公開鍵暗号と線形符号

松田 修三　　平松 豊一

法政大学工学部システム制御工学科

本研究の目的は、公開鍵暗号と線形符号とを結びつけることにある。一般な線形符号の復号問題が NP-完全であることはよく知られている。このことを安全性のよりどころとして公開鍵暗号を構成する。そして、符号をいかに選べばより安全な暗号が得られるかについて論じる。最後の節で、我々は一つの公開鍵暗号を提案する。

1　はじめに

ここでは、線形符号と公開鍵暗号についての諸概念をまとめておく。

1.1　線形符号

p を素数とし、$q = p^l$ (l : 自然数) とおく。q 個の元からなる有限体を $\mathbf{F}_q$ と書く。$\mathbf{F}_q$ 上の n 次元線形空間 $\mathbf{F}_q^n$ の k 次元部分空間 C を (n, k) 線形符号という。C を決めるには 2 つの方法がある。その第一は、C の基底を作る k 個のベクトルを行ベクトルとする $k \times n$ 行列を G とするとき、G の階数は k で、$C = \{aG : a \in \mathbf{F}_q^k\}$ と表される。行列 G を C の生成行列という。次に、

$$C^{\perp} = \{\boldsymbol{x} \in \mathbf{F}_q^n : (\boldsymbol{x}, \boldsymbol{y}) = 0 \ for \ all \ \boldsymbol{y} \in C\}$$

とおく。ここで、$(\boldsymbol{x}, \boldsymbol{y})$ は $\mathbf{F}_q^n$ 内の内積を表す。$C^{\perp}$ は C の双対符号と呼ばれ、$(n, n-k)$ 線形符号である。そこで、$C^{\perp}$ の生成行列を H とするとき、

$$C = \{\boldsymbol{x} \in \mathbf{F}_q^n : xH^t = 0\}$$

が成立する。H を C の検査行列という。これが C の第二の構成方法である。

1.2　公開鍵暗号

次の条件をみたす 5 つの要素からなる $\{P, C, K, E, D\}$ を暗号系という:

1) P は発生しうる平文の有限集合,

2) C は発生しうる暗号文の有限集合,

3) K は可能性のある鍵の有限集合,

4) 任意の $k \in K$ に対し、1 つの暗号化規則 $e_k \in E$ と対応する復号化規則 $d_k \in D$ があり、

$$e_k : P \longrightarrow C, \quad e_k : C \longrightarrow P$$

に対し、全ての $x \in P$ で $d_k(e_k(x)) = x$ が成立する。つまり、e_k は 1 対 1 写像で、d_k と e_k は互いの逆関数である。

与えられた暗号化鍵 e_k から復号化鍵 d_k を求めることが計算量的に実行不可能な場合を「公開鍵暗号」という。このとき e_k を公開することができる。ここで、「計算量的に実行不可能」とは、多項式計算量で計算できないことを意味する。

2　McEliece 暗号

この節では、McEliece 暗号系の導入とその後の発展について述べる。

2.1　McEliece 暗号

まず、NP-完全について説明しよう。多項式時間のプログラムで解決できる問題を多項式時間の問題といい、P で表す。また NP 問題とは、例えば、素数でない自然数が与えられたとき、n の約数を求める問題は P に属さないと予想されている。しかし、n より小さい自然数 a で割ってみて割り切れれば、a は n の約数とわかる。この割り算は多項式時間の問題だから、多項式時間で解けたことになる。しかし、すべての a についてこの方法をやるのは多項式時間でなくなる。このように、うまい試行実験 (今述べた例では、うまい a がみつかること) をしたときに、多項式時間で解ける問題を NP の問題という。P

は NP であるが、P≠NP と予想されている。さて、NP-完全とは、まず、$A(a)$ を NP の命題とする。つまり、自然数 a が $A(a)$ をみたすかどうかを判定するのが NP 問題とする。このとき $A(a)$ が NP-完全とは、$A(a)$ が P なら、すべての NP 命題が P であることを意味する。一般な線形符号の復号問題が NP-完全であることは、1978 年に証明された ([1])。

これを踏まえて McEliece は次のような暗号系を導入した ([4])。C を $\mathbf{F}_q$ 上の (n,k) 線形符号とし、d をその最小距離とする。また、C の生成行列を G とし、S, P をそれぞれ $\mathbf{F}_q$ 上の $k\times k$ 正則行列、$n\times n$ 置換行列とする。$G'=SGP$ を生成行列とする線形符号は、C に属する符号語で座標を入れかえたものから成り立っている。

そこで、G' を公開し、G, S, P を秘密とする公開鍵暗号を次のように定義する。与えられた平文 $\boldsymbol{x}\in\mathbf{F}_q^k$ に対し、$\boldsymbol{e}\in\mathbf{F}_q^n$ をその重さ $w(\boldsymbol{e})\leqq\lfloor\dfrac{d-1}{2}\rfloor(=t)$ となるように任意に選んで、

$$\boldsymbol{y}=\boldsymbol{x}G'+\boldsymbol{e}\ (\in\mathbf{F}_q^n)$$

と暗号化する。そして、その復号は次のように実行される:

1. $\boldsymbol{y}'=\boldsymbol{y}P^{-1}=\boldsymbol{x}SG+\boldsymbol{e}P^{-1}$ を計算する。
2. $w(v\boldsymbol{y}'-\boldsymbol{x}SG)=w(\boldsymbol{e}P^{-1})=w(\boldsymbol{e})\leqq t$ かつ $\boldsymbol{x}SG=(\boldsymbol{x}S)G\in C$ だから、$\boldsymbol{y}'$ に C の復号アルゴリズムを適用して、$\boldsymbol{x}'G\in C$ を得る。
3. $\boldsymbol{x}'G=\boldsymbol{x}SG$ から、$\boldsymbol{x}=\boldsymbol{x}'S^{-1}$ を計算する。

線形符号の復号は、一般には NP-完全であるが、多くの符号のクラスに対してはそれが多項式時間アルゴリズムで可能である。つまり、McEliece の暗号の「安全性のよりどころ」は、NP-完全問題の簡単に解ける特別な符号を使い、あたかもその問題の一般な難しい場合であるかのように見せかけるところにある。そのためには、同じパラメータをもつ本質的に異なる符号が沢山あることが望ましい。また、符号の生成が簡単であり、かつ効率的な復号アルゴリズムが存在することも必要である。

(例 1)

$$G=\begin{pmatrix}1&0&0&0&1&1&0\\0&1&0&0&1&0&1\\0&0&1&0&0&1&1\\0&0&0&1&1&1&1\end{pmatrix}$$

を生成行列とする $\mathbf{F}_2$ 上の $(7,4)$ ハミング符号をとる。そして、S, P を次のように選ぶ:

$$S=\begin{pmatrix}1&1&0&1\\1&0&0&1\\0&1&1&1\\1&1&0&0\end{pmatrix},$$

$$P=\begin{pmatrix}0&1&0&0&0&0&0\\0&0&0&1&0&0&0\\0&0&0&0&0&0&1\\1&0&0&0&0&0&0\\0&0&1&0&0&0&0\\0&0&0&0&0&1&0\\0&0&0&0&1&0&0\end{pmatrix}$$

このとき公開生成行列は

$$G'=\begin{pmatrix}1&1&1&1&0&0&0\\1&1&0&0&1&0&0\\1&0&0&1&1&0&1\\0&1&0&1&1&1&0\end{pmatrix}$$

ここで、平文 $\boldsymbol{x}=(1101)$ を重さ 1 の誤りベクトル $\boldsymbol{e}=(0000100)$ を用いて暗号化を行うと、

$$\begin{aligned}\boldsymbol{y}&=\boldsymbol{x}G'+\boldsymbol{e}\\&=(0110110)\end{aligned}$$

となる。そして、$\boldsymbol{y}$ の復号は次のようである。

$$\begin{aligned}\boldsymbol{y}'&=\boldsymbol{y}P^{-1}\\&=(1000111).\end{aligned}$$

この $\boldsymbol{y}'$ を復号し、$\boldsymbol{x}'G=(1000110)$, $\boldsymbol{x}'=(1000)$. これより、

$$\begin{aligned}\boldsymbol{x}&=S^{-1}\boldsymbol{x}'\\&=(1011).\end{aligned}$$

2.2 その後の発展

$\mathbf{F}_q$ 上の (n,k) 線形符号 C の検査行列を H とし、M, P をそれぞれ $(n-k)\times(n-k)$ 正則行列、$n\times n$ 置換行列とする。$H'=MHP$ とおく。1986 年に、Niederreiter によって次の公開鍵暗号が提案された ([5])。H' を公開し、M, H, P を秘密とする暗号を次のように定義する。

暗号化: 与えられた平文 $\boldsymbol{x} \in \mathbf{F}_q^n$, $w(\boldsymbol{x}) \leqq t$ に対して

$$\boldsymbol{y} = H'\boldsymbol{x}$$

と暗号化する。

復号: $\boldsymbol{y} \in \mathbf{F}_q^{n-k}$ に対し、$\boldsymbol{y}' = M^{-1}\boldsymbol{y} = HP\boldsymbol{x}$ を求め、$\boldsymbol{x}' = P\boldsymbol{x}$ とおく。$w(\boldsymbol{x}') \leqq t$ だから、$\boldsymbol{x}'$ は誤りベクトルである。そこで、シンドローム $\boldsymbol{y}' = H\boldsymbol{x}'$ に C の復号アルゴリズムを適用して $\boldsymbol{x}'$ を計算する。そして、$\boldsymbol{x} = P^{-1}\boldsymbol{x}'$ を得る。

McEliece の公開鍵暗号と Niederreiter のそれとは、次の関係をもつ。どちらか一方を破る問題は他方を破る問題に多項式時間で帰着される ([3])。

3 符号の選択

前節で暗号に適した符号の条件を述べたが、もう一つ大切な条件は、与えられた相対最小距離 d/n 及び q に対し情報率 k/n が可能な限り大きいことが望ましい。この条件は、符号として良い符号であることに他ならない。

$\mathbf{F}_2$ 上の Goppa 符号は、パラメータが

$$n = 2^m,\ k = n - mt,\ d = 2t + 1$$

で与えられる線形符号である。Goppa 符号は、今上で述べた条件の多くをみたしている。McEliece は、$m = 10$, $t = 50$ のときの $(1024, 524)$ Goppa 符号をすすめている。他にも、代数幾何符号は暗号に適した符号といえる。

4 一つの提案

4.1 モジュラー曲線符号

有限体 $\mathbf{F}_q$ 上の種数 g の代数曲線を X とする。X は絶対既約、滑らかで射影的とする。$P_1, \cdots, P_n$ を X 上の $\mathbf{F}_q$-有理点とし、$D = \sum_{i=1}^n P_i$ とおく。X 上の因子で、$\mathbf{F}_q$-有理点のみからなる台をもち D と互いに素なものを G とする。また、G のリーマン・ロッホ空間を

$$L(G) = \{f \in F^\times : \mathrm{div}(f) + G \geqq 0\} \cup \{0\}$$

とおく。ここで、F は X の関数体、$\mathrm{div}(f)$ は f に対応する主因子である。このとき、

$$L(G) \ni \longrightarrow (f(P_1), \cdots, f(P_n)) \in \mathbf{F}_q^n$$

なる $\mathbf{F}_q$-線形写像の像 $C(D, G)$ を代数幾何符号という。$2g - 2 < \deg G < n$ のとき、(n, k) 線形符号 $C(D, G)$ のパラメータは

$$n = \deg G,$$
$$k = \deg G - g + 1,$$
$$d \geqq n - \deg G$$

をみたす。曲線 X がモジュラー関数から得られるモジュラー曲線のとき、$C(D, G)$ をモジュラー曲線符号という ([2])。

4.2 その漸近的性質

モジュラー曲線符号では、定義体 $\mathbf{F}_q$ を固定し種数 g を拡大させることによって、系列的に符号を発生させ、漸近的な符号列を作る。このことを説明しよう。

$$R = \frac{k}{n},\ \delta = \frac{d}{n},\ \gamma = \frac{g-1}{n}$$

、とおくとき、

$$R \geqq 1 - \delta - \gamma$$

が成立する。ここで、$g \to \infty$ とするとき $n \to \infty$ となり、

$$R \geqq 1 - \delta - \frac{1}{\sqrt{q} - 1}$$

を得る。$q \geqq 7^2$ のとき、上の不等式は Varshamov-Gilbert の下界式

$$R \geqq 1 - \delta \log_q(q-1) + \delta \log_q(\delta) + (1-\delta)\log_q(1-\delta)$$

を上回ることを示している。このようなすぐれた符号が構成でき、その高速復号も坂田等によってそのアルゴリズムが完成しつつあることを鑑み、ここにモジュラー曲線符号を利用した公開鍵暗号を提案する次第である。

参考文献

[1] Berlekamp,E.R., MacEliece,R.J. and van Tilborg,H.C.A., On the inherent intractabilty of certain coding problems, IEEE Trans. Inform. Theory, **24** (1978), 384-386.

[2] Hiramatsu,T. and Köhler,G., Coding Theory and Number Theory, Kluwer Academic Publishers, Boston / Dordrecht / London, 2003.

[3] Li,Y.X., Deng,R.H., and Wang,X.M., On the equivalence of McEliece's and Niederreiter's public-key cryptosystems, IEEE Trans. Inform. Theory, **40** (1994), 271-273.

[4] MacEliece,R.J., A public-key cryptosystem based on algebraic coding theory, DSN Progress Report 42-44, pp.114-116.Jet Propulsion Lab., Pasadena, CA, 1978.

[5] Niederreiter,H., Error-correcting codes and cryptography, in Public-Key Cryptosystem and Computational Number Theory, Alster,K., Urabanowicz,J. and Williams,H.C. (Eds.), Walter de Gruyter, 2001, pp.209-219.

キーワード.

公開鍵暗号系, 線形符号, モジュラー曲線符号

Summary

Public-key cryptosystems and linear codes

Shuzo Matsuda Toyokazu Hiramatsu

Faculty of Engineering, Department of Systems and Control Engineering, Hosei University

In this paper, we will give a link between public-key cryptosystems and linear codes. It is well-known that the decoding problem for linear codes is in generally NP-complete. We propose a public-key cryptosystem by using this property.

Keywords.

public-key cryptosystems, linear codes, modular codes.