新公開鍵暗号システムの本人認証及び ディジタル署名の研究

永野哲也　穴田啓晃　(長崎県立大学)*

はじめに

フィンスラー暗号は、永野･穴田が論文「Approach to Cryptography from Differential Geometry with Example」（2020）で定義した。ただし、この暗号システムの基礎的な概念は、微分幾何学のひとつのフィンスラー幾何学、特に、線形平行移動を詳しく論じた永野等の先行研究による。それゆえ、フィンスラー暗号に現れるすべての対象は、可微分な多様体上での幾何的な量である。一般に、暗号システムは、離散数学上の対象として論じられることが多い。しかし、我々は、量子化により、このフィンスラー暗号システムを離散的（整数、有理数）な場の上で機能させることに成功した。今回は、この暗号システムの数学的な構造とその研究により明らかになった構造からディジタル署名の仕組みを新たに提案した。

研究内容

フィンスラー暗号の数学的構造

まず、この暗号システムの暗号化と復号アルゴリズムの数学的構造をしらべた。ただし、今回は、すべて2次元での話である。その結果、暗号化（PK）については、暗号文空間を2次元空間の第1象限の格子点の全体として、そこから、暗号文空間としての9次元の実数空間へのある部分集合への写像であることを明らかにした。この写像は、数学的には、非対称なフィンスラー空間の線形平行移動をその基礎としている。非対称性から、逆の平行移動でも平文にはもどらないという性質がある。つまり、この写像 (PK) は逆が期待できない。

次に、復号アルゴリズム (SK) についての研究は、暗号化がもつ非対称性から工夫が必要であった。そのそもの写像として PK の逆は存在しない。そこで筆者らは、まず、9次元の暗号文空間から、2次元の数空間への写像と暗号文から作られる2次元の平文空間からの逆写像が、復号アルゴリズム (SK) を実現することに気づいた。これらを図示したのが図 1 の可換図式である。

ディジタル署名

フィンスラー暗号の数学構造の研究で明らかになったことのもう一つの点が、ディジタル署名の構造を自然に持ち更にその応用であるグループ署名の構造をも持っているということである。

まず**ディジタル署名**については、暗号化 PK を署名鍵（秘密鍵）とし、復号アルゴリズム SK を認証鍵（秘密鍵）とする。これは、フィンスラー暗号をほぼそのまま使っている。

グループ署名については、フィンスラー暗号では、暗号化に 4 パラメータを必要とする。 1 つのバラメータの値はグループ全員に共通にし、他の 3 つのパラメータをメンバーごとに異なるものとする。すると、検証者は、共通のパラメータ値が同じグルー

* 〒 851-2195　長崎県西彼杵郡長与町まなび野 1-1-1　長崎県立大学 情報セキュリティ学科
e-mail: hnagano@sun.ac.jp

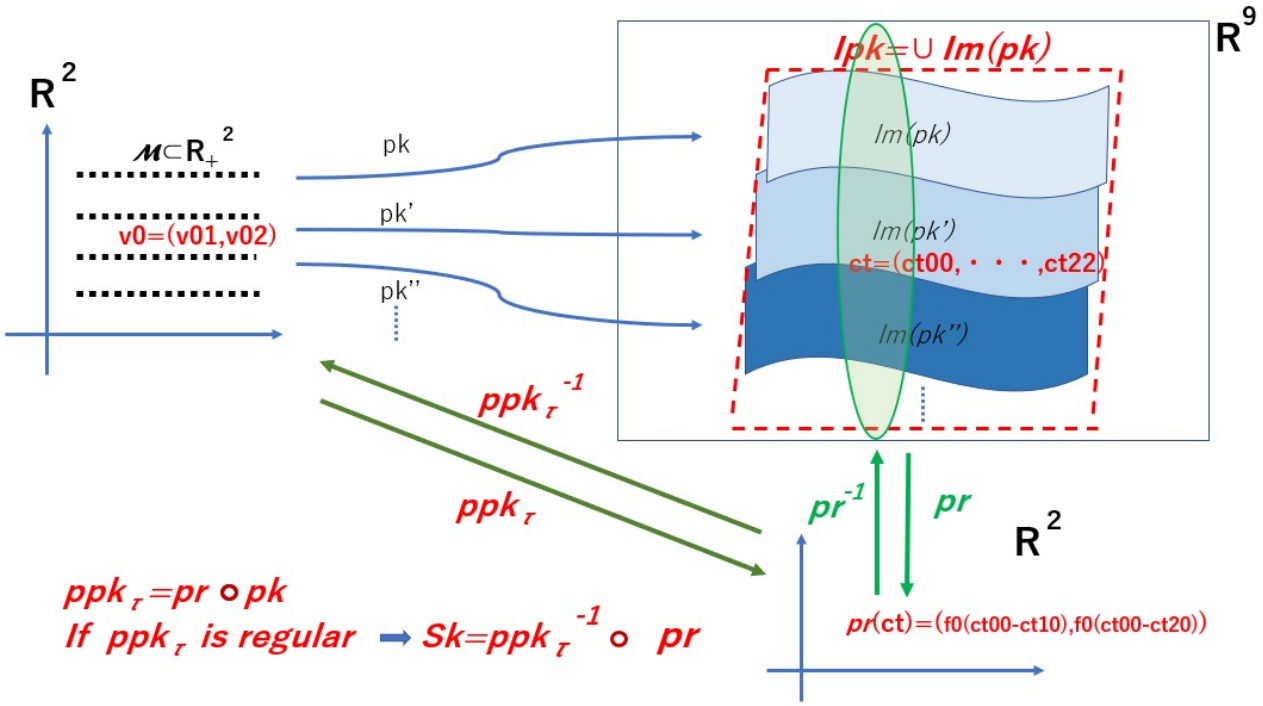

図 1:

プに入る正当なメンバーであることを保証するので、なりすましを防止ができる。しかし、他の 3 つのパラメータ値を求めることができない（署名者の秘匿性が保たれる）ので、ユーザーを特定できない。他の 3 つのパラメータを求められるのは、各ユーザーに署名鍵を配った管理者のみである。

おわりに

現在は、この提案したフィンスラー暗号の強度についての研究が不十分である。今回の数学構造の研究から暗号化鍵には耐量子計算機暗号として候補の一つにあがっている「多変数多項式公開鍵暗号」と同様の強度が期待できるのではないかと推測される。今後は、強度についての研究を深めて、確固たる安全性をもつ新公開鍵暗号システムの構築に努力したい。なお、タイトルにある「本人認証」については、広義のディジタル署名システムに含まれるので割愛した。

参考文献

[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).

T.Nagano, H.Anada: “Mathematical Structure of Finsler Encryption”, 2021-CSEC-95, No.6 of IPSJ SIG Technical Report.

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