}_{33}f_2X_2 \\ ct_{21}f_0 + \overline{ct}_{22}f_1X_1 + \overline{ct}_{23}f_2X_2 = ct_{31}f_0 + \overline{ct}_{32}f_1X_1 + \overline{ct}_{33}f_2X_2. \end{cases}$$

Finally, the solution X_1, X_2 of the above system leads to the plain text $v = (v^1, v^2)$. In this algorithm, there is no using of $E(v_1)$.□

Proof of Theorem We consider the following game of any given PPT attacker **A** and our FE, (1) to (5), that is in accordance with the experiment $\mathsf{Exp}^{\text{ind-cpa}}_{\mathsf{FE},\mathbf{A}}(1^\lambda)$.
(1) The challenger sends the public key **PK** of FE to the attacker.
(2) The attacker gives two plaintext $m_0, m_1 \in \mathbb{Z}_+^2$ to the challenger (We denote a message as m_i instead of v_i to avoid confusion).
(3) The challenger selects $b = 0$ or $b = 1$ at random.
(4) The challenger selects $\alpha \in \mathbb{Q}_+$ at random and sends the ciphertext $ct_b(\alpha)$ (that is encryption of m_b with $\Pi_c(\alpha)$) to the attacker.
(5) The attacker returns a guess b' to the challenger.

Now we consider another game that is the same as the above procedure (1) to (5) *except* that a simulated $ct_b(\alpha, \alpha')$ is used, which is generated using $\Pi_c(\alpha')$ where a random α' is sampled independently of α, while E_0/f_0 is dependent of α. (This is an analogy of the security proof of IND-CPA security of the El Gamal encryption [18, 19].) Then $\Pi_c(\alpha)$ and $\Pi_c(\alpha')$ are indistinguishable under the LPD assumption because of Proposition 41. Therefore the following relation holds.

$$\left| \Pr[b' = b \mid \Pi_c(\alpha)] - \Pr[b' = b \mid \Pi_c(\alpha')] \right| < \varepsilon \tag{1}$$

On the other hand, $ct_b(\alpha, \alpha')$ is actually a one-time pad because α' is sampled uniformly at random and independently of α, and the components of a ciphtertext, except the E_0/f_0, is obtained by multiplying $\Pi_c(\alpha')$. Therefore $Pr[b' = b|\Pi_c(\alpha')] = \frac{1}{2}$ is true. Thus, the following holds.

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{FE},\mathbf{A}}(\lambda) = \left| \Pr[b' = b \mid \Pi_c(\alpha)] - \frac{1}{2} \right| < \varepsilon \tag{2}$$

Therefore, the theorem holds. □

Remark 41 *In the case of the example in Appendix, the determined differential equations(Appendix* (4)*) is completely solved and the general solution* $\mathit{\Pi}_c(t)$ *is obtained(Appendix* (5)*).*
Therefore there is the polynomial time algorithm to generate key $(\mathbf{PK}, \mathbf{SK})$*.*

4.5 Remarks

In this section, we state other strength, for example, splitting method of $E(v_1)$ and transforming method to rational form for parameter t_2. And any other issues requiring special attention are stated.

1. In Step5 of KeyGen, we treat the splitting $E(v_1) = \sum_{i=0}^{n} E_i$. We first use different parameters t_2, t_3 and make the matrix

$$\widetilde{E} = {}^tC(\tau)\ {}^t\mathit{\Pi}_c(t_3)G(t_2)\mathit{\Pi}_c(t_3)C(\tau)$$

because of $E = {}^tC\ {}^t\mathit{\Pi}_cG\mathit{\Pi}_cC$. Next $\widetilde{E}(v_1) = {}^tv_0\widetilde{E}v_0$ is calculated and is splitted to $\widetilde{E}(v_1) = \sum_{i=0}^{n} \widetilde{E}_i$. And last, parameter t_3 of each component $\widetilde{E}_i$ is change to t_2. In this way, we have the splitting of $E(v_1) = \sum_{i=0}^{n} E_i$. Therefore, by different splitting of $\widetilde{E}(v_1)$ we have other splitting of $E(v_1)$. The splitting method is arbitrary.

2. In §2.1, we use the following transformation because of obtaining rational forms of formations in $G, \mathit{\Pi}_c$

$$t_2^2 := l^2 - (b^2h_1 + a^2h_2m^2)t.$$

However, many other transformations exist, for example,

$$\begin{aligned} t_2^4 &:= l^2 - (b^2h_1 + a^2h_2m^2)t, \\ (t_2+1)^2 &:= l^2 - (b^2h_1 + a^2h_2m^2)t, \\ (\frac{t_2+1}{t_2})^2 &:= l^2 - (b^2h_1 + a^2h_2m^2)t, \\ &\vdots \end{aligned}$$

The transforming method of the parameter t in the solution$(B_1^1, B_2^1, B_2^1, B_2^2)$ of the differential equation $(\star)$ is arbitrary. By using above transformations, all equations in **PK** and **SK** come to algebraic (or rational), fortunately. However, such thing will not always happen to us. Further, the differential equations(which give geodesics in Appendix (4)) which we must solve and its solutions are always complex.

3. Next, we state the regularity of the simultaneous linear equation (I). In Step4 of $\mathsf{Dec}(\mathbf{SK}, ct)$, for the ciphertext $ct = (ct_1, \cdots, ct_{n+1})$, each inner product $EX_1 :=< sx, \bar{ct}_1 >, \cdots, EX_{n+1} :=< sx, \bar{ct}_{n+1} >$ is expressed as follows:

$$\begin{aligned} EX_1 &= ct_{11}f_0 + \bar{ct}_{12}f_1X_1 + \cdots + \bar{ct}_{1(n+1)}f_nX_n \\ &\vdots \qquad \vdots \\ EX_{n+1} &= ct_{(n+1)1}f_0 + \bar{ct}_{(n+1)2}f_1X_1 + \cdots + \bar{ct}_{(n+1)(n+1)}f_nX_n \end{aligned}$$

Then, the determinant Det of (I)

$$Det = \begin{vmatrix} f_1(\bar{c}t_{12} - \bar{c}t_{(n+1)2}) & \cdots & f_n(\bar{c}t_{1(n+1)} - \bar{c}t_{(n+1)(n+1)}) \\ \vdots & \ddots & \vdots \\ f_1(\bar{c}t_{n2} - \bar{c}t_{(n+1)2}) & \cdots & f_n(\bar{c}t_{n(n+1)} - \bar{c}t_{(n+1)(n+1)}) \end{vmatrix}$$

For example, in the case $n = 2$ in p.7,
$Det = \frac{1}{2}(ct_{12}ct_{23} - ct_{12}ct_{33} + ct_{13}ct_{32} - ct_{13}ct_{22} + ct_{22}ct_{33} - ct_{23}ct_{32})\tau^3$
is satisfied. If $Det = 0$, then we can change β_i so that $Det \neq 0$ is satisfied. Therefore the regularity of (I) is recognized from the ciphertext ct only.

4. The encryption map $PK_{\alpha,\beta_1,\cdots,\beta_{(n+1)k}} : \mathbb{Z}_+^2 \to \mathbb{Q}^9$ defined by parameters $(\alpha, \beta_1, \cdots, \beta_{(n+1)k})$ is one to one if $Det \neq 0$ of (I) is satisfied.Namely, different plaintexts $v, \bar{v}(\neq v)$ don't have the same ciphertext $ct = PK_{\alpha,\beta_1,\cdots,\beta_{(n+1)k}}(v) = PK_{\alpha,\beta_1,\cdots,\beta_{(n+1)k}}(\bar{v})$. On the other hand, if $(\alpha, \beta_1, \cdots, \beta_{(n+1)k}) \neq (\bar{\alpha}, \bar{\beta}_1, \cdots, \overline{\beta_{(n+1)k}})$, $PK_{\alpha,\beta_1,\cdots,\beta_{(n+1)k}}(v) \neq PK_{\bar{\alpha},\bar{\beta}_1,\cdots,\overline{\beta_{(n+1)k}}}(v)$ will happen for a plaintext v.

5. We state the solution of the energy equation

$$EX_1|_{X_1 \leftarrow \bar{X}_1, \cdots, X_n \leftarrow \bar{X}_n} - E(v_1)|_{v_0^1 \leftarrow \bar{X}_1, \cdots, v_0^n \leftarrow \bar{X}_n} = 0.$$

This equation is an algebraic equation of a certain degree in τ. Further the real solution's number is two only. In addition, true solution is rational number. Indeed, in Decryption of the case $n = 2$ in p.7, this is an algebraic equation of degree 4 in τ. How to solve this equation? It, however, is no problem because we have known the method of finding rational solutions, for example, Newton-Raphson method for an algebraic equation.
The next problem is particularly important.

6. Does the energy equation

$$EX_1|_{X_1 \leftarrow \bar{X}_1, \cdots, X_n \leftarrow \bar{X}_n} - E(v_1)|_{v_0^1 \leftarrow \bar{X}_1, \cdots, v_0^n \leftarrow \bar{X}_n} = 0$$

have two rational solutions α_1 and α_2? Further, do α_1 and α_2 yield two integer plaintext v, $\bar{v}$? This means that different plaintext $v, \bar{v}$ have the same ciphertext with different parameters $(\alpha, \beta_1, \cdots, \beta_{(n+1)k}) \neq (\bar{\alpha}, \bar{\beta}_1, \cdots, \overline{\beta_{(n+1)k}})$. **This is an open problem.**

7. In 2 above, we state the transformations about t. This is called "coordinate transformation" in differential geometry, in general. Then, the transformation $t = \phi(t_2)$ must satisfy

$$\frac{dt}{dt_2} = \phi'(t_2) \neq 0.$$

If there exist a certain $\tilde{t}$ which satisfies $\phi'(\tilde{t}) = 0$, then we omit such $\tilde{t}$.

5 Conclusion

Based on a Finsler space, we formalized Finsler encryption.
1. We must choose a Finsler space with the asymmetry property(See Appendix (2)).
2. We must choose a geodesic on the Finsler space.

3. We must obtain the linear parallel displacement on the geodesic.
4. The strength is based on the three following open problems (i),(ii),(iii):
(i). LPD problem(See Appendix (1)),
(ii). Mapping-decomposition problem: To decompose the matrix $E = {}^tC\ {}^t\Pi_c G \Pi_c C$ is computationally hard (See §4.1, 3),
(iii). SUS problem: To solve underdetermined system of equations is very hard(See §4.2),
and further, it owes of arbitrariness of $C(\tau)$, splitting of E and the method of rationalization of forms.
5. In Example(p.4), Finsler space is defined as a single (a, b, h_1, h_2), namely, the form $(\star\star)$ expresses the family of Finsler spaces, its amount is about $10^{4\lambda}$(λ is a security parameter). The parameter m expresses a geodesic, and t_0, t_1 express the start point and the end point. Therefore **the amount of $(\mathbf{PK}, \mathbf{SK})$ is about at least** $10^{7\lambda}$.
6. In our Finsler encryption scheme FE, all calculations are over **rational number field** $\mathbb{Q}$ with λ-bit quantization.

Key generation, encryption and decryption were given in detail. For intuitive understanding, an example was presented. Then we analyzed the strength of Finsler encryption. Future direction would be a digital signature scheme on a Finsler space.

Appendix

(1) **LPD problem and LPD assumption**

Computational problem for linear parallel displacement (LPD problem) Suppose that each variable is quantized with λ-bit, uniformly. Let (M, F) be a Finsler space and p, q be points on M. For a geodesic c from p to q, the problem is stated as the computational problem to find values of the parameters of linear parallel displacement along c from T_pM to T_qM, where T_pM, T_qM are tangent spaces at p, q respectively.

LPD assumption
For a fixed Finsler space with $H^i_j \neq 0$, there exists no polynomial time algorithm to solve a random instance of LPD problem.

(2) Let M be an n-dimensional differentiable real manifold. Let (M, F) be a Finsler space with the metric function F which is $2n$-variable real-valued function on the tangent bundle TM. F plays very important role of which geodesic, linear parallel displacement and norm are determined. Further, we assume that

$$H^i_j(x, y) := \sum_r F^i_{rj}(x, y)y^r + \sum_r F^i_{rj}(x, -y)(-y^r) \neq 0$$

where

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

$$\frac{\delta}{\delta x^i} := \frac{\partial}{\partial x^i} - \sum_{r,j} N^r_i(x, y)\frac{\partial}{\partial y^r}.$$

Hereafter the indices $h, i, j, \cdots, p, q, r, \cdots$ of $\sum$ run from 1 to $n(= dimM)$.

(3)

$$N^i_j(x,y) = \sum_r \gamma^i_{rj}(x,y)y^r - \sum_{p,q,r} C^i_{jr}(x,y)\gamma^r_{pq}(x,y)y^p y^q,$$

where

$$\gamma^i_{pq}(x,y) = \sum_h \frac{1}{2}g^{hi}\left(\frac{\partial g_{ph}}{\partial x^q} + \frac{\partial g_{hq}}{\partial x^p} - \frac{\partial g_{pq}}{\partial x^h}\right),$$

$$C^i_{jr}(x,y) = \sum_h \frac{1}{2}g^{hi}\frac{\partial g_{jh}}{\partial y^r}.$$

(4) Geodesic is the curve which is minimizing of the distance between two points locally. Then, a geodesic $c(t) = (c^i(t))$ satisfies the following equation

$$\frac{d^2c^i}{dt^2} + \sum_{j,r} F^i_{jr}(c,\dot{c})\dot{c}^j\dot{c}^r = 0 \quad (\dot{c} = (\dot{c}^i), \dot{c}^i = \frac{dc^i}{dt}),$$

where t is an affine parameter.

(5)

$$\begin{aligned}
B^1_1 = &-\frac{1}{\left(a^2\left(b^2\left(m^2+1\right) - h_2m^2(t+t_0)\right) - b^2h_1(t+t_0)\right)^{3/2}}\times \\
&\bigg(a^2\bigg(h_2{m}^2(t+t_0)\sqrt{a^2\left(b^2\left(m^2+1\right) - h_2m^2t_0\right) - b^2h_1t_0} \\
&- b^2\bigg(\sqrt{a^2\left(b^2\left(m^2+1\right) - h_2m^2(t+t_0)\right) - b^2h_1(t+t_0)} \\
&+{m}^2\sqrt{a^2\left(b^2\left(m^2+1\right) - h_2m^2t_0\right) - b^2h_1t_0}\bigg)\bigg) \\
&+{b}^2h_1t_0\sqrt{a^2\left(b^2\left(m^2+1\right) - h_2m^2(t+t_0)\right) - b^2h_1(t+t_0)}\bigg)
\end{aligned}$$

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

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

$$
\begin{aligned}
&B_2^2 = -\frac{1}{\left(a^2\left(b^2\left(m^2+1\right)-h_2m^2(t+t_0)\right)-b^2h_1(t+t_0)\right)^{3/2}}\times \\
&\Big(-a^2b^2\,\Big(m^2\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2(t+t_0)\right)-b^2h_1(t+t_0)} \\
&+\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2t_0\right)-b^2h_1t_0}\Big) \\
&+b^2h_1(t+t_0)\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2t_0\right)-b^2h_1t_0} \\
&+a^2h_2m^2t_0\sqrt{a^2\left(b^2\left(m^2+1\right)-h_2m^2(t+t_0)\right)-b^2h_1(t+t_0)}\Big)
\end{aligned}
$$

(6)

$$
\begin{aligned}
&\frac{E_0}{f_0} = \frac{1}{64t_2^4}\times \\
&\Big(t_2^6\left(3\tau^2(v_0^1)^2-6\tau(v_0^1)^2+3(v_0^1)^2-6\tau^2v_0^1v_0^2+6v_0^1v_0^2+3\tau^2(v_0^2)^2\ +6\tau(v_0^2)^2+3(v_0^2)^2\right) \\
&+t_2^5\left(-8\tau^2(v_0^1)^2-8\tau(v_0^1)^2+16(v_0^1)^2-8\tau^2v_0^1v_0^2+48\tau v_0^1v_0^2\right. \\
&\quad\left.+8v_0^1v_0^2+16\tau^2(v_0^2)^2+8\tau(v_0^2)^2-8(v_0^2)^2\right) \\
&+t_2^4\left(-2\tau^2(v_0^1)^2+28\tau(v_0^1)^2+10(v_0^1)^2+28\tau^2v_0^1v_0^2+24\tau v_0^1v_0^2\right. \\
&\quad\left.-28v_0^1v_0^2+10\tau^2(v_0^2)^2-28\tau(v_0^2)^2-2(v_0^2)^2\right) \\
&+t_2^3\left(16\tau^2(v_0^1)^2+16\tau(v_0^1)^2-32(v_0^1)^2+16\tau^2v_0^1v_0^2-96\tau v_0^1v_0^2\right. \\
&\quad\left.-16v_0^1v_0^2-32\tau^2(v_0^2)^2-16\tau(v_0^2)^2+16(v_0^2)^2\right) \\
&+t_2^2\left(44\tau^2(v_0^1)^2-40\tau(v_0^1)^2+68(v_0^1)^2-40\tau^2v_0^1v_0^2+48\tau v_0^1v_0^2\right. \\
&\quad\left.+40v_0^1v_0^2+68\tau^2(v_0^2)^2+40\tau(v_0^2)^2+44(v_0^2)^2\right) \\
&+24\tau^2(v_0^1)^2-48\tau(v_0^1)^2+24(v_0^1)^2-48\tau^2v_0^1v_0^2+48v_0^1v_0^2+24\tau^2(v_0^2)^2+48\tau(v_0^2)^2+24(v_0^2)^2\Big),
\end{aligned}
$$

$$
\begin{aligned}
&V_3^1 = \frac{-1}{64\tau^2 t_2^4 v_0^1 v_0^2} \times \\
&\Bigl(t_2^6 \bigl(2\tau^3(v_0^1)^3 - 6\tau^2(v_0^1)^3 + 6\tau(v_0^1)^3 - 2(v_0^1)^3 + 3\tau^3(v_0^1)^2 v_0^2 \\
&\quad -3\tau^2(v_0^1)^2 v_0^2 - 3\tau(v_0^1)^2 v_0^2 + 3(v_0^1)^2 v_0^2 - 12\tau^3 v_0^1(v_0^2)^2 \\
&\quad -12\tau^2 v_0^1(v_0^2)^2 + 12\tau v_0^1(v_0^2)^2 + 12 v_0^1(v_0^2)^2 + 7\tau^3(v_0^2)^3 + 21\tau^2(v_0^2)^3 \ +21\tau(v_0^2)^3 + 7(v_0^2)^3\bigr) \\
&+ t_2^5 \bigl(-4\tau^2(v_0^1)^3 + 8\tau(v_0^1)^3 - 4(v_0^1)^3 - 12\tau^3(v_0^1)^2 v_0^2 - 12\tau^2(v_0^1)^2 v_0^2 \\
&\quad +4\tau(v_0^1)^2 v_0^2 + 20(v_0^1)^2 v_0^2 - 12\tau^3 v_0^1(v_0^2)^2 + 48\tau^2 v_0^1(v_0^2)^2 \\
&\quad +76\tau v_0^1(v_0^2)^2 + 16 v_0^1(v_0^2)^2 + 24\tau^3(v_0^2)^3 + 40\tau^2(v_0^2)^3 + 8\tau(v_0^2)^3 \ -8(v_0^2)^3\bigr) \\
&+ t_2^4 \bigl(-8\tau^3(v_0^1)^3 + 20\tau^2(v_0^1)^3 - 24\tau(v_0^1)^3 + 12(v_0^1)^3 - 30\tau^3(v_0^1)^2 v_0^2 \\
&\quad +6\tau^2(v_0^1)^2 v_0^2 + 26\tau(v_0^1)^2 v_0^2 - 26(v_0^1)^2 v_0^2 + 56\tau^3 v_0^1(v_0^2)^2 \\
&\quad +76\tau^2 v_0^1(v_0^2)^2 - 56\tau v_0^1(v_0^2)^2 - 60 v_0^1(v_0^2)^2 - 38\tau^3(v_0^2)^3 \\
&\quad -106\tau^2(v_0^2)^3 - 110\tau(v_0^2)^3 - 42(v_0^2)^3\bigr) \\
&+ t_2^3 \bigl(8\tau^2(v_0^1)^3 - 16\tau(v_0^1)^3 + 8(v_0^1)^3 + 24\tau^3(v_0^1)^2 v_0^2 + 24\tau^2(v_0^1)^2 v_0^2 \\
&\quad -8\tau(v_0^1)^2 v_0^2 - 40(v_0^1)^2 v_0^2 + 24\tau^3 v_0^1(v_0^2)^2 - 96\tau^2 v_0^1(v_0^2)^2 \\
&\quad -152\tau v_0^1(v_0^2)^2 - 32 v_0^1(v_0^2)^2 - 48\tau^3(v_0^2)^3 - 80\tau^2(v_0^2)^3 - 16\tau(v_0^2)^3 \ +16(v_0^2)^3\bigr) \\
&+ t_2^2 \bigl(8\tau^2(v_0^1)^3 + 8\tau(v_0^1)^3 - 16(v_0^1)^3 + 52\tau^3(v_0^1)^2 v_0^2 + 44\tau^2(v_0^1)^2 v_0^2 \\
&\quad +36\tau(v_0^1)^2 v_0^2 + 108(v_0^1)^2 v_0^2 - 8\tau^3 v_0^1(v_0^2)^2 + 64\tau^2 v_0^1(v_0^2)^2 \\
&\quad +144\tau v_0^1(v_0^2)^2 + 24 v_0^1(v_0^2)^2 + 100\tau^3(v_0^2)^3 + 124\tau^2(v_0^2)^3 + 68\tau(v_0^2)^3 \ +44(v_0^2)^3\bigr) \\
&+ 16\tau^3(v_0^1)^3 - 48\tau^2(v_0^1)^3 + 48\tau(v_0^1)^3 - 16(v_0^1)^3 + 24\tau^3(v_0^1)^2 v_0^2 \\
&\quad - 24\tau^2(v_0^1)^2 v_0^2 - 24\tau(v_0^1)^2 v_0^2 + 24(v_0^1)^2 v_0^2 - 96\tau^3 v_0^1(v_0^2)^2 \\
&\quad - 96\tau^2 v_0^1(v_0^2)^2 + 96\tau v_0^1(v_0^2)^2 + 96 v_0^1(v_0^2)^2 + 56\tau^3(v_0^2)^3 + 168\tau^2(v_0^2)^3 \\
&\quad + 168\tau(v_0^2)^3 + 56(v_0^2)^3\Bigr),
\end{aligned}
$$

$$
\begin{aligned}
&V_3^2 = \frac{1}{64\tau^2 t_2^4 v_0^1 v_0^2} \times \\
&\Big(t_2^6 \left(2\tau^3(v_0^1)^3 - 2\tau^2(v_0^1)^3 - 2\tau(v_0^1)^3 + 2(v_0^1)^3 + 3\tau^3(v_0^1)^2 v_0^2\right. \\
&\quad -25\tau^2(v_0^1)^2 v_0^2 + 25\tau(v_0^1)^2 v_0^2 - 3(v_0^1)^2 v_0^2 - 12\tau^3 v_0^1 (v_0^2)^2 \\
&\quad \left.+20\tau^2 v_0^1 (v_0^2)^2 + 20\tau v_0^1 (v_0^2)^2 - 12 v_0^1 (v_0^2)^2 + 7\tau^3 (v_0^2)^3 + 7\tau^2 (v_0^2)^3 - 7\tau (v_0^2)^3 - 7(v_0^2)^3\right) \\
&+ t_2^5 \left(-4\tau^2(v_0^1)^3 + 4(v_0^1)^3 - 12\tau^3(v_0^1)^2 v_0^2 - 4\tau^2(v_0^1)^2 v_0^2\right. \\
&\quad +52\tau(v_0^1)^2 v_0^2 - 20(v_0^1)^2 v_0^2 - 12\tau^3 v_0^1 (v_0^2)^2 + 88\tau^2 v_0^1 (v_0^2)^2 \\
&\quad \left.-44\tau v_0^1 (v_0^2)^2 - 16 v_0^1 (v_0^2)^2 + 24\tau^3 (v_0^2)^3 - 8\tau^2 (v_0^2)^3 - 24\tau (v_0^2)^3 + 8(v_0^2)^3\right) \\
&+ t_2^4 \left(-8\tau^3(v_0^1)^3 + 4\tau^2(v_0^1)^3 - 12(v_0^1)^3 - 30\tau^3(v_0^1)^2 v_0^2\right. \\
&\quad +114\tau^2(v_0^1)^2 v_0^2 - 126\tau(v_0^1)^2 v_0^2 + 26(v_0^1)^2 v_0^2 + 56\tau^3 v_0^1 (v_0^2)^2 \\
&\quad -84\tau^2 v_0^1 (v_0^2)^2 - 96\tau v_0^1 (v_0^2)^2 + 60 v_0^1 (v_0^2)^2 - 38\tau^3 (v_0^2)^3 \\
&\quad \left.-30\tau^2 (v_0^2)^3 + 26\tau (v_0^2)^3 + 42(v_0^2)^3\right) \\
&+ t_2^3 \left(8\tau^2(v_0^1)^3 - 8(v_0^1)^3 + 24\tau^3(v_0^1)^2 v_0^2 + 8\tau^2(v_0^1)^2 v_0^2\right. \\
&\quad -104\tau(v_0^1)^2 v_0^2 + 40(v_0^1)^2 v_0^2 + 24\tau^3 v_0^1 (v_0^2)^2 - 176\tau^2 v_0^1 (v_0^2)^2 \\
&\quad \left.+88\tau v_0^1 (v_0^2)^2 + 32 v_0^1 (v_0^2)^2 - 48\tau^3 (v_0^2)^3 + 16\tau^2 (v_0^2)^3 + 48\tau (v_0^2)^3 - 16(v_0^2)^3\right) \\
&+ t_2^2 \left(8\tau^2(v_0^1)^3 + 24\tau(v_0^1)^3 + 16(v_0^1)^3 + 52\tau^3(v_0^1)^2 v_0^2 - 28\tau^2(v_0^1)^2 v_0^2\right. \\
&\quad +148\tau(v_0^1)^2 v_0^2 - 108(v_0^1)^2 v_0^2 - 8\tau^3 v_0^1 (v_0^2)^2 + 144\tau^2 v_0^1 (v_0^2)^2 \\
&\quad \left.-96\tau v_0^1 (v_0^2)^2 - 24 v_0^1 (v_0^2)^2 + 100\tau^3 (v_0^2)^3 - 76\tau^2 (v_0^2)^3 + 20\tau (v_0^2)^3 - 44(v_0^2)^3\right) \\
&+ 16\tau^3(v_0^1)^3 - 16\tau^2(v_0^1)^3 - 16\tau(v_0^1)^3 + 16(v_0^1)^3 + 24\tau^3(v_0^1)^2 v_0^2 \\
&\quad - 200\tau^2(v_0^1)^2 v_0^2 + 200\tau(v_0^1)^2 v_0^2 - 24(v_0^1)^2 v_0^2 - 96\tau^3 v_0^1 (v_0^2)^2 \\
&\quad + 160\tau^2 v_0^1 (v_0^2)^2 + 160\tau v_0^1 (v_0^2)^2 - 96 v_0^1 (v_0^2)^2 + 56\tau^3 (v_0^2)^3 \\
&\quad + 56\tau^2 (v_0^2)^3 - 56\tau (v_0^2)^3 - 56(v_0^2)^3\Big).
\end{aligned}
$$

References

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. T.Nagano, H.Anada: Public-Key Encryption Scheme Using Non-symmetry of Finsler Spaces(in Japanese), Proceedings of Computer Security Symposium 2019, Information Processing Society of Japan, pp.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(SCIS 2020), 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 (SecITC) 2020, Springer, LNCS12596, pp.110-129 (2021).
11. T.Nagano, H.Anada: Mathematical Structure of Finsler Encryption, IPSJ SIG Technical Report, Vol.2021-CSEC-95 No.6(Vol.2021-SPT-45 No.6, Vol.2021-EIP-94 No.6), (2021).
12. T.Nagano, H.Anada: Mathematical Structure of Finsler Encryption and Signature, Proceedings of 2022 Symposium on Cryptography and Information Security Osaka(SCIS 2022), Japan & Online, Jan. 18 – 21, 2022, The Institute of Electronics,Information and Communication Engineers, 2A3-2(1-7), (2022).
13. T.Nagano, H.Anada: Finsler Encryption, 2022 Workshop on interaction between Cryptography, Information Security and Mathematics(CRISMATH 2022), Joint Research Center for Advanced and Fundamental Mathematics-for-Industry, Kyushu Univ. Dec. 20-21, 2022
14. T. Nagano: Notes on the notion of the parallel displacement in Finsler geometry. Tensor (N.S.), 70(3):302-310 (2008).
15. T. Nagano: On the parallel displacement and parallel vector fields in Finsler geometry, Acta Math. Acad. Paedagog. Nyhazi., 26(2):349-358 (2010).
16. 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).
17. 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).
18. T. El Gamal: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In proc. CRYPTO 84 on Advances in Cryptology, pp.10–18, 1985.
19. J. Katz and Y. Lindell: *Introduction to Modern Cryptography, Second Edition*, CRC Press, Florida (2014).
20. O. Goldreich: *The Foundations of Cryptography - Volume 1, Basic Techniques*, Cambridge University Press, Cambridge (2001).
21. O. Goldreich: *The Foundations of Cryptography - Volume 2, Basic Applications*, Cambridge University Press, Cambridge (2004).