平成16年度卒業論文

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

理学部数学科
1371054F 上野 絵理

平成17年2月10日

目 次

第1章　はじめに

通信網の発達により、インターネットを使った情報交換は、身近で日常的なものとなってきている。情報流通の増大により、情報保護は追いつかず、情報内に隠された人々のプライバシーが第三者に浮き彫りになる可能性も高い。また、通信上の罠やトラブル、詐欺など多くの危険も潜んでいる。社会的にも通信への依存性が高まる中、使用を中断せずに打開策を考えるしかない。そこで、安全に情報を交わすためには利用者それぞれが危機感を高め、自ら防衛策をはる必要がある。自己防衛策の一つとして、暗号がある。

ビジネスや日常生活で利用する公衆網による電話を例に挙げる。電話のセキュリティ上の問題の一つとして、ストーカーの話題や某金融業者による事件などで話題になった盗聴がある。これから急速な普及が期待されるインターネット電話でもこの問題は、公衆網の場合以上に深刻化することが予測される。これは、IP（InternetProtocol）を利用するがために、技術的にも、公衆網以上に盗聴しやすくなることが考えられるからである。そのための対策として暗号化が使われている[1]。

ここでは、暗号についての正確な定義と論文の目的について述べる。

1.1　暗号とは

ネットワークを利用して秘密裏に情報を交換したい 2 人（送信者、受信者）が、第 3 者に傍受されている安全でない通信網を使う際に、暗号が必要となる。暗号の古典的な手法は暗号系である。

暗号系を定義する。

[1] http://enterprise.watch.impress.co.jp/cda/special/2004/05/28/2286.html

Definition 1.1 (暗号系の定義). 次の性質をもつ $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ の 5 つの成分からなる組を暗号系、または暗号化方式という。

1. $\mathcal{P}$ は集合であり平文空間という。その元を平文と呼ぶ。
2. $\mathcal{C}$ は集合であり暗号文空間という。その元を暗号文または暗号化文と呼ぶ。
3. $\mathcal{K}$ は集合であり鍵空間という。その元を鍵と呼ぶ。
4. $\mathcal{E} = \{E_k : k \in \mathcal{K}\}$ は関数 $E_k : \mathcal{P} \to \mathcal{C}$ の族である。その元を暗号化関数と呼ぶ。
5. $\mathcal{D} = \{D_k : k \in \mathcal{K}\}$ は関数 $D_k : \mathcal{C} \to \mathcal{P}$ の族である。その元を復号化関数と呼ぶ。
6. 全ての $p \in \mathcal{P}$ に対して、次のことが成り立つ: 任意の $e \in \mathcal{K}$ に対して、等式 $D_d(E_e(p)) = p$ が成り立つような $d \in \mathcal{K}$ が存在する。

ここで、暗号理論の分野で用いられる用語の解説を行う。

平文：暗号化される前の文書、あるいはデータ

暗号文：暗号化された文書、あるいはデータ

暗号化：平文を暗号文に変換する操作

復号（化）：正規の利用者が暗号文を平文に変換する操作

解読：第三者が暗号文を平文に変換する操作

oracle：内部構造はわからないが値を入力した瞬間に出力値を必ず返すこと

（oracle は別名、神託、神のお告げとも呼ばれる）

1.2 論文の目的

論文は参考文献 [1] をまとめたものである。

この論文を書くに至った背景を述べる。暗号は共通鍵暗号と公開鍵暗号の 2 つに大別される。送信側における暗号化鍵と受信側における複合化鍵とが同一である暗号系を共通鍵暗号と称する。暗号は古い歴史を有しているが、従来の暗号はすべてこのタイプに属している。公開鍵暗号と共通鍵暗号の著しい差は、公開鍵暗号においては暗号化鍵と複合化鍵とが異なっていることである。通常、公開鍵暗号においては、その複合化鍵を暗号化鍵から導くことが計算量の点できわめて困難となり、この理由によって暗号化鍵を公開することができ

る。共通鍵暗号の場合、暗号通信したい相手ごとに個別の秘密鍵を安全に共有し管理する必要がある。その秘密鍵共有交換プロトコルに Diffie – Hellman 秘密鍵交換方式がある。当初、論文の目的は Diffie – Hellman 秘密鍵交換方式ついて述べることであった。Diffie – Hellman 秘密鍵交換方式の安全性は、離散対数問題を解く難しさと同値であるという予想に基づいている。この予想は未だ証明されていない。ここで、参考文献 [1] によると、BBF 上では同値であることが示されている。この内容をも盛り込んで論文を書く予定であったが、BBF の概念を修得する段階で留まり、目的を変更して、この論文では、BBF と BBFP の正確な定義を与え、慣れ親しむことが目的となった。BBFP に対するアルゴリズムは Diffie – Hellman 秘密鍵交換方式の安全性を証明することにも使われうるため重要な事前準備といえる。また、任意の代数的準同型暗号化スキームと定式化される暗号系が準指数時間で解読できることを証明することも論文の目的の一つとする。これにより、暗号系が準指数時間で解読できることを示すためには、代数的に準同型であるかどうかを調べれば十分であることがいえ、暗号解析に対する一般的な手法を与える重要な定理であることがわかる。

BBF は暗号利用を目的とした抽象的代数構造である。代数構造とは、ある母集団において演算に閉じている集合を指す。計算機を用いる際の、代数的準同型暗号化スキームと定式化された暗号系から BBF との対応を与えることができる。この場合、暗号化と復号化の鍵はそれぞれ一つに定まっている。暗号には様々なものがあるが、それらは数学的根拠の元、各々の数学的体系を構築している。実際に計算機を用いて処理する場合、代数構造をもつ BBF との対応を考えることでその理論の解析につなげることができる。この論文中で示す定理の証明においても、BBF に対する準指数アルゴリズムの存在に基づいて、代数的準同型暗号化スキームと定式化される暗号系と BBF との対応により暗号系が準指数時間で解読できることを示している。

暗号の復号（化）と解読は同じ意味で用いられる場合も多いが、復号と解読は全く別の意味で用いられる場合があることに注意されたい。暗号の解読は本来、不正な利用者が盗聴、改ざん、なりすましなどを目的に行われる場合を想定している。しかしながら、アルゴリズムが公開されている現代暗号においては、その暗号の安全性を保障する意味でも多くの専門家による解読が不可欠である。このため現在においては、暗号に関する研究者の多くが解読作業を主な研究対象としており、解読作業そのものが主要な研究分野となっている。BBFP とは解読者側の立場に立った、暗号において自然に生じる問題である。暗号系と BBF との対応を与えた際に、復号化関数を求めることが BBFP である。

第2章　定義

2.1　BBF と BBFP

BBF とは、Black Box Field(ブラックボックスフィールド) の略であり、BBFP とは Black Box Field Problem(ブラックボックスフィールド問題) の略である。以下に BBF と BBFP の正確な定義を与える。

Definition 2.1 (ブラックボックスフィールドの定義). ブラックボックスフィールド $\mathbb{F}_p$ は、7 つの組 $(p, n, h, F, G, T, [\,])$ で表される。
ここで p は素数、n は符号化している範囲のビット数を表す正の整数である。関数 $h, F, G, T, [\,]$ は次のように定義される。

1. 関数 $h : \{0,1\}^n \to \mathbb{F}_p$ はすべての n ビット 2 進長を体の元と対応させる。関数 h は全射である, すなわち, 全ての体の元は少なくとも 1 つの n ビット 2 進長により表される。

2. 関数 $F, G : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ は加法と乗法を演算とする。それらは次の関係をみたす:

$$h(F(x,y)) = h(x) + h(y),\ \ h(G(x,y)) = h(x)h(y). \tag{2.1}$$

3. 関数 $T : \{0,1\}^n \times \{0,1\}^n \to \{\mathrm{true}, \mathrm{false}\}$ は 2 つのブラックボックスの元の等式を試す:

$$T(x,y) = \mathrm{true} \Leftrightarrow h(x) = h(y). \tag{2.2}$$

4. 関数 $[\,] : \mathbb{F}_p \to \{0,1\}^n$ は単射である。$x \in \mathbb{F}_p$ の $[\,]$ による像を x のブラックボックス表現と呼び、$[x] \in \{0,1\}^n$ で表す。次の関係をみたす：

$$h([x]) = h([\,](x)) = (h \circ [\,])(x) = x. \tag{2.3}$$

Definition 2.2 (ブラックボックスフィールド問題の定義). p は素数、$\mathbb{F}_p$ を BBF として与えられる有限体とする。関数 $F, G, T, [\,]$ の oracle が与えられている。このとき、$h^{-1}(\alpha) \in \{0,1\}^n$ に対して明確に $\alpha \in \mathbb{F}_p$ の値を返すアルゴリズム A を求めることをブラックボックスフィールド問題という。
形式上、$A^{F,G,T,[\,]}(h^{-1}(\alpha)) = a$ と書く。ここで $a \equiv \alpha \pmod{p}$.
アルゴリズムが $\log^{O(1)} p$ で稼動するとき、多項式時間で稼動するという。$\log p$ における準指数時間で稼動するときにはそのアルゴリズムを準指数アルゴリズムという。

Remark. BBFP とは、h による行き先を求めることに相当する。

Remark. 計算理論が扱う計算量は、問題を解くのに必要な演算量の大きさを、入力情報の大きさで表したものであり、この関数の定数倍の違いは考慮しない。上述においては、$\log_2 p$ が入力情報に相当する。

例えば、入力情報の大きさが x であり、問題 P_1, P_2, P_3 を解くのに必要な計算量が、それぞれ、$f_1(x) = x^2, f_2(x) = 10x^2, f_3(x) = x^2 + x$ という関係で与えられる場合、問題 P_1, P_2 を解くのに必要な計算量は同じであり、この計算量は $O(x^2)$ で表される。x^2 が x に比べて十分大きい場合は、問題 P_3 の $f_3(x) = x^2 + x$ の x が無視され、問題 P^3 を解く計算量も同様に $O(x^2)$ となる（通常、x は十分大きい)。また、計算量を表す関数 $f(x)$ が多項式で与えられるとき、この計算量を多項式オーダー（時間）といい、$f(x)$ が指数関数で与えられる場合、指数関数オーダー（時間）という。

Remark. $f(x) \in O(\exp g(x))$ が成り立つような $g(x) \in o(x)$ が存在するとき、$f(x)$ を準指数関数という。

2.2 代数的準同型暗号化スキーム

Definition.1.1 で定義した暗号系 $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ を考えたとき、2 つの平文 $x, y \in \mathcal{P}$ の暗号文 $E_k(x), E_k(y) \in \mathcal{C}$ が与えられているとする。

多項式時間内に平文 $x + y, xy \in \mathcal{P}$ の暗号文 $E_k(x + y), E_k(xy) \in \mathcal{C}$ を構成することができるとき、この暗号系は代数的準同型の暗号化スキームと定式化される。これは次の定義において定められる。

Definition 2.3 (代数的準同型暗号化スキームの定義). d, e, k を正の整数として、それぞれ平文、暗号文、鍵の長さのビット数を表す。$\mathbb{Z}_n$ を整数 n を法とした環として n は $\lceil \log_2 n \rceil = d$ を満たすとする。環 $\mathbb{Z}_n$ は平文の集合を構成する。(E, D) を暗号化スキームとする。すなわち、

$$E : \mathbb{Z}_n \times \{0,1\}^k \longrightarrow \{0,1\}^e$$
$$D : \{0,1\}^e \times \{0,1\}^k \longrightarrow \mathbb{Z}_n$$

であるとし、E, D は決定論的多項式時間で計算できる関数とする。さらに、ある暗号・復号化鍵の組 (K_E, K_D) に対して

$$D(E(x, K_E), K_D) = x \tag{2.4}$$

が成り立っているとする。暗号化スキームが代数的準同型であるとは、確率的多項式時間で計算可能な 2 つの写像 $A, M : \{0,1\}^e \times \{0,1\}^e \longrightarrow \{0,1\}^e$ がすべての $x, y \in \mathbb{Z}_n$ と暗号化鍵 K_E に対して、

$$A(E(x, K_E), E(y, K_E)) = E(x + y, K_E)$$
$$M(E(x, K_E), E(y, K_E)) = E(xy, K_E)$$

となることである。

ある暗号・復号化鍵の組 (K_E, K_D) に対して E は単射、D は全射である。

Proof. $E(x, K_E) = E(y, K_E)$ とする。D で写すと、

$$D(E(x, K_E), K_D) = D(E(y, K_E), K_D) \Longrightarrow x = y$$

従って、E は単射である。

D は全射でないと仮定すると、ある元 $x \in \mathbb{Z}_n$ が存在して、どんな元 $y \in \{0,1\}^e$ に対しても $D(y, K_D) \neq x$ が成り立つ。この元 $x \in \mathbb{Z}_n$ に対して、

$$w = E(x, K_E)$$

となる元 $w \in \{0,1\}^e$ がただ一つ存在する。D で写すと、

$$D(w, K_D) = D(E(x, K_E), K_D) = x$$

となり、$D(w, K_D) \neq x$ に反するので矛盾。 □

第3章　BBFとBBFPの例

3.1　BBFの例

3.1.1　例1

Definition.2.1 において、BBF の組を $p = 2, n = 2$ として以下のように $h, F, G, T, [\,]$ を与える。

1.

$$\begin{aligned} \pi : \mathbb{Z} &\longrightarrow \mathbb{F}_2 = \{\bar{0}, \bar{1}\} \\ a &\longmapsto a \equiv b \mod 2 \ (0 \leq b \leq 1) \end{aligned}$$

$\bar{b}$ を b と同一視する。
ここで $0 \sim 3$ の 2 ビット 2 進表示 $(0,0) \sim (1,1)$ を h で送ると、$0 \sim 3$ を $p = 2$ で割った余りの値へ写す写像を h とする。

Remark. BBF として与えられる h とは、ランダムに n ビット 2 進長に写すものであり、今回のように、2 ビット 2 進表示に写されるとは限らない。

$$\begin{aligned} h : \{0,1\}^2 &\longrightarrow \mathbb{F}_2 = \{0,1\} \\ (0,0) &\longmapsto 0 \\ (1,0) &\longmapsto 1 \\ (0,1) &\longmapsto 0 \\ (1,1) &\longmapsto 1 \end{aligned}$$

2. $w_1, w_2 \in \{0,1\}^2$ に対して、$h(F(w_1, w_2)) = h(w_1) + h(w_2)$ を満たす写

像 F を考える。

$$\begin{aligned}
F : \{0,1\}^2 \times \{0,1\}^2 &\longrightarrow \{0,1\}^2 \\
((0,0),(0,0)) &\longmapsto (0,0) \\
((0,0),(0,1)) &\longmapsto (0,1) \\
((0,0),(1,0)) &\longmapsto (1,0) \\
((0,0),(1,1)) &\longmapsto (1,1) \\
((0,1),(0,1)) &\longmapsto (0,0) \\
((0,1),(1,0)) &\longmapsto (1,0) \\
((0,1),(1,1)) &\longmapsto (1,1) \\
((1,0),(1,0)) &\longmapsto (0,0) \\
((1,0),(1,1)) &\longmapsto (0,1) \\
((1,1),(1,1)) &\longmapsto (0,0)
\end{aligned}$$

Remark. ここで、$F(x,y) = F(y,x)$ が成り立っているとする。以下が成り立つことが分かる。しかし BBF の定義からは次のことと $F(x,y) = F(y,x)$ が常に成り立つとは限らない。h が単射のときに成り立つ。

$$\begin{aligned}
&F([0],[0]) = [0+0] = [0]. \\
&F([0],[1]) = [0+1] = [1]. \\
&F([1],[1]) = [1+1] = [0].
\end{aligned}$$

3. $w_1, w_2 \in \{0,1\}^2$ に対して、$h(G(w_1,w_2)) = h(w_1)h(w_2)$ を満たす写像 G を考える。

$$\begin{aligned}
G : \{0,1\}^2 \times \{0,1\}^2 &\longrightarrow \{0,1\}^2 \\
((0,0),(0,0)) &\longmapsto (0,0) \\
((0,0),(0,1)) &\longmapsto (0,1) \\
((0,0),(1,0)) &\longmapsto (0,0) \\
((0,0),(1,1)) &\longmapsto (0,1) \\
((0,1),(0,1)) &\longmapsto (0,0) \\
((0,1),(1,0)) &\longmapsto (0,1) \\
((0,1),(1,1)) &\longmapsto (0,0) \\
((1,0),(1,0)) &\longmapsto (1,0) \\
((1,0),(1,1)) &\longmapsto (1,1) \\
((1,1),(1,1)) &\longmapsto (1,0)
\end{aligned}$$

Remark. ここで、$G(x,y) = G(y,x)$ が成り立っているとする。以下が成り立つことが分かる。しかし BBF の定義からは次のことと $G(x,y) = G(y,x)$ が常に成り立つとは限らない。h が単射のときに成り立つ。

$$G([0],[0]) = [0 \times 0] = [0].$$
$$G([0],[1]) = [0 \times 1] = [0].$$
$$G([1],[1]) = [1 \times 1] = [1].$$

4.

$$\begin{aligned} T : \{0,1\}^2 \times \{0,1\}^2 &\longrightarrow \{\mathrm{true}, \mathrm{false}\} \\ ((0,0),(0,1)) &\longmapsto \mathrm{true} \\ ((0,0),(1,0)) &\longmapsto \mathrm{false} \\ ((0,0),(1,1)) &\longmapsto \mathrm{false} \\ ((0,1),(1,0)) &\longmapsto \mathrm{false} \\ ((0,1),(1,1)) &\longmapsto \mathrm{false} \\ ((1,0),(1,1)) &\longmapsto \mathrm{true} \end{aligned}$$

Remark. $T(x,x) = \mathrm{true}$ と $T(x,y) = T(y,x)$ は定義から明らか。

5. $0,1 \in \mathbb{F}_2$ のブラックボックス表現 [0]、[1] は

$$[0] = (0,0) \in h^{-1}(0) = \{(0,0),(0,1)\}.$$
$$[1] = (1,0) \in h^{-1}(1) = \{(1,0),(1,1)\}.$$

とする。

3.1.2 例 2

紀元前から使用が始まった古代の暗号は、簡単な規則により文字の転置や置換により行われていた。例えばシーザー暗号（巡回シフト暗号）を例にとり、BBF との対応を考える。シーザー暗号は、アルファベットの文字 $A, B, C, \cdots, Y, Z$ の各々に $0, 1, 2, \cdots, 24, 25$ を対応させることにより、平文を数字に変換し、その数字にある定数（シーザーが用いたのは定数 3）を加えた後、その数に対応する文字を戻すことにより暗号化を行う。ただし、26 を越えた数字は 26 を引く。このような操作を巡回置換という。この巡回置換に用いられる定数をシーザー暗号の鍵と見なすことができる。複合化は、暗号化文を数字に変換して、その数字を暗号化する際に用いた定数で減じた後、その数に対応する文字を戻すことにより行う。暗号化鍵と複合化鍵とが同一であるため、シーザー暗号は共通鍵暗号に属する。

Remark. Definition.1.1 で定義した暗号系の例ともなる。次のように暗号系 $(\mathbb{Z}_{26}, \mathbb{Z}_{26}, \mathbb{Z}_{26}, \mathcal{E}, \mathcal{D})$ を考える。

1. 平文空間、暗号文空間はアルファベットで構成されるが、数字との対応により $\mathbb{Z}_{26}$ とする。

2. 鍵空間は $\mathbb{Z}_{26}$ である。
3. $\mathcal{E} = \{E_k : k \in \mathbb{Z}_{26}\}$. 暗号化関数は次のように与える。
   $k \in \mathbb{Z}_{26}$ に対して

$$\begin{aligned} E_k : \mathbb{Z}_{26} &\longrightarrow \mathbb{Z}_{26} \\ p &\longmapsto p + k \pmod{32} \end{aligned}$$

4. $\mathcal{D} = \{D_k : k \in \mathbb{Z}_{26}\}$. 復号化関数は次のように与える。
   $k \in \mathbb{Z}_{26}$ に対して

$$\begin{aligned} D_k : \mathbb{Z}_{26} &\longrightarrow \mathbb{Z}_{26} \\ c &\longmapsto c - k \pmod{32} \end{aligned}$$

5. 全ての $p \in \mathbb{Z}_{26}$ に対して、次のことが成り立つ: 任意の $k \in \mathbb{Z}_{26}$ に対して、等式 $D_k(E_k(p)) = p$ が成り立つ。

アルファベットの文字 $A, B, C, \cdots, Y, Z$ の 26 文字に次の 6 文字

“ , ”“ . ”“ (スペース) ”“ 「 ”“ 」 ”“ ! ”

を加えて、平文空間、暗号文空間を $\mathbb{Z}_{32}$ とする。鍵空間は $\mathbb{Z}_{32}$ である。鍵 $3 \in \mathbb{Z}_{32}$ の場合のシーザー暗号を次のように定める。

$$\begin{aligned} E_3 : \mathbb{Z}_{32} &\longrightarrow \mathbb{Z}_{32} \\ p &\longmapsto p + 3 \pmod{32} \\ D_3 : \mathbb{Z}_{32} &\longrightarrow \mathbb{Z}_{32} \\ c &\longmapsto c - 3 \pmod{32} \end{aligned}$$

暗号文を 5 ビット 2 進表示にし、暗号文空間を $\{0,1\}^5$ と置き換え、Definition.2.3 の暗号化スキーム (E, D) と対応させる。この場合 $K_E, K_D = (1,1)$ とおく。すなわち、

$$\begin{aligned} E : \mathbb{Z}_{32} \times \{(1,1)\} &\longrightarrow \{0,1\}^5 \\ p &\longmapsto E(p) := (E_3(p) \pmod{32})_2 \\ D : \{0,1\}^5 \times \{(1,1)\} &\longrightarrow \mathbb{Z}_{32} \\ c &\longmapsto D(c) := D_3((c)_{10}) \pmod{32} \end{aligned}$$

である。

Remark. 平文“「I AM SUM.」”を数字に対応させると、“ $29, 8, 28, 0, 12, 28, 18, 20, 12, 27, 30$ ” となる。これを E_3 で写すと、“ $0, 11, 31, 3, 15, 31, 21, 23, 15, 30, 1$ ”となる。従って暗号文は、“ AL!DP!VXP」B ”である。

平文を E で写した場合は、“ $(0,0,0,0,0), (0,1,0,1,1), (0,1,1,1,1), \cdots, (1,1,1,1,0), (0,0,0,0,1)$ ”となる。

Definition.2.1 において、BBF の組を $p = 13, n = 5$ として以下のように $h, F, G, T, [\,]$ を与える。

1. $w \in \{0,1\}^5$ に対して、$h(w) := D(w,(1,1)) \pmod{13}$ と定義する。以下、示されていない元の行き先は、条件を満たすように定められていることとする。

$$
\begin{array}{rcl}
h : \{0,1\}^5 & \longrightarrow & \mathbb{F}_{13} \\
(0,0,0,0,0) & \longmapsto & 29 \equiv 3 \\
(0,0,0,0,1) & \longmapsto & 30 \equiv 4 \\
(0,0,0,1,0) & \longmapsto & 31 \equiv 5 \\
(0,0,0,1,1) & \longmapsto & 0 \\
(0,0,1,0,0) & \longmapsto & 1 \\
(0,0,1,0,1) & \longmapsto & 2 \\
(0,0,1,1,0) & \longmapsto & 3 \\
(0,0,1,1,1) & \longmapsto & 4 \\
(0,1,0,0,0) & \longmapsto & 5 \\
(0,1,0,0,1) & \longmapsto & 6 \\
(0,1,0,1,0) & \longmapsto & 7 \\
(0,1,0,1,1) & \longmapsto & 8 \\
(0,1,1,0,0) & \longmapsto & 9 \\
(0,1,1,0,1) & \longmapsto & 10 \\
(0,1,1,1,0) & \longmapsto & 11 \\
(0,1,1,1,1) & \longmapsto & 12 \\
(1,0,0,0,0) & \longmapsto & 13 \equiv 0 \\
(1,0,0,0,1) & \longmapsto & 14 \equiv 1 \\
(1,0,0,1,0) & \longmapsto & 15 \equiv 2 \\
(1,0,0,1,1) & \longmapsto & 16 \equiv 3 \\
(1,0,1,0,0) & \longmapsto & 17 \equiv 4 \\
(1,0,1,0,1) & \longmapsto & 18 \equiv 5 \\
(1,0,1,1,0) & \longmapsto & 19 \equiv 6 \\
\vdots & \vdots & \vdots \\
(1,1,1,1,0) & \longmapsto & 27 \equiv 1 \\
(1,1,1,1,1) & \longmapsto & 28 \equiv 2
\end{array}
$$

2. $w_1, w_2 \in \{0,1\}^5$ に対して、$h(F(w_1,w_2)) = h(w_1) + h(w_2)$ を満たす写

像 F を考える。

$$
\begin{array}{rcl}
F: \ \{0,1\}^5 \times \{0,1\}^5 & \longrightarrow & \{0,1\}^5 \\
((0,0,0,0,0),(0,0,0,0,0)) & \longmapsto & (0,1,0,0,1) \\
((0,0,0,0,0),(0,0,0,0,1)) & \longmapsto & (0,1,0,1,0) \\
((0,0,0,0,0),(0,0,0,1,0)) & \longmapsto & (0,1,0,1,1) \\
\vdots & \vdots & \vdots \\
((0,0,0,0,1),(0,0,0,0,0)) & \longmapsto & (0,1,0,1,0) \\
((0,0,0,0,1),(0,0,0,0,1)) & \longmapsto & (0,1,0,1,1) \\
\vdots & \vdots & \vdots \\
((1,1,1,1,0),(1,0,1,1,0)) & \longmapsto & (0,1,0,1,0) \\
\vdots & \vdots & \vdots \\
((1,1,1,1,1),(1,1,1,1,0)) & \longmapsto & (0,0,0,0,0) \\
((1,1,1,1,1),(1,1,1,1,1)) & \longmapsto & (0,0,0,0,1)
\end{array}
$$

3. $w_1, w_2 \in \{0,1\}^5$ に対して、$h(G(w_1,w_2)) = h(w_1)h(w_2)$ を満たす写像 G を考える。

$$
\begin{array}{rcl}
G: \ \{0,1\}^5 \times \{0,1\}^5 & \longrightarrow & \{0,1\}^5 \\
((0,0,0,0,0),(0,0,0,0,0)) & \longmapsto & (0,1,1,0,0) \\
((0,0,0,0,0),(0,0,0,0,1)) & \longmapsto & (0,1,1,1,1) \\
((0,0,0,0,0),(0,0,0,1,0)) & \longmapsto & (0,0,1,0,1) \\
\vdots & \vdots & \vdots \\
((0,0,0,0,1),(0,0,0,0,0)) & \longmapsto & (0,1,1,1,1) \\
((0,0,0,0,1),(0,0,0,0,1)) & \longmapsto & (0,0,0,0,0) \\
\vdots & \vdots & \vdots \\
((1,1,1,1,0),(1,0,1,1,0)) & \longmapsto & (0,1,0,0,1) \\
\vdots & \vdots & \vdots \\
((1,1,1,1,1),(1,1,1,1,0)) & \longmapsto & (0,0,1,0,1) \\
((1,1,1,1,1),(1,1,1,1,1)) & \longmapsto & (0,0,0,0,1)
\end{array}
$$

4.

$$
\begin{array}{rcl}
T: \{0,1\}^5 \times \{0,1\}^5 & \longrightarrow & \{\mathtt{true}, \mathtt{false}\} \\
((0,0,0,0,0),(0,0,0,0,1)) & \longmapsto & \mathtt{false} \\
((0,0,0,0,0),(0,0,0,1,0)) & \longmapsto & \mathtt{false} \\
((0,0,0,0,0),(0,0,0,1,1)) & \longmapsto & \mathtt{false} \\
\vdots & \vdots & \vdots \\
((0,0,0,1,1),(1,1,1,0,0)) & \longmapsto & \mathtt{false} \\
((0,0,0,1,1),(1,1,1,0,1)) & \longmapsto & \mathtt{true} \\
\vdots & \vdots & \vdots \\
((1,0,0,0,1),(1,1,1,1,0)) & \longmapsto & \mathtt{true} \\
((1,0,0,0,1),(1,1,1,1,1)) & \longmapsto & \mathtt{false} \\
\vdots & \vdots & \vdots \\
((1,1,1,1,1),(1,1,1,1,0)) & \longmapsto & \mathtt{false} \\
((1,1,1,1,1),(1,1,1,1,1)) & \longmapsto & \mathtt{true}
\end{array}
$$

5. $x \in \mathbb{F}_{13}$ に対して、$[x] := E(x', (1,1)), x' \equiv x \pmod{13}$ と定義する。

$$
\begin{array}{rcl}
[\,] : \mathbb{F}_{13} & \longrightarrow & \{0,1\}^5 \\
0 & \longmapsto & E(26,(1,1)) = (1,1,1,0,1) \\
1 & \longmapsto & E(14,(1,1)) = (1,0,0,0,1) \\
2 & \longmapsto & E(15,(1,1)) = (1,0,0,1,0) \\
3 & \longmapsto & E(29,(1,1)) = (0,0,0,0,0) \\
4 & \longmapsto & E(4,(1,1)) = (0,0,1,1,1) \\
5 & \longmapsto & E(31,(1,1)) = (0,0,0,1,0) \\
6 & \longmapsto & E(19,(1,1)) = (1,0,1,1,0) \\
7 & \longmapsto & E(20,(1,1)) = (1,0,1,1,1) \\
8 & \longmapsto & E(8,(1,1)) = (0,1,0,1,1) \\
9 & \longmapsto & E(9,(1,1)) = (0,1,1,0,0) \\
10 & \longmapsto & E(23,(1,1)) = (1,1,0,1,0) \\
11 & \longmapsto & E(24,(1,1)) = (1,1,0,1,1) \\
12 & \longmapsto & E(25,(1,1)) = (1,1,1,0,0)
\end{array}
$$

(4.1) より次の関係をみたす：

$$h([x]) = D(E(x', (1,1)), (1,1)) = x' \equiv x \pmod{13} (0 \leq x \leq 13)$$

3.2 BBFP の例

3.2.1 例 1

前節での例 1. の BBF を考える。仮定から $\mathsf{F}, \mathsf{G}, \mathsf{T}, [\,]$ の oracle は与えられている。

1. $(1,0) \in \{0,1\}^2$ が与えられたとき、$\mathbb{F}_2$ のどの元と一致するかを調べる。
   $[\,]$ の oracle から $0, 1 \in \mathbb{F}_2$ のブラックボックス表現 $[0]$、$[1]$ は

   $$[0] = (0,0).$$
   $$[1] = (1,0).$$

   とわかる。(2.3) から

   $$\mathsf{h}((1,0)) = \mathsf{h}([1]) = (\mathsf{h}([\,](1)) = (\mathsf{h} \circ [\,])(1) = 1.$$

   $(1,0) \in \{0,1\}^2$ が与えられたとき、h による行き先は $1 \in \mathbb{F}_2$ と分かる。

2. 上同様に $(0,0) \in \{0,1\}^2$ が与えられたとき、h による行き先は $0 \in \mathbb{F}_2$ と分かる。

3. $(1,1) \in \{0,1\}^2$ が与えられたとき、$\mathbb{F}_2$ のどの元と一致するかを調べる。
   T の oracle により、

   $$\mathsf{T}((0,0),(1,1)) = \mathsf{false},\ \mathsf{T}((1,1),(1,0)) = \mathsf{true}$$

   と分かる。よって、(2.2) から

   $$\mathsf{h}((1,1)) = \mathsf{h}((1,0)).$$

   今、$[1] = (1,0)$ だったので、

   $$\mathsf{h}((1,1)) = \mathsf{h}((1,0)) = \mathsf{h}([1]) = (\mathsf{h} \circ [\,])(1) = 1.$$

   よって、$(1,1) \in \{0,1\}^2$ が与えられたとき、h による行き先は $1 \in \mathbb{F}_2$ と分かる。

4. $(0,1) \in \{0,1\}^2$ が与えられたとき、$\mathbb{F}_2$ のどの元と一致するかを調べる。
   今度は F の oracle を使って調べてみる。$(1,1)$ と $(0,1)$ を入力してみると F の oracle により、

   $$\mathsf{F}((0,1),(1,1)) = (1,1)$$

   と出力される。(2.1) から、

$$h(F((0,1),(1,1))) = h((0,1)) + h((1,1))$$

が成り立っていなければならない。$h((1,1)) = 1$ より、

$$\begin{aligned}(\text{左辺}) &= h(F((0,1),(1,1))) = h((1,1)) = 1\\ (\text{右辺}) &= h((0,1)) + h((1,1)) = h((0,1)) + 1.\end{aligned}$$

両辺から、

$$h((0,1)) = 0$$

よって、$(0,1) \in \{0,1\}^2$ が与えられたとき、h による行き先は $0 \in \mathbb{F}_2$ と分かる。

求まった写像が、前節での例 1 における写像 h と一致していることを確認する。

$$\begin{aligned}A^{F,G,T,[\,]} : \{0,1\}^2 &\longrightarrow \mathbb{F}_2 = \{0,1\}\\ (0,0) &\longmapsto 0\\ (1,0) &\longmapsto 1\\ (0,1) &\longmapsto 0\\ (1,1) &\longmapsto 1\end{aligned}$$

3.2.2 例 2

前節での例 2. の BBF を考える。

1. $[0] = E(26,(1,1)) = (1,1,1,0,1)$ だった。(2.3) から

$$h((1,1,1,0,1)) = h([0]) = (h([\,](0)) = (h \circ [\,])(0) = 0.$$

$(1,1,1,0,1) \in \{0,1\}^5$ が与えられたとき、h による行き先は $0 \in \mathbb{F}_{13}$ と

分かる。同様に [] の oracle から

$$
\begin{aligned}
A^{F,G,T,[\,]} : \{0,1\}^5 &\longrightarrow \mathbb{F}_{13} \\
(1,1,1,0,1) &\longmapsto 0 \\
(1,0,0,0,1) &\longmapsto 1 \\
(1,0,0,1,0) &\longmapsto 2 \\
(0,0,0,0,0) &\longmapsto 3 \\
(0,0,1,1,1) &\longmapsto 4 \\
(0,0,0,1,0) &\longmapsto 5 \\
(1,0,1,1,0) &\longmapsto 6 \\
(1,0,1,1,1) &\longmapsto 7 \\
(0,1,0,1,1) &\longmapsto 8 \\
(0,1,1,0,0) &\longmapsto 9 \\
(1,1,0,1,0) &\longmapsto 10 \\
(1,1,0,1,1) &\longmapsto 11 \\
(1,1,1,0,0) &\longmapsto 12
\end{aligned}
$$

と分かる。次に T の oracle を用いると、$(1,1,1,0,1),\cdots,(1,1,1,0,0)$ から残り全て求まる。例えば、$(1,1,1,0,1),\cdots,(1,1,1,0,0)$ の $A^{F,G,T,[\,]}$ による行き先はわかっているので、任意の元 $w \in \{0,1\}^5$ をとってきたとき、$T(w,(1,1,1,0,1)) = \mathrm{true}$ と出力されたら、$A^{F,G,T,[\,]}(w) = 0$ と分かる。

Remark. 今回の例においては、全数チェックによる力づくの方法で BBFP を解いている。が、今回の論文では示さなかったものの一つずつ元をテストせずとも求めることができる。それが BBFP に対する準指数アルゴリズムである。

第4章　定理

Theorem 1 (代数的準同型暗号化スキームにおける定理). 大きさ p の有限体における BBFP が $T_{BBF}(p)$ 時間で解けたと仮定する。その時、大きさ n の平文空間環上の任意の代数的準同型暗号化スキーム (E, D) は平均計算時間

$$O(T_{BBF}(n) + \exp((1 + o(1)) \sqrt[3]{\log n \log^2 \log n}))$$

で解読できる。

Proof. 証明を簡略化するため、n は平方数を持たないとする。この制限は Pohlig と Hellman の手法（参考文献 [4]) を用いれば簡単に取り除くことができる。参考文献 [5] を見れば、平均計算時間

$$\exp((1 + o(1)) \sqrt[3]{\log n \log^2 \log n})$$

で整数を因数分解できるため、次のように有限体の直積への平文環の因数分解が可能である：

$$\mathbb{Z}_n = \prod_{i=1}^{s} \mathbb{F}_{p_i} \text{ ここで } p_i \text{ は異なった素数.}$$

(E, D) を代数的準同型暗号化スキームとする。

$$E : \mathbb{Z}_n \times \{0,1\}^k \longrightarrow \{0,1\}^e,$$
$$D : \{0,1\}^e \times \{0,1\}^k \longrightarrow \mathbb{Z}_n.$$

関数 E, D は決定論的多項式時間で計算できる関数であり、ある暗号・複合化鍵の組 K_E, K_D に対して

$$D(E(x, K_E), K_D) = x \tag{4.1}$$

が成り立つ。Definition.2.3 より、すべての $x, y \in \mathbb{Z}_n$ と暗号化鍵 K_E に対して、

$$A(E(x, K_E), E(y, K_E)) = E(x + y, K_E) \tag{4.2}$$

$$M(E(x, K_E), E(y, K_E)) = E(xy, K_E) \tag{4.3}$$

を満たす確率的多項式時間で計算可能な 2 つの写像 $A, M : \{0,1\}^e \times \{0,1\}^e \longrightarrow \{0,1\}^e$ が存在する。

K_E, K_D をある暗号・複合化鍵の組とする。$E(x, K_E) \in \{0,1\}^e$ を与えたとき、要求された時間内で $x \in \mathbb{Z}_n$ を求めたい。

各々の p_i に対して、組 $(p_i, e, h, A, M, T, [\,])$ がブラックボックスフィールドであるかを検討する：

1.

$$\begin{aligned} \text{関数 } h : \{0,1\}^e &\longrightarrow \mathbb{F}_{p_i} \\ w &\longmapsto h(w) := D(w, K_D) \equiv x \pmod{p_i} (0 \le x \le p_i) \end{aligned}$$

関数 h の全射性は、D の全射性より従う。

2.

$$\begin{aligned} \text{関数 } [\,] : \mathbb{F}_{p_i} &\longrightarrow \{0,1\}^e \\ x &\longmapsto [\,](x) = [x] := E(x', K_E), x' \equiv x \pmod{p_i} (0 \le x \le p_i) \end{aligned}$$

関数 $[\,]$ の単射性は、E の単射性より従う。(4.1) より次の関係をみたす：

$$h([x]) = D(E(x', K_E), K_D) = x' \equiv x \pmod{p_i} (0 \le x \le p_i)$$

3. 関数 $A, M : \{0,1\}^e \times \{0,1\}^e \to \{0,1\}^e$ は Definition.2.1 の F, G に対応しない。すなわち、ある元 $w_1, w_2 \in \{0,1\}^e$ に対して

$$\begin{aligned} h(A(w_1, w_2)) &\neq h(w_1) + h(w_2), \\ h(M(w_1, w_2)) &\neq h(w_1)h(w_2), \end{aligned}$$

が成り立つ。

反例：

$n = 6, p_2 = 3$ の時を考える。$\lceil \log_2 6 \rceil \le e$ を満たすように $e = 3$ とする。

$$\begin{aligned} \text{関数 } E : \mathbb{Z}_6 \times \{K_E\} &\longrightarrow \{0,1\}^3 \\ (0, K_E) &\longmapsto E(0, K_E) = (0,0,0) \\ (1, K_E) &\longmapsto E(1, K_E) = (0,0,1) \\ (2, K_E) &\longmapsto E(2, K_E) = (0,1,0) \\ (3, K_E) &\longmapsto E(3, K_E) = (1,0,0) \\ (4, K_E) &\longmapsto E(4, K_E) = (0,1,1) \\ (5, K_E) &\longmapsto E(5, K_E) = (1,1,0) \end{aligned}$$

と定める。

$$\begin{aligned} \text{関数 } h : \{0,1\}^3 &\longrightarrow \mathbb{F}_{p_i} \\ (1,1,1) &\longmapsto h(1,1,1) = 2 \end{aligned}$$

と定める。

$$\begin{array}{rcl} \text{関数 } A : \{0,1\}^3 \times \{0,1\}^3 & \longrightarrow & \{0,1\}^3 \\ ((0,0,1),(1,1,1)) & \longmapsto & A((0,0,1),(1,1,1)) = (0,0,1) \end{array}$$

と定める。

示されていない残りの元の行き先については、(4.1),(4.2) を満たすように適当に定められていることとする。例えば、$(0,0,1)$ の h による行き先は

$$h((0,0,1)) = D((0,0,1), K_D) = D(E(1, K_E), K_D) = 1.$$

また、例えば $((0,0,1),(0,1,0))$ の A による行き先は

$$\begin{array}{rcl} A((0,0,1),(0,1,0)) & = & A(E(1,K_E), E(2,K_E)) \\ & = & E(1+2, K_E) \\ & = & E(3, K_E) \\ & = & (1,0,0). \end{array}$$

今、$w_1 = (0,0,1), w_2 = (1,1,1)$ とおくと、

$$\begin{array}{c} h(A(w_1,w_2)) = h(A((0,0,1),(1,1,1))) = h((0,0,1)) = 1 \pmod 3. \\ h(w_1) + h(w_2) = h((0,0,1)) + h((1,1,1)) = 1 + 2 \equiv 0 \pmod 3. \end{array}$$

従って、$h(A(w_1,w_2)) \neq h(w_1) + h(w_2)$ となり反例となる。

同様に、$M((0,0,1),(1,1,1)) = (0,0,1)$ とおけば、$h(M(w_1,w_2)) \neq h(w_1)h(w_2)$ の反例となる。

Remark. ImE から任意に元 $E(x', K_E)$ をとった時、$x' \equiv x \pmod{p_i}$ が成り立つからといって、$E(x', K_E) = [x]$ が成り立つとは限らない。例えば、上述の反例において、

$$\begin{array}{rcl} \text{関数 } [\,] : \mathbb{F}_3 & \longrightarrow & \{0,1\}^3 \\ 0 & \longmapsto & [0] = E(0, K_E) = (0,0,0) \\ 1 & \longmapsto & [1] = E(1, K_E) = (0,0,1) \\ 2 & \longmapsto & [2] = E(5, K_E) = (1,1,0) \end{array}$$

と定める。$4 \equiv 1 \pmod 3$ だが、E の単射性より、

$$4 \not\equiv 1 \pmod 6 \Longrightarrow E(4, K_E) \neq E(1, K_E) = [1].$$

従って $E(4, K_E) \neq [1]$ となる。

4. 関数 $T : \{0,1\}^e \times \{0,1\}^e \to \{\mathtt{true}, \mathtt{false}\}$ は Definition.2.1 の T に対応しない。関数 A, M の時同様に、ある元 $w_1, w_2 \in \{0,1\}^e \backslash \mathrm{Im}E$ に対して

$$T(w_1,w_2) = \mathtt{false} \text{ かつ } h(w_1) = h(w_2),$$

が成り立つ反例が作れる。

以上から各々の p_i に対する組 $(p_i, e, h, A, M, T, [\,])$ において、A, M, T はブラックボックスフィールドの性質を満たさない。ここで、ブラックボックスフィールドの性質を満たすように $\{0,1\}^e$ を $\mathrm{Im}E$ に置き換える。解読するとは、与えられた暗号文 $E(x, K_E) \in \{0,1\}^e$ を平文 $x \in \mathbb{Z}_n$ に変換することである。暗号文全体は $\mathrm{Im}E$ に含まれるので、この制限は定理を証明する上では支障がない。

各々の p_i に対してブラックボックスフィールド $(p_i, e, h, A, M, T, [\,])$ を次のように定義する：

1.

$$\begin{aligned} \text{関数 } h : \mathrm{Im}E &\longrightarrow \mathbb{F}_{p_i} \\ w &\longmapsto h(w) := D(w, K_D) \equiv x \pmod{p_i} (0 \le x \le p_i) \end{aligned}$$

関数 h の全射性は、D の全射性より従う。決定論的多項式時間で計算できる関数である。

2.

$$\begin{aligned} \text{関数 } [\,] : \mathbb{F}_{p_i} &\longrightarrow \mathrm{Im}E \\ x &\longmapsto [\,](x) = [x] := E(x', K_E), x' \equiv x \pmod{p_i} (0 \le x \le p_i) \end{aligned}$$

関数 $[\,]$ の単射性は、E の単射性より従う。決定論的多項式時間で計算できる関数である。(4.1) より次の関係をみたす：

$$h([x]) = h(E(x', K_E)) = D(E(x', K_E), K_D) = x' \equiv x \pmod{p_i} (0 \le x \le p_i) \tag{4.4}$$

3. 関数 $A, M : \mathrm{Im}E \times \mathrm{Im}E \to \mathrm{Im}E$ は Definition.2.1 の F, G に対応する。すなわち、任意の元 $w_1 = E(x, K_E), w_2 = E(y, K_E) \in \mathrm{Im}E$ に対して

$$\begin{aligned} h(A(w_1, w_2)) &= h(A(E(x, K_E), E(y, K_E))) \\ \text{(4.2) から} &= h(E(x+y), K_E) \\ \text{(4.4) から} &= x + y \\ &= h(E(x, K_E)) + h(E(y, K_E)) \\ &= h(w_1) + h(w_2) \end{aligned}$$

$$\begin{aligned} h(M(w_1, w_2)) &= h(M(E(x, K_E), E(y, K_E))) \\ \text{(4.3) から} &= h(E(xy), K_E) \\ \text{(4.4) から} &= xy \\ &= h(E(x, K_E))h(E(y, K_E)) \\ &= h(w_1)h(w_2) \end{aligned}$$

が成り立つ。A, M は確率的多項式時間で計算できる関数である。

4. 関数 $T : ImE \times ImE \to \{\mathtt{true}, \mathtt{false}\}$ は任意の元 $w_1 = E(x, K_E), w_2 = E(y, K_E) \in ImE$ に対して

$$E((x-y) \times \tfrac{n}{p_i}, K_E) = E(0, K_E) \iff T(w_1, w_2) = \mathtt{true}$$

として定める。このとき、

$$E((x-y) \times \tfrac{n}{p_i}, K_E) = E(0, K_E) \iff h(w_1) = h(w_2)$$

が成り立つことを示す。

$$E((x-y) \times \tfrac{n}{p_i}, K_E) = E(0, K_E)$$

とする。E は単射より、

$$(x-y) \times \tfrac{n}{p_i} \equiv 0 \pmod{n}$$

が成り立つ。

$$(x-y) \times \tfrac{n}{p_i} = n \times k$$

を満たす $k \in \mathbb{Z}$ が存在する。両辺を p_i をかけて n で割ると、

$$x - y = p_i \times k.$$

従って、

$$x \equiv y \pmod{p_i}$$

が成り立ち、(4.4) より、

$$h(E(x, K_E)) = h(E(y, K_E)) \pmod{p_i}.$$

よって、

$$h(w_1) = h(w_2) \pmod{p_i}$$

が成り立つ。逆に、

$$h(w_1) = h(w_2)$$

とすると、先ほどの逆もたどっていけるので

$$E((x-y)\times\tfrac{n}{p_i},K_E)=E(0,K_E)$$

が成り立つ。従って、

$$T(w_1,w_2)=\mathrm{true}\quad\Longleftrightarrow h(w_1)=h(w_2)$$

がいえたので、Definition.2.1 の T に対応する oracle が与えられた。T は確率的多項式時間で計算できる関数である。

Remark. 任意の元 $E(x,K_E),E(y,K_E)\in \mathrm{Im}E$ が与えられたとき、$E((x-y)\times\frac{n}{p_i},K_E)$ は確率的多項式時間で求められる。

$$\mathbb{Z}_n\ni -1\longmapsto E(-1,K_E)\in\{0,1\}^e$$

から、$E(-1,K_E)$ が決定論的多項式時間で求まった。(4.3) より、

$$M(E(-1,K_E),E(y,K_E))=E(-y,K_E)$$

となり $E(-y,K_E)$ が確率的多項式時間で求まる。(4.2) より、

$$A(E(x,K_E),E(-y,K_E))=E(x-y,K_E).$$

$$\mathbb{Z}_n\ni\tfrac{n}{p_i}\longmapsto E(\tfrac{n}{p_i},K_E)\in\{0,1\}^e$$

最後に M の oracle により、

$$M(E(x-y,K_E),E(\tfrac{n}{p_i},K_E))=E((x-y)\times\tfrac{n}{p_i},K_E).$$

あとは

$$\mathbb{Z}_n\ni 0\longmapsto E(0,K_E)\in\{0,1\}^e$$

から $E(0,K_E)$ と、求めた $E((x-y)\times\frac{n}{p_i},K_E)$ が一致するかどうかで T による行き先が定まる。T は A, M の oracle をも用いるので $E((x-y)\times\frac{n}{p_i},K_E)$ が確率的多項式時間で求まることが分かる。

各々のブラックボックスフィールド $\mathbb{F}_{p_i}$ において、BBFP に対するアルゴリズムを用いると、$E(x,K_E)$ が与えられたときに $x \pmod{p_i}$ の値を各々が返してくれる。中国式剰余の定理から $\prod_{i=1}^{s}\mathbb{F}_{p_i}\ni(x \pmod{p_1},x \pmod{p_2},\cdots,x \pmod{p_s})$ に対応する $x \pmod{p_n}\in\mathbb{Z}_n$ が求まる。この $x\in\mathbb{Z}_n$ が求めたかったものである。全平均計算時間 $\sum_{i=1}^{s}O(T_{BBF}(p_i))$ は $O(T_{BBF}(n))$ でおさえられるので、整数を因数分解する時間と併せて、大きさ n の平文空間環上の任意の代数的準同型暗号化スキーム (E, D) は平均計算時間

$$O(T_{BBF}(n)+\exp((1+o(1))\sqrt[3]{\log n\log^2\log n}))$$

で解読できることが示せた。 □

謝辞

最後になりますが、この論文を書くにいたってご指導いただいた松本眞教授をはじめ、アドバイスをいただいた皆様に厚く御礼を申し上げます。

参考文献

[1] Dan Boneh, Richard J.Lipton: *Algorithms for Black-Box Fields and their Application to Cryptograp hy*,Advances in Cryptology —Crypto '96, Springer-Verlag,pp.283-297.

[2] Jahannes A. Buchmann: *INTRODUCTION TO CRYPTOGRAPHY*,Springer,2000.

林芳樹:暗号理論入門, シュプリンガー・フェアラーク社,2001.

[3] 笠原正雄, 境隆一: 暗号-ネットワーク社会の安全を守る鍵, 共立出版,2002.

[4] S.Pohlig,M.Hellman: *An improved algorithm for computing discrete logarithms over GF(p) and its cryptographic significance*, IEEE Trans. Inform. Theory, Vol.24,1978,pp.106-110

[5] A. Lenstra, H. Lenstra Jr., M Manasse, J. Pollard: *The number field sieve*,Proceedings of STOC 1990,pp.564-572