2004年度 卒業論文

ブラックボックスフィールド問題とその応用

理学部 数学科

1271055H　山本 健児

指導教官 松本 眞

目 次

1　序文

この論文の目的は、ブラックボックスフィールド問題といわれる問題が準指数時間で解けるという事実[1][1] を利用して、Diffie-Hellman 問題と離散対数問題が同程度難しい問題であることを示すことである。

まずはじめに、この論文で使われる基本事項などを紹介する。3 章ではアルゴリズムの時間評価式について考える。4 章ではブラックボックスフィールドとブラックボックスフィールド問題の定義をあたえる。5 章で Diffie-Hellman 鍵交換プロトコルを説明し Diffie-Hellman 問題や離散対数問題との簡単な関係性をみる。最後に、本論文の目的であるブラックボックスフィールド問題を利用して Diffie-Hellman 問題と離散対数問題が部分的に同程度難しい問題であること証明する。

この論文は、多くの部分で [1] を参照した。

2　基本事項

定義 2.1 (群). 集合 G が群であるとは次の 4 つの性質を満たすことである。

1. ある演算 $\circ$ について閉じている。
2. $a, b, c \in G$ のとき、$a \circ (b \circ c) = (a \circ b) \circ c$
3. 任意の $a \in G$ について、$a \circ e = e \circ a = a$ となるような $e \in G$ が存在する。
4. 任意の $a \in G$ について、$a \circ h = h \circ a = e$ となるような $h \in G$ が存在する。

群 G が n 個の元を持つとき、G の位数は n といい。$|G|$ で表す。また、群 G の元 a が n 回目の演算で初めて e になるとき、すなわち

$$(\cdots((\underbrace{a \circ a) \circ a) \cdots) \circ a}_{n}) = e$$

$$(\cdots((\underbrace{a \circ a) \circ a) \cdots) \circ a}_{k \quad (0<k<n)}) \neq e$$

であるとき、元 a の位数は n であるという。

定義 2.2 (部分群). 群 G の空でない部分集合 H が G と同じ演算で群になっているとき、H を G の部分群であるという。

群 G の任意の元 $a, b \in G$ に対して、$a \circ b = b \circ a$ が成り立つとき、この群をアーベル群と呼ぶ。

[1] 厳密には確率的準指数時間であるが本論文では準指数時間として考える

命題 2.3. G をアーベル群とするとき $g \in G$ に対して、$< g >= \{g^n | n \in \mathbb{Z}\}$ は部分群になる。
ここで、$< g >$ のことを巡回群といい。g を群 $< g >$ の生成元と呼ぶ。

定理 2.4. G を有限巡回群とし $g \in G$ をその生成元とする。$|G|$ を割る素数 p に対して、$< g^{|G|/p} >$ は位数 p を持つ部分群となる。

Proof. $h = g^{|G|/p}$ とおく。g は生成元であるので $h = g^{|G|/p} \neq e$ である。h の位数が p であることを示せばよい。今、$h^p = e$ である。ある $k \in \{1, 2, 3, 4, \ldots, p-1\}$ に対して、$h^k = e$ を満たしているとする。p は素数より $GCD(k, p) = 1$ であり、$ak + bp = 1$ なる整数 a, b が存在する。[ユークリッドの互除法を参照] これより $h^{ak+bq} = h$ となるが、$h^{ak+bp} = (h^k)^a (h^p)^b = e$ なので、$h = e$ となり矛盾。 □

3 計算量の評価

3.1 big-O 記法

定義 3.1 (big-O 表記). $f(n), g(n)$ が正の値をとる関数

$$\begin{aligned} f : \mathbb{N} &\rightarrow \mathbb{R}_+ \\ g : \mathbb{N} &\rightarrow \mathbb{R}_+ \end{aligned}$$

とするとき、ある $n_0 \in \mathbb{N}$ に対して、$n > n_0$ となるすべての n に対してある定数 C が存在して不等式 $f(n) \leq Cg(n)$ を満たすとき、$f(n) = O(g(n))$ または $g(n) = \Omega(f(n))$ と書く。

例えば、$x^2 + 3x + 1 = O(x^2)$ である。

3.2 アルゴリズムの時間評価

アルゴリズムの時間を定義するために関数 $L_n(\gamma; c)$ を定義する。

$$L_n(\gamma; c) := e^{c(\log n)^{\gamma}(\log \log n)^{1-\gamma}}$$

とする。

定義 3.2. $L_n(0, c)$ を多項式時間、$L_n(1, c)$ を指数時間、$0 < \gamma < 1$ のとき、$L_n(\gamma, c)$ を準指数時間といい、扱う整数が n であるアルゴリズムのビット演算回数が $O(L_n(0, c)) = O(\log^c n)$ であるようなアルゴリズムを多項式時間アルゴリズムという。また、ビット演算回数が $O(L_n(1, c)) = O(n^c)$ であるようなアルゴリズムを指数時間アルゴリズムという。$0 < \gamma < 1$ に対して、ビット演算回数が $O(L_n(\gamma, c))$ であるようなアルゴリズムを準指数時間アルゴリズムという。

この論文中で使う「時間」とはビット演算回数のことを意味する。

定理 3.3. $L_n(\gamma; c)$ は γ について単調増加関数である。

Proof. 関数 $f(x) = e^x$ は x について単調増加関数であるので、関数

$$g(x) = (\log n)^x (\log\log n)^{1-x}$$

が x について単調増加であることをみる。いま n を固定して、$a = \log n, b = \log\log n$ とおく。$a > b$ である。

$$g'(x) = a^x b^{1-x} \log a - a^x b^{1-x} \log b = a^x b^{1-x} (\log a - \log b) > 0$$

□

定理 3.4. 任意の実数 $a, b \in \mathbb{R}$ に対して

$$L_n(\gamma; a) L_n(\gamma; b) = L_n(\gamma; a + b)$$

が成り立つ。

Proof.

$$e^{a(\log n)^\gamma (\log\log n)^{1-\gamma}} e^{b(\log n)^\gamma (\log\log n)^{1-\gamma}} = e^{(a+b)(\log n)^\gamma (\log\log n)^{1-\gamma}}$$

□

定理 3.5. 正の実数 $\gamma_1, \gamma_2 \in \mathbb{R}$ に対して $\gamma_1 < \gamma_2$ ならば、

$$L_n(\gamma_1; c) L_n(\gamma_2; c) = O(L_n(\gamma_2; 2c))$$

が成り立つ。

Proof.

$$L_n(\gamma_1; c) L_n(\gamma_2; c) < L_n(\gamma_2; c)^2 = L_n(\gamma_2; 2c)$$

□

上記の定理は

$$\text{多項式時間} \cdot \text{多項式時間} = \text{多項式時間}$$

$$\text{準指数時間} \cdot \text{準指数時間} = \text{準指数時間}$$

$$\text{指数時間} \cdot \text{指数時間} = \text{指数時間}$$

であることを示している。

また、特に $T(n)$ が指数時間であるとき

$$T(x) + T(y) \leq T(xy)$$

が成り立つ。

4　ブラックボックスフィールド問題

4.1　ブラックボックスフィールド

ブラックボックスフィールド問題を考えるために、まずブラックボックスフィールドを定義する。以下、ブラックボックスフィールドはBBF、ブラックボックスフィールド問題はBBFPと略す。

定義 4.1. *BBF* は *6* つの組 (p, n, h, F, G, T) で構成される。ここで p は素数で、n は符号化している範囲を表す正の整数である。h, F, G, T は関数で次のように定義する*;*

1. $h : \{0,1\}^n \to \mathbb{F}_p$ は全射とする。すなわち、全ての体 $\mathbb{F}_p$ の元は少なくとも *1* つの *2* 進長により表される。
2. $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ は加法関数といい。次の関係をみたす。$h(F(x,y)) = h(x) + h(y)$。
3. $G : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ は乗法関数といい。次の関係をみたす。$h(G(x,y)) = h(x)h(y)$。
4. $T : \{0,1\}^n \times \{0,1\}^n \to \{true, false\}$ は等号関数といい。次の関係をみたす。$T(x,y) = true \Leftrightarrow h(x) = h(y)$。

ここで、h は全射であるために n は $\log_2 p$ よりも大きい整数である。また、ある $x \in \mathbb{F}_p$ に対応する $\{0,1\}^n$ の元を x のブラックボックス表現といい $[x]$ で表す。定義では $x \in \mathbb{F}$ のブラックボックス表現は複数存在する場合があるが、本論文では $[x]$ の値は2進数での一番小さな値をとることにするにして一意に定める。

4.2　BBFP

次に、ブラックボックスフィールド問題の定義をする。

定義 4.2 (BBFP). (p, n, h, F, G, T) はある素数 p に対する *BBF* とする。[] によりある $[x]$ へ x を送る写像を表す。つまり、

$$[\cdot] : \mathbb{F}_p \to \{0,1\}^n$$

で任意の $x \in \mathbb{F}_p$ に対して $h([x]) = x$ を満たす。*BBFP* とは p, n と多項式時間で計算可能な関数 $F, G, T, []$ だけを使って、ある与えられたブラックボックス表現 $a \in \{0,1\}^n$ からそれに対応する $\mathbb{F}_p$ の元を見つける問題をいう。ここで、a は $T([h(a)], a) = true$ を満たしている。

このBBFPは確率的準指数時間で解ける事が知られている。[1] 本論文ではこれが準指数時間で解けることを仮定する。

5 Diffie-Hellman秘密鍵交換プロトコル

Diffie-Hellman 秘密鍵交換プロトコルは最も古い公開鍵プロトコルの中の 1 つで、1976 年に Whitfield Diffie と Martin E. Hellman によって考案された。

安全でないネットワークを使って秘密鍵を安全に共有するための鍵交換方式である。このプロトコルによって、2 人のひと（ここではアリスとボブとする）が秘密の鍵交換を実行することができる。

簡単のために、ある素数 p を法とするの乗法群 $\mathbb{Z}_p^*$ を使ってプロトコルを説明する。この群は $p-1$ 個の元を含んでいる。 2 人はまず群 G のある生成元 $g \in G$ を決めて公開する。

Step 1 アリスはランダムに整数 $0 < a < |G|$ を選び、g^a を計算しボブに送る。

Step 2 同様にボブもランダムに整数 $0 < b < |G|$ を選び、g^b を計算しアリスに送る。

Step 3 アリスはボブから送られてきた g^b を a 乗し鍵 g^{ab} を得る。

Step 4 同様にボブもアリスから送られてきた g^a を b 乗し鍵 g^{ab} を得る。

こうして得た g^{ab} が共有鍵である。

盗聴者イブは、2 人の通信をすべて傍受することができるとする。また、イブは公開されている群 G とその生成元 $g \in G$ を知ることができる。イブは 2 人の通信路から g^a と g^b を傍受し、秘密の鍵を発見するために、g^{ab} を計算しようと試みる。ここで、次の問題がでてくる。g^a と g^b から g^{ab} を計算できるであろうか？ Diffie-Hellman 関数を以下と定義する。

$$DH_g(g^a, g^b) = g^{ab}$$

この関数を計算する問題のことを Diffie-Hellman 問題という。この表記法で書くときは G は暗黙で巡回群であるとする。Diffie と Hellman は彼らの論文において、$G = \mathbb{Z}_p^*$ 上で関数 $DH_g(x, y)$ を計算することが困難であろうと予想した。

Diffie-Hellman 秘密鍵交換プロトコルは他の群でも定義されている。例は、合成数の乗法群、有限体の上の楕円曲線、有限体の上の超楕円曲線の Jacobian、虚二次体上のクラス群などがある。すべてのこれらの群において関数 $DH_g(x, y)$ の計算が困難であることが信じられている。

また、他のいくつかの暗号系は Diffie-Hellman 問題に依存している。例えば、ElGamal 公開鍵暗号などがある。

古い暗号の未解決問題は、$DH_g(x, y)$ を計算することが、群 G 上の離散対数問題と同じぐらい難しいかどうかである。離散対数問題とは、ある群 G 上の元 $g, x \in G$ が与えられたとき、$g^a = x$ を満たすような自然数 a を求める問題である。離散対数関数は $Dlog_g(x) = a$ と定義される。$Dlog_g(x)$ を多項式時間で解くアルゴリズムが

存在するとき、$DH_g(x,y)$ を多項式時間に計算できることはやさしい問題である。難しい問題は、逆が成り立つかどうかである。すなわち、$DH_g(x,y)$ を計算するための演算が与えられたとき、どのぐらい時間の計算で $Dlog_g(z)$ を解くことができるかということである。この問題は未だ未解決である。次の章で、その問題の部分的な定理と証明を示す。

6 Diffie-Hellman 秘密鍵交換プロトコルの安全性

この章では、Diffie-Hellman 問題の安全性を示す。まず証明のための準備をする。

6.1 証明の準備

[**ユークリッドの互除法**] 自然数 $a > b$ が与えられたとき、次の方法を繰り返すことにより最小公倍数を求めることができる。

Step 1 a を b で割り商を q_1 と剰余を r_1 する。$a = q_1 b + r_1$

Step 2 b を r_1 で割り商を q_2 と剰余を r_2 する。$b = q_2 r_1 + r_2$

Step 3 r_1 を r_2 で割り商を q_3 と剰余を r_3 する。$r_1 = q_3 r_2 + r_3$

$\vdots$

同様に繰り返す

このように、繰り返すことによって $r_1, r_2, \ldots,$ は剰余で $r_1 > r_2 > \cdots$ なので最後には 0 になる。r_n で初めて 0 なったとき、r_{n-1} が最大公約数である。

定理 6.1. 自然数 $a > b$ が与えられたときユークリッドの互除法で最小公倍数を求めるアルゴリズムは高々$O(\log a)$ 回のステップで計算できる。

Proof. $r_{i+2} < \frac{1}{2} r_i$ であることを示す。
もし、$r_{i+1} \leq \frac{1}{2} r_i$ ならば、$r_{i+2} < r_{i+1} \leq \frac{1}{2} r_i$ となる。
もし、$r_{i+1} > \frac{1}{2} r_i$ ならば、$r_{i+2} = r_i - q_{i+1} r_{i+1} < (1 - \frac{q_{i+1}}{2}) r_i$ が成り立つ。$q_{i+1} > 1$ より $r_{i+2} < \frac{1}{2} r_i$ となる。したがって、高々$O(\log a)$ 回のステップで計算できる。□

各ステップで一定の多項式演算を行うので最大公約数を求めるアルゴリズムに要する時間は $O(\log^2 a)$ となる。

例 6.2. $a = 9672, b = 8437$ を考える。まず、$a = 9672$ を $b = 8437$ で割ると $q_1 = 1, r_1 = 1235$。
次に、$b = 8437$ を $r_1 = 1235$ で割ると商は $q_2 = 6$、余りは $r_2 = 1027$。
$r_1 = 1235$ を $r_2 = 1027$ で割ると商は $q_3 = 1$、余りは $r_3 = 208$。
$r_2 = 1027$ を $r_3 = 208$ で割ると商は $q_4 = 4$、余りは $r_4 = 195$。
$r_3 = 208$ を $r_4 = 195$ で割ると商は $q_5 = 1$、余りは $r_5 = 13$。
$r_4 = 195$ を $r_5 = 13$ で割ると商は $q_6 = 15$、余りは $r_6 = 0$。
よって $GCD(9672, 8437) = 13$

このアルゴリズムを使うと、与えられた整数 a, b に対して、

$$na + mb = GCD(a, b)$$

を満たす整数 n, m を構成することができる。その方法を例によって示す。

例 6.3. 上の 例 6.2 で考えると、

$$\begin{aligned}
13 &= 208 - 195 \\
&= 208 - (1027 - 208 \cdot 4) \\
&= 208 \cdot 5 - 1027 \\
&= (1235 - 1027) \cdot 5 - 1027 \\
&= 1235 \cdot 5 - 1027 \cdot 6 \\
&= 1235 \cdot 5 - (8437 - 1235 \cdot 6) \cdot 6 \\
&= 1235 \cdot 41 - 8437 \cdot 6 \\
&= (9672 - 8437) \cdot 41 - 8437 \cdot 6 \\
&= 9672 \cdot 41 - 8437 \cdot 47
\end{aligned}$$

次に、よく知られた中国式剰余の定理を証明する。

定理 6.4 (中国式剰余の定理). $m_1, \ldots, m_n$ を 1 より大きい整数とし、どの 2 つも互いに素とする。このとき、任意の整数の組 $c_1, c_2, \ldots, c_n$ に対して、連立合同式

$$\begin{aligned}
x &\equiv c_1 \mod m_1 \\
x &\equiv c_2 \mod m_2 \\
x &\equiv c_3 \mod m_3 \\
&\vdots \\
x &\equiv c_n \mod m_n
\end{aligned}$$

は解を持ち、$m = m_1 m_2 \cdots m_n$ を法として一意に定まる。

Proof. (一意性を示す) x, x' がともに解となるとき、$x - x'$ はすべての i について m_i で割り切れる。したがって、m でも割り切れるので、$x \equiv x' \mod m$

(存在性を示す) $M_i = m/m_i \ \ (i = 1, 2, 3, \ldots, n)$ とする。M_i と m_i は互いに素なので、ユークリッドの互除法により $a_i Mi \equiv 1 \mod m_i \ \ (i = 1, 2, 3, \ldots, n)$ となる整数 a_i を構成できる。$x = \sum_{i=1}^{n} c_i M_i a_i$ とする。このとき、$j \neq i$ ならば $m_i | M_j$ なので、和の中の i 番目以外の項はすべて m_i によって割り切れる。よって、x は連立合同式の解となる。 □

次に、中国式剰余で連立合同式の解を構成する時間を評価する。

定理 6.5. 中国式剰余で解を構成する時間は高々$O(\log^3 m)$ である。

Proof. まず、$\log m > n$ である。なぜなら

$$\log m = \log m_1 + \log m_2 + \cdots + \log m_n > n$$

解を構成するステップは次のようになる。

Step 1 m を求める。すなわち、$m = m_1 m_2 \cdots m_n$ を計算する。

Step 2 各 i に対して、M_i を計算する。

Step 3 各 i に対して、ユークリッドの互除法により a_i を計算する。

Step 4 最後に、$x = \sum_{i=1}^{n} c_i M_i a_i$ を計算する。

Step 1 は $n-1$ 回の積算が必要であるから、その計算時間は $O(\log m)$ である。*Step* 2 は n 回の除算が必要であるから、その計算時間は $O(\log m)$ である。*Step* 3 は n 回のユークリッドの互除法が必要であるから、その計算時間は $O(\log m \cdot \log^2 m) = O(\log^3 m)$ である。*Step* 4 は $2n$ 回の積算と $n - 1$ の和算が必要であるから、その計算時間は $O(2 \log m + \log m) = O(\log m)$ である。よって、その総計算時間は $O(\log m + \log m + \log^3 m + \log m) = O(\log^3 m)$ となる。 □

補題 6.6 (Pohlig-Hellman). G を有限巡回群とし、$|G|$ の素因数分解が知られているとする。もし、位数 p が素数である任意の元 $h \in G$ に対して $Dlog_h(x)$ が時間 $T(p)$ で計算できると仮定するとき、任意の元 $g \in G$ に対する $Dlog_g(x)$ は、時間 $T(|G|) \log^{O(1)} |G|$ に計算できる。

Proof. $|G| = \Pi_{j=1}^{r} p_j^{\alpha_j}$ とし p_j はそれぞれ異なった素数とする。G の元 $x = g^a$ とするとき、$Dlog_g(x)$ を計算したい。すべての j に対して $a \mod p_j^{\alpha_j}$ を求めることができれば定理 6.4 によって a を構成することができる。

p は $|G|$ を割り切る素数として、p^α は $|G|$ を割り切る最も高い指数を持つ数とする。まず、$b = a \mod p^k$ が分かっていると仮定する。$0 \leq k < \alpha$(最初は$b = k = 0$)。次にどのように $\mod p^{k+1}$ を決定するかを示す。

まずはじめに、$h = g^{|G|/p}$ を計算する。定理 2.4 より元 h は素数位数を持つ。すなわち、h は G の素数位数の部分群を生成する。また、$a \mod p^{k+1}$ を計算するために $y = (xg^{-b})^{|G|/p^{k+1}}$ の値を計算する。

$a - b$ が p^k によって割り切れるので、元 y は次のように表現される。

$$y = (xg^{-b})^{|G|/p^{k+1}} = g^{(a-b)|G|/p^{k+1}} = g^{\frac{|G|}{p}\frac{a-b}{p^k}} = h^{(a-b)/p^k} \tag{1}$$

これは、y が、h により生成された部分群にあることを示す。h は素数位数を持つので仮定より $t = Dlog_h(y)$ を計算できる。$t = (a-b)/p^k \mod p$ である。これを変形すると、ある整数 m があって

$$\begin{aligned} t - (a-b)/p^k &= mp \\ tp^k - (a-b) &= mp^{k+1} \\ a - (b + tp^k) &= mp^{k+1} \end{aligned}$$

これは $a \equiv b + tp^k \mod p^{k+1}$ を意味している。

従って、$b = a \mod p^k$ が与えられたら、$b' = a \mod p^{k+1}$ を計算することができた。この手続を繰返すことにより $a \mod p^\alpha$ が計算できる。この方法ですべての j について $a \mod p_j^{\alpha_j}$ を計算することができる。そして、p_j は互いに異なった素数であるので中国式剰余定理より a を構成することができる。総計算時間は、$|G|$ の各素因数 p_i に対して α_i 回の $Dlog_h(y)$ の計算が必要であるり、一定のビット演算を必要としているので、$\Sigma_i \alpha_i T(p_i) \log^{O(1)} p \leq T(|G|) \log^{O(1)} |G|$。となる。中国式剰余の時間は $\log^{O(1)} |G|$ に含まれる。 □

6.2 安全性の証明

Diffie-Hellman プロトコルの安全性と BBFP の関係は以下の定理で述べる。すなわち、BBFP が準指数時間に解くことができるということを仮定して。

離散対数が準指数時間で解けない ⇒Diffie-Hellman 問題は準指数時間で解けない

ということを対偶を使って示す。

定理 6.7. 時間 $T_{BBF}(p)$ で体 $\mathbb{F}_p$ 上の *BBFP* を解くことができると仮定する。G を $|G|$ の因数分解が知られているある有限巡回群とする。任意の素数位数の元 $h \in G$ に対して $DH_h(x, y)$ は、時間 $T_{DH}(|G|)$ で計算できると仮定するとき、任意の元

$g \in G$ に対して、関数 $Dlog_g(x)$ は時間

$$T_{BBF}(|G|)T_{DH}(|G|)\log^{O(1)}|G|$$

で計算できる。

Proof. g を G の生成元として、$x = g^a$ とする。$Dlog_g(x)$ を計算したい。はじめに、G が素数位数のときを示す。$DH_g(x, y)$ を計算することを BBFP に変換する。$\mathrm{BBF}(p, n, h, F, G, T)$ を次のように定める。

- $p = |G|$
- $n = \lceil \log |G| \rceil$
- $h(x) = Dlog_g(x)$
- $F : [a], [b]$ に対して,$g^a g^b$ を定める。
- $G : [a], [b]$ に対して,$g^{ab} = DH_g(g^a, g^b)$ を定める。
- $T : [a], [b]$ に対して,$T([a], [b]) = \begin{cases} true & (a = b) \\ false & (a \neq b) \end{cases}$

$[]$ は $a \in \mathbb{F}_p$ に対して $[] : a \mapsto g^a$ とする。$[a] = x$ の BBFP のアルゴリズムは x を入力すると a を出力する事であった。仮定より、BBFP を解くアルゴリズムは $T_{BBF}(|G|)$ で計算される。

また、このアルゴリズムは多くても $T_{BBF}(|G|)$ 回の掛け算の演算を必要とする。よって、総計算時間は $O(T_{BBF}(|G|)T_{DH}(|G|))$ である。

$|G|$ が素数でないとき、補題 6.6 を使つかう。p を $|G|$ を割る素数とし、$h = g^{|G|/p}$. とおく。h により生成された群は、定理 2.4 より素数位数をもつ。仮定によって $DH_h(x, y)$ は 時間 $T_{DH}(p)$ で計算できる。また、上の議論により $Dlog_h(y)$ は時間 $T_{BBF}(p)T_{DH}(p)$ で計算できる。補題 6.6 より任意の G の元 g に対して、$Dlog_g(x)$ が時間 $T_{BBF}(|G|)T_{DH}(|G|)\log^{O(1)}|G|$ で計算できることが示された。 □

7 謝辞

最後になりましたが、本論文を仕上げるに当たりまして、ご助言とご指導をいただいた松本眞教授をはじめ様々なサポートして下さった方々に感謝いたします。

参考文献

[1] Dan Boneh, Richard Lipton 『Searching for Elements in Black Box Fields and Applications』

[2] Johannes A.Buchmann 『INTRODUCTION TO CRYPTOGRAPHY』 Springer

[3] N. コブリッツ 櫻井幸一訳 『数論アルゴリズムと楕円暗号理論入門』 Springer

[4] N. コブリッツ 林彬訳 『暗号の代数理論』 Springer