SCIS 2022 2022 Symposium on Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics, Information and Communication Engineers

Mathematical Structure of Finsler Encryption and Signature

Tetsuya NAGANO * Hiroaki ANADA †

Keywords: Finsler encryption, Public-key encryption, Digital signature, Differential geometry

Abstract

Finsler encryption was defined by Nagano and Anada at [3]. The basic structure of this encryption is supported by the differential geometry, especially, Finsler geometry(cf.[1],[2]). Thus, all items of Finsler encryption are initially introduced by a real and smooth manifold and have continuous real forms. In general, encryption system is constructed in a discrete mathematical system(cf.[5]). By quantization, however, we succeed in changing their forms into integer and rational forms.

In this paper, firstly, we study the mathematical structure of the encryption and decryption algorithm of Finsler encryption([4]). A plaintext is a 2-dimensional vector v. The space of plaintext is the first quadrant of the tangent plane $\mathbb{R}^2$. The algorithm of encoding is, first, transforming by the linear parallel displacement(cf.[2]) with parameter β_i for a vector v, next, calculating the energy of a transformed vector and dividing it. Lastly, we transforms a obtaining vector from dividing by using a linear parallel displacement with τ. For a plaintext v, We do three times the above same calculation with different parameter($\beta_i(i = 0, 1, 2)$). So, the public key PK of Finsler encryption is very complicated form. It has four parameters $(\tau, \beta_0, \beta_1, \beta_2)$. So, when different four parameters are chosen, on each occasion, the function of the encryption is different. We make it clear that the function is a mapping from $\mathbb{R}^2$ to $\mathbb{R}^9$. The ciphertext space is a subset of $\mathbb{R}^9$.

Next, by using a linear simultaneous equations, we decode a cipher. First of all, by using the inverse matrix of linear parallel displacement with τ, we prepare three the energy forms of vector obtained by the linear parallel displacement with parameter β_i for a vector v. These three form represent the same value of the energy. Next, by connecting these three forms with "=", a linear simultaneous equation is obtained. And solving the equation system with unknown parameter τ, if its formal solution is input the energy equation(one of secret key), then we can get a certain algebraic equation of τ with some degree. Final, if the algebraic equation is solved, then we can obtain the plaintext v.

According to the above decryption algorithm, we have two mappings. One of them is a projection pr from $\mathbb{R}^9$ to $\mathbb{R}^2$, and the other is a linear mapping ppk_τ from $\mathbb{R}^2$ to $\mathbb{R}^2$. If the cipher is made by satisfying a certain condition, then ppk_τ is regular. Therefore the mapping $ppk_\tau^{-1} \circ pr$ is constructed and gives the plaintext v from the cipher. However, $ppk_\tau^{-1} \circ pr$ depends on the pair (plaintext, its ciphertext).

Finally, we introduce a digital signature system based on this Finsler encryption. It is very easy. For the keys of Finsler encryption (PK, SK), we should put only the encryption key PK as the the signature(secret) key sk, namely, $sk := PK$, and the decryption key SK as the verification(public) key vk, namely, $vk := SK$, respectively. In addition, we state the encryption strength is similarly to one of Multivariate Public Key Cryptsystems(MPKC).

References

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

[2] 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.

[3] T.Nagano, H.Anada: "Approach to Cryptography from Differential Geometry with Example", *Innovative Security Solutions for Information Technology and Communications 2021,Springer Nature*, pp.110-129 (2021).

[4] T.Nagano, H.Anada: "Mathematical Structure of Finsler Encryption", 2021-CSEC-95, No.6 of IPSJ SIG Technical Report.

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

* University of Nagasaki, 1-1-1, Manabino, Nagayocho, Nagasaki prefecture, Japan (hnagano@sun.ac.jp)
† * (anada@sun.ac.jp)