コンピュータセキュリティ 19－7
（２００２．１２．２０）

結託耐性符号のモデル化について

吉岡　克成†　　四方　順司†　　松本　勉†

あらまし fingerprinting や traitor tracing に対する結託攻撃への耐性を高めるため、結託耐性符号が多数提案されている。しかし、想定するアプリケーションの違いから、結託攻撃のモデルは各結託耐性符号により異なっている。本論文では、これまで提案されている結託耐性符号を含めて、より広範囲の結託耐性符号を定義し、これらを解析する。特に各モデルにおける符号クラス間の関係について考察する.

Various Models of Collusion Secure Codes

Katsunari YOSHIOKA†　Junji SHIKATA†　Tsutomu MATSUMOTO†

Abstract　For fingerprinting and traitor tracing schemes, several collusion secure codes have been proposed to enhance resilience against collusion attacks. However several models of collusion secure codes, according to their applications, have been defined without consistency. In this paper, in order to treat them with generality we define various models for collusion secure codes including those models, and analyze them in details. In particular, we reveal some relations among the classes of collusion secure codes under consideration.

1. はじめに

ディジタルコンテンツの著作権保護の方策として，コンテンツの複製にユーザ ID 情報を電子透かしとして埋込むことで海賊版の流出先の特定を行うことが考えられている (fingerprinting). 一方，放送型 pay TV のようにコンテンツ自体が暗号化されて放送され，料金を払いデコーダを取得したユーザのみコンテンツを復号し利用することができる方式において，デコーダ内の復号鍵をデコーダのユーザ ID 情報として用いることで，海賊版のデコーダの流出先を特定することが考えられている (traitor tracing).

このようなコンテンツまたはデコーダに対する ID 情報付加に対する共通の脅威として，複数のコンテンツ(デコーダ)を所有する攻撃者による結託攻撃(collusion attack)がある.

Boneh, Shaw は論文[1]において, fingerprinting 対象ユーザ総数 n 人のうち，c 人以下の結託によっては結託者以外の正規ユーザ ID 情報を生成することができないという性質をもつ符号, c-frameproof 符号を提案した. Stinson, Trung, Wei は論文[8]で，共通要素をもたない 2 つの c 人以下の結託が同様の ID 情報を生成することができないという性質をもつ符号，c-secure frameproof 符号を示した.

Boneh らは論文[1]において，c 人以下の結託が生成するどのような ID 情報からも必ず 1 人は結託者の追跡が行える追跡アルゴリズムをもつ 2 元符号，totally c-secure 符号を定義した. Boneh らは，totally c-secure 符号が 2 元符号において存在しないことを示し，追跡アルゴリズムが誤ったユーザを出力する確率 (誤追跡率) ε をもつ 2 元 c-secure 符号 (c-secure code with ε-error) を新たに示した. Guth, Pfitzmann は論文[3]において，fingerprinting に対する攻撃として結託攻撃に加えてランダム誤り付加が行われる可能性に言及し，ランダム誤り付加を考慮に入れた 2 元 c-secure 符号を示した. Muratani は論文[5]において，Boneh らの示した誤り ε をもつ c-secure 符号の構成法を改良し，中国人剰余定理を用いて符号長を削減した 2 元 c-secure CRT 符号を提案した. Yoshioka, Matsumoto は論文[9]において，c-secure CRT 符号のランダム誤り耐性を向上させる追跡アルゴリズムを提案した. 折原，水木，西関は論文[10]で，c 人以下の結託が生成する ID 情報から，結託者を少なくとも g 人含み，大きさが s の容疑者集合を提示することができる性質, $(c, g/s)$-安全性をもつ 2 元符号を定義し, その構成方法を示した. Safavi-Naini,

† 横浜国立大学大学院環境情報学府
〒240-8501 横浜市保土ヶ谷区常盤台 79-7
† Graduate School of Environment and Information Sciences, Yokohama National University
79-7 Tokiwadai, Hodogaya, Yokohama, 240-8501, Japan
{yoshioka,shikata,tsutomu}@mlab.jks.ynu.ac.jp

Wang は論文[6]において，q 元符号における誤追跡率 ε をもつ c-secure 符号 (q-ary c-secure code with ε-error)を定義した．

一方，Chor, Fiat, Naor は論文[2]において，c 人以下の結託より構成される海賊デコーダから結託者のうち最低 1 人を特定することが可能な放送型コンテンツ配信システムを提案した (traitor tracing)．Staddon, Stinson, Wei は論文[7]において，Chor らの提案したデコーダへの復号鍵の割り当てと同様の組み合わせ論的性質をもつ符号を c-traceability 符号とよび，fingerprinting への適用を想定したその他の符号との関係について言及した．Staddon らはまた，Hollmann, Lint, Linnartz が論文[4]において示した identifiable parent property をもつ符号 (code with identifiable parent property) が c-traceability 符号と組み合わせ論的に近い性質をもつことを示し，その関係について言及した．

本論文では，結託攻撃に対して有効な性質を有する以上のような符号を総じて結託耐性符号 (collusion secure code) とよぶこととする．

本論文では，結託耐性符号のモデル化を行い，各符号間の関係について言及する．

2． 準備

本章では，以降の議論で用いる ID 情報付加と攻撃のモデルについて定義する．以下において，n, l, q, i, j は正整数であるとする．

2．1 ID 情報付加

本論文では，n 人のユーザに対してユーザ ID 情報を含んだデコーダ及びコンテンツを配布するシステムを想定する．デコーダ，コンテンツに付加されるユーザ ID は集合 $Q = \{1, 2, \ldots, q\}$ の元が l 個連結したもので，それぞれ $w^{(1)}, w^{(2)}, \ldots, w^{(n)} \in Q^l$ とする．集合 $F = \{w^{(1)}, w^{(2)}, \ldots, w^{(n)}\}$ は，符号長 l，符号語数 n，符号アルファベット Q の符号である．これを (l, n, q)符号 F とよぶ．

ID 情報は ID 検査アルゴリズムによりデコーダ，コンテンツから取り出される．ID 検査アルゴリズムの出力は集合 $\sum_i = Q \cup M\ (i = \#M \geq 0)$ の元が l 個連結したもので $\sum_i^l$ の元となっている．以降，$\sum_i^l$ の元を l-tuple とよぶ．l-tuple x の j 番目のディジットを x_j とし，$x = x_1 x_2 \ldots x_j \ldots x_l$ のように書く．

ID 情報付加のシナリオは traitor tracing と fingerprinting の 2 つに大別される．traitor tracing [2]では，暗号化されたコンテンツを復号するデコーダに ID 情報が付加される．まずコンテンツを復号するための鍵 (以下セッションキー) SK を l 個に分割する．これを分割セッションキーとよび，それぞれ DK_1, $DK_2, \ldots, DK_l$ とする．各分割セッションキー $DK_i\ (1 \leq i \leq l)$ をそれぞれ q 個の鍵 $K_{1,i}, K_{2,i}, \ldots, K_{q,i}$ を用いて暗号化する．このようにして，分割セッションキーを暗号化したものが $l \cdot q$ 個得られる．これをヘッダとして暗号化されたコンテンツと共に放送する．したがって分割セッションキー DK_i の復号は，鍵 $K_{1,i}, K_{2,i}, \ldots, K_{q,i}$ のどれか 1 つを持っていれば可能である．ユーザに配布されるデコーダは各分割セッションキーに対して復号鍵をそれぞれ 1 つもち，デコーダのもつ l 個の復号鍵が ID 情報を示す．

fingerprinting では，各コンテンツに対して電子透かしにより ID 情報が付加される．今，$1, 2, \ldots, q$ のいずれかを示す透かしをマークとよぶこととする．各コンテンツには l 個のマークが容易に検出されることのない方法で埋込まれるものとする．

2．2 ID 検査アルゴリズム

ID 検査アルゴリズムは入力されたデコーダまたはコンテンツの ID 情報を出力する．出力される ID 情報は $\sum_i^l$ の元，つまり l-tuple である．

traitor tracing においては，ID 検査アルゴリズムは $i = 1, 2, \ldots, l$ について，それぞれ分割セッションキー DK_i を復号している鍵を調べる．この鍵が $K_{j,i}$ であるとき j を出力する．これが $K_{2,i}, \ldots, K_{q,i}$ のいずれとも異なるとき，$\perp$を出力する．得られた l 個の出力を順に連結し最終出力 $x \in \{1, 2, \ldots, q, \perp\}^l$ を得る．この場合 $\sum_l = Q \cup \{\perp\}$ である．$\perp$を出力させるような鍵が存在するかは，使用している暗号アルゴリズムに依存するが論文[2]において Chor らはこのような鍵を想定していない．この場合得られる最終出力は $x \in Q^l$ となる．つまり $\sum_0 = Q$ である．

一方 fingerprinting においては，ID 検査アルゴリズムは入力されたコンテンツから l 個のマークを抽出し，それぞれマークから対応する出力 $1, 2, \ldots, q$ を得る．論文[1][6]ではマークが読み取り不可の場合や，マークそのものがコンテンツの切り取りなどによって失われている場合を想定し，この場合に$\perp$を出力することとしている．この場合 $\sum_l = Q \cup \{\perp\}$ となる．一方，マークは必ず $1, 2, \ldots, q$ のいずれかに対応するものとし，アルゴリズムの出力 x は $x \in Q^l$ とする場合もある．これは $\#Q = 2$ の 2 元符号の場合に多い[3][9]．我々は $\sum_0 = Q$ $(\#M = 0)$ の場合と，$\sum_l = Q \cup \{\perp\}$ $(\#M = 1)$ の場合について考察する．前者をモデル 0 とよび，後者をモデル 1 とよぶこととする．

2．3 攻撃

今，b 個の符号語 $w^{(u_1)}, w^{(u_2)}, \ldots, w^{(u_b)} \in Q^l$ が結託している場合を考える．集合 $C = \{w^{(u_1)}, w^{(u_2)}, \ldots, w^{(u_b)}\} \subset F$ を結託 C とよぶこととする．b は n 以下の正整数である．まず以下の U(C)を定める．

$$\mathrm{U}(C) = \{i \mid w_i^{(u_1)} = w_i^{(u_2)} = \ldots = w_i^{(u_b)}\}.$$

U(C)は結託 C を構成する全ての符号語において値が同じディジット位置の集合である．結託 C は U(C)の位置

のディジットを検出できないため，これを undetected digit とよぶ．それ以外のディジットは結託によって検出されるので detected digit とよぶ．また，結託 C が生成可能な l-tuple の集合を(結託 C の)feasible set とよぶ．

付加された ID 情報に対する最も基本的な攻撃として, detected digit の値の入換が考えられる．これは traitor tracing において，結託がもつデコーダの復号鍵の入換に相当する．モデル i (i = 0, 1) における detected digit の値の入換による攻撃を A(i, 1)とよぶこととする．攻撃 A(i, 1)における結託 C の feasible set を FeS(C ; i, 1)とすると，

$$\mathrm{FeS}(C;i,1)=\{x\in\Sigma_i^l \mid x_j\in\{w_j \mid w\in C\},1\le j\le l\}$$

となる．A(0, 1)は論文[2][7]で用いられている．次にモデル i における結託 C の feasible set が次の FeS(C ; i, 2)となるような攻撃 A(i, 2)を考える．

$$\mathrm{FeS}(C;i,2)=\{x\in\Sigma_i^l \mid x_j=w_j^{(u_1)} \quad for \quad j\in \mathrm{U}(C),1\le j\le l\}.$$

攻撃 A(0, 2)は論文[8]で用いられている．また攻撃 A(1,2)は論文[1]で用いられている．さらに feasible set が以下の FeS(C ; 1, 3), FeS(C ; 1, 4), FeS(C ; 1, 5)となるような攻撃 A(1, 3), A(1, 4), A(1, 5)をそれぞれ考える．

$$\mathrm{FeS}(C;1,3)=\{x\in\Sigma_1^l \mid x_j=w_j^{(u_1)} \quad for \quad j\in \mathrm{U}(C) \quad and$$
$$x_j\in\{w_j \mid w\in C\}\cup\{\perp\} \quad for \quad j\in\{1,2,\ldots,n\}-\mathrm{U}(C),1\le j\le l\},$$

$$\mathrm{FeS}(C;1,4)=\{x\in\Sigma_1^l \mid x_j\in\{w_j \mid w\in C\}\cup\{\perp\},1\le j\le l\},$$

$$\mathrm{FeS}(C;1,5)=\{x\in\Sigma_1^l \mid x_j\in\{w_j^{(u_1)}\}\cup\{\perp\} for \quad j\in \mathrm{U}(C)\}.$$

上の３種類の攻撃はモデル 1 のみで想定される．攻撃 A(1, 4)は論文[6]で用いられている．最後に符号語にランダム誤りが付加される攻撃を考える．この場合Σ_i^l に含まれる全ての l-tuple が生成される可能性がある．モデル i におけるこの攻撃を A(i, 6)とすると feasible set FeS(C ; i, 6) = Σ_i^l となる．図 1 に Q = {1, 2, 3}, C = {221, 231}の場合の各 feasible set を示す．

	A(i, 1)	A(i, 2)	A(i, 3)	A(i, 4)	A(i, 5)	A(i, 6)
モデル0	$2\{2,3\}1$	$2\{1,2,3\}1$				$\{1,2,3\}\{1,2,3\}\{1,2,3\}$
モデル1	$2\{2,3\}1$	$2\{1,2,3,\perp\}1$	$2\{2,3,\perp\}$	$\{2,\perp\}\{2,3\}\{1,\perp\}$	$\{2,\perp\}\{1,2,3\}\{1,\perp\}$	$\{1,2,3\}\{1,2,3\}\{1,2,3\}\{\perp\}\{\perp\}\{\perp\}$

図1．Q = {1, 2, 3}, C = {221, 231}における feasible set

今，desc(A(i, j); c, F)を次のように定義する．但し，c はn以下の正整数であり, (i ,j)∈ {(0, 1), (0,2), (0, 6), (1,1), (1, 2), (1,3), (1,4), (1, 5), (1, 6)}とする．

$$\mathrm{desc}(\mathrm{A}(i,j);c,F)=\bigcup\{\mathrm{FeS}(C;i,j) \mid C\subset F,\#C\le c\}.$$

desc(A(i, j); c, F)は符号 F に関して c 人以下の全ての結託が攻撃 A(i, j)によって生成することが可能な l-tuple の集合である．また l-tuple x ∈ Σ_i^l について次の par(A(i,j); c, x)を定義する．

$$\mathrm{par}(\mathrm{A}(i,j);c,x)=\{C\subset F \mid \#C\le c, x\in \mathrm{FeS}(C;i,j)\}.$$

par(A(i, j); c, x)は，符号 F に関して，攻撃 A(i, j)によって l-tuple x を生成できる c 人以下の全ての結託の集合である．

3． 結託耐性符号

結託 C が C に含まれない符号語 $w\in F$, $w\notin C$ を生成することが可能な場合，C は w を ID 情報としてもつ海賊版コンテンツ(またはデコーダ)を生成することで w が割り当てられたユーザを陥れることが可能である．これを防止するような性質をもつ符号として c-frameproof 符号[1]，c-secure frameproof 符号[8]が提案されている．以降の定義では結託 C の feasible set を FeS(C; i, j)とし，符号 F は(l, n, q)符号とする．

定義1 全ての x ∈ desc(A(i, j); c, F)と全ての C ∈ $\{C\subset F \mid \#C\le c\}$に対して, $x\in$ FeS(C; i,j) ∩ F ならば $x\in C$ であるとき，符号 F は c-frameproof 符号であるといい，これを FP(A(i,j); c)と書く．

定義2 全ての x ∈ desc(A(i, j); c, F), 全ての C, D ∈ $\{C\subset F \mid \#C\le c\}$, $C\neq D$ に対して, x ∈ FeS(C; i, j) ∩ FeS(D; i, j)ならば $C\cap D\neq\phi$ となるとき，符号 F は c-secure frameproof 符号であるといい，SFP(A(i,j); c)と書く．

符号 F が FP(A(i,j); c)であるとき，c 人以下のどの結託も結託者自身らがもつ符号語以外の符号語を生成することができない．符号 F が SFP(A(i,j); c)であるとき，c 人以下のどの結託 C も，C と共通元をもたない c 人以下の結託 D が生成し得る l-tuple を生成することで D を陥れることができない．

結託 C により生成された l-tuple から, 結託 C の元の符号語を特定することを追跡とよぶこととする．追跡が可能な符号として，c-IPP 符号 (code with identifiable parent property)[4], c-traceability 符号[2][7], totally c-secure 符号[1]，誤追跡率ε の c-secure 符号[1][6]がある．

定義3 全ての$x\in$ desc(A(i,j); c, F)に対して，

$$\bigcap_{C\in \mathrm{par}(\mathrm{A}(i,j);c,x)} C \neq \phi$$

が成り立つとき，符号 F は c-IPP 符号であるといい，IPP(A(i,j); c)と書く．

定義4a 2 つの ID $x, y\in\Sigma^l$ に対して，I(x, y) = $\{i \mid x_i=y_i\}$ ($1\le i\le l$)を定義する．

定義4b 全ての $C \in \{C \subset F \mid \#C \leq c\}$と全ての $x \in \mathrm{FeS}(C; i, j)$に対して，$\#\mathrm{I}(x, y) > \#\mathrm{I}(x, z)$となるような符号語 $y \in C$ が必ず 1 つは存在するとき，符号 F は c-traceability 符号であるといい，$\mathrm{TA}(\mathrm{A}(i, j); c)$と書く．但し，$z$ は集合 $F \setminus C$ の任意の元であるとする．

定義5a $x \in \sum_i^l$を入力として，F の符号語 1 つを出力するアルゴリズム T を追跡アルゴリズムとよぶ．

定義5b 全ての $C \in \{C \subset F \mid \#C \leq c\}$，全ての $x \in \mathrm{FeS}(C; i, j)$ に対して，$\mathrm{T}(x) \in C$ となる追跡アルゴリズム T が存在するとき，符号 F は totally c-secure 符号であるといい，$\mathrm{TS}(\mathrm{A}(i, j); c)$と書く．

定義6 全ての $C \in \{C \subset F \mid \#C \leq c\}$，全ての $x \in \mathrm{FeS}(C; i, j)$に対して，$\Pr[\mathrm{T}(x) \in C] > 1 - \varepsilon$ となる追跡アルゴリズムが存在するとき，符号 F を誤追跡率 ε をもつ c-secure 符号であるといい，$\mathrm{S}(\mathrm{A}(i, j); c, \varepsilon)$と書く．但し，Pr[]は入力 x が $\mathrm{FeS}(C; i, j)$の元を 1 つランダムに選ぶことで決定する場合の確率を示す．

$\mathrm{T}(x) \in F \setminus C$ のときを誤追跡という．符号 F が $\mathrm{IPP}(\mathrm{A}(i, j); c)$，$\mathrm{TA}(\mathrm{A}(i, j); c)$，$\mathrm{TS}(\mathrm{A}(i, j); c)$のいずれかであるとき，$c$ 人以下のどのような結託に対しても必ず 1 人は正しく追跡を行うことができる．

折原らは論文[10]において，大きさ s の符号語の集合(容疑者集合) S を提示し，S のうち少なくとも g 人が x を生成した結託の元であることを主張できる性質に注目し，このような性質を$(c, g / s)$-安全性とよんだ．以下$(c, g / s)$-安全性を説明する．まず，集合 F の部分集合を元とする集合族 $\alpha \subset \beta(F)$について以下を定義する．$\beta(F)$は，集合 F のベキ集合を表す．

定義7 g, s を $g \geq 0, s \geq 1$ を満たす整数とする．集合族 α の全ての元と g 個以上の共通元をもつ大きさ s の集合 $S \subset F$ が存在するとき，α は$[g / s]$-detectable であるという．

定義8 g, s を $g \geq 0, s \geq 1$ を満たす整数とするとき，$[g / s]$を指数とよぶ．

一般に，ある集合族 α に対して定義 7 の条件を満たす集合 S は複数存在する．つまり α に対して $[g / s]$-detectable であるような整数の組 g, s は複数組存在する．そこで，α の性質を最も良く表す指数 $[g / s]$ を選ぶために以下のような大小関係 $\prec$ を定義する．

定義9 $g / s < g' / s'$であるか，$g / s = g' / s'$かつ $g < g'$ であるとき，$[g / s] \prec [g' / s']$と書く．$g = g', s = s'$であるとき，$[g / s] = [g' / s']$と書く．$[g / s] \prec [g' / s']$ あるいは $[g / s] = [g' / s']$のとき，$[g / s] \preccurlyeq [g' / s']$と書く．また，任意の$[g / s]$について$[g / s] \preccurlyeq [\infty / \infty]$である．

定義10 $\mathrm{detect}(\alpha) = \max\{[g / s] \mid \alpha$ は$[g / s]$-detectable$\}$を集合族 α の detectable 指数とよぶ．ここで max は大小関係 $\prec$における最大をしめす．また，$\alpha = \phi$ のとき，$\mathrm{detect}(\alpha) = [\infty / \infty]$とする．

定義11 $\mathrm{SI}(F, c) = \min\{\mathrm{detect}(\mathrm{par}(\mathrm{A}(i, j); c, x)) \mid x \in \sum_i^l\}$を符号 F の安全度という．符号 F の安全度 $\mathrm{SI}(F, c) = [g / s]$のとき，$F$ は$(c, g / s)$安全であるといい，$\mathrm{SS}(\mathrm{A}(i, j); c, g / s)$と書く．min は大小関係 $\prec$における最小を示す．

符号 F が $\mathrm{SS}(\mathrm{A}(i, j); c, g / s)$であるとき，海賊版から得られる l-tuple x から，大きさ s の容疑者集合 S を提示しその中の g 人が x を生成したことを主張することができる．

4. 関係

各符号の関係について考察する．

4.1 同一符号クラスにおける feasible set 間の関係

まず $\mathrm{FP}(\mathrm{A}(i, j); c)$に関する以下の命題を示す．

命題1 符号 F が $\mathrm{FP}(\mathrm{A}(0, 2); c)$ならば，$F$ は $\mathrm{FP}(\mathrm{A}(0, 1); c)$である．

(証明) F が $\mathrm{FP}(\mathrm{A}(0, 2); c)$であるとする．このとき定義 1 より，全ての $x \in \mathrm{desc}(\mathrm{A}(0, 2); c, F)$と全ての $C \in \{C \subset F \mid \#C \leq c\}$に対して，

$$x \in \mathrm{FeS}(C; 0, 2) \cap F \text{ ならば } x \in C \quad (1)$$

が成り立つ．$\mathrm{desc}(\mathrm{A}(0, 1); c, F) \subset \mathrm{desc}(\mathrm{A}(0, 2); c, F)$であるから，(1)は，全ての $x \in \mathrm{desc}(\mathrm{A}(0, 1); c, F)$について成り立つ．次に全ての $C \in \{C \subset F \mid \#C \leq c\}$に対して $\mathrm{FeS}(C; 0, 1) \subset \mathrm{FeS}(C; 0, 2)$であるから，式(1)が成り立つとき，以下の式(2)も成り立つ．

$$x \in \mathrm{FeS}(C; 0, 1) \cap F \text{ ならば } x \in C \quad (2)$$

よって F は $\mathrm{FP}(\mathrm{A}(0, 1); c)$である． □

図 2 に $\mathrm{FP}(\mathrm{A}(i, j); c)$の各 feasible set 間の関係を示す．各証明は省略するが，命題 1 と同様に証明が可能である．

次に $\mathrm{SFP}(\mathrm{A}(i, j); c)$に関する以下の命題を示す．

命題2 符号 F が $\mathrm{SFP}(\mathrm{A}(0, 2); c)$ならば，$F$ は $\mathrm{SFP}(\mathrm{A}(0, 1); c)$である．

(証明) F が $\mathrm{SFP}(\mathrm{A}(0, 2); c)$であるとする．このとき定義 2 より全ての $x \in \mathrm{desc}(\mathrm{A}(0, 2); c, F)$, 全ての $C, D \in \{C \subset F \mid \#C \leq c\}, C \neq D$ に対して，

$$x \in \mathrm{FeS}(C; 0, 2) \cap \mathrm{FeS}(D; 0, 2) \text{ ならば } C \cap D \neq \phi \quad (3)$$

が成り立つ．$\mathrm{desc}(\mathrm{A}(0, 1); c, F) \subset \mathrm{desc}(\mathrm{A}(0, 2); c, F)$であるから，式(3)は，全ての $x \in \mathrm{desc}(\mathrm{A}(0,1); c, F)$について成り立つ．また，全ての $C, D \in \{C \subset F \mid \#C \leq c\}, C \neq D$

に対して FeS(C; 0, 1) ∩ FeS(D; 0, 1) ⊂ FeS(C; 0, 2) ∩ FeS(C; 0, 2)であるから，式(3)が成り立つとき，以下の式(4)も成り立つ.

$$x \in \mathrm{FeS}(C; 0, 1) \cap \mathrm{FeS}(D; 0, 1) \text{ならば } C \cap D \neq \phi \quad (4)$$

よって F は SFP(A(0, 1); c)である. □

図3 に SFP(A(i,j); c)の関係を示す. 次に命題3 を示す.

命題3 F が IPP(A(0, 2); c)ならば，F は IPP(A(0, 1); c)である.

(証明) F が IPP(A(0, 2); c)であるとする．このとき定義3 より，全ての $x \in$ desc(A(0, 2); c, F)に対して,

$$\bigcap_{C \in \mathrm{par}(\mathrm{A}(0,2);c,x)} C \neq \phi \quad (5)$$

が成り立つ．desc(A(0, 1); c, F) ⊂ desc(A(0, 2); c, F)であるから，式(5)は，全ての $x \in$ desc(A(0, 1); c, F)について成り立つ．次に全ての $x \in$ desc(A(0, 1); c, F)について par(A(0, 1); c, x) ⊂ par(A(0, 2); c, x)であるから,

$$\left(\bigcap_{C \in \mathrm{par}(\mathrm{A}(0,2);c,x)} C \right) \subset \left(\bigcap_{C \in \mathrm{par}(\mathrm{A}(0,1);c,x)} C \right)$$

である．よって，式(5)が成り立つとき，以下の式(6)も成り立つ.

$$\bigcap_{C \in \mathrm{par}(\mathrm{A}(0,1);c,x)} C \neq \phi \quad (6)$$

したがって F は IPP(A(0, 1); c)である. □

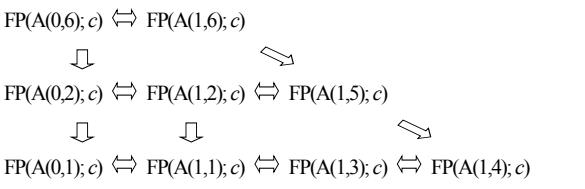

図2. FP(A(i,j); c)の各 feasible set 間の関係

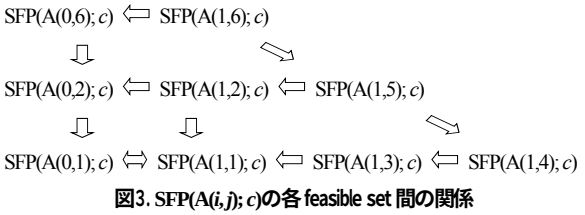

図3. SFP(A(i,j); c)の各 feasible set 間の関係

ここで，FP(A(0, 6); c)と SFP(A(1, 4))が存在しないことを示す命題4, 命題5 を示す.

命題4 $n \geq 2$ において FP(A(i, 6); c)は存在しない.

(証明) 命題4 が c = 1 の場合に成り立つことを証明すれば十分である. ある F の任意の2 つの符号語 $w^{(1)}, w^{(2)}$ ($w^{(1)} \neq w^{(2)}$)を考える．結託 $C = \{w^{(1)}\}$ とすると，$w^{(2)} \in$ FeS(C; i, 6) ∩ F かつ $w^{(2)} \notin C$ である．よって F は FP(A(i, 6); 1)でない．以上は $n \geq 2$ の任意の F について成り立つので FP(A(i, 6); 1)は存在しない. □

命題5 $n \geq 2$ において SFP(A(1, 4); c)は存在しない.

(証明) 命題5 が c = 1 の場合に成り立つことを証明すれば十分である. ある F の任意の2 つの符号語 $w^{(1)}, w^{(2)}$ ($w^{(1)} \neq w^{(2)}$)を考える．結託 $C = \{w^{(1)}\}$，$D = \{w^{(2)}\}$ とすると，$\{\perp\}^I = \mathrm{FeS}(C; 1, 4) \cap \mathrm{FeS}(D; 1, 4)$ かつ $C \cap D = \phi$ である．よって F は SFP(A(1, 4); 1)でない．以上は $n \geq 2$ の任意の F について成り立つので SFP(A(1, 4); 1)は存在しない. □

4．2 符号クラス間の関係

論文[7]では FP(A(0, 1); c), SFP(A(0, 1); c), IPP(A(0, 1); c), TA(A(0, 1); c)の関係について言及している．主要な結果として以下を示す.

命題6[7] F が TA(A(0, 1); c)ならば，F は IPP(A(0, 1); c)である.

命題7[7] F が IPP(A(0, 1); c)ならば, F は SFP(A(0, 1); c)である.

命題8[7] F が SFP(A(0, 1); c)ならば，F は FP(A(0, 1); c)である.

TS(A(0, 1); c)と IPP(A(0, 1); c)について定理1 を示す.

定理1 F が IPP(A(0, 1); c)ならば，F は TS(A(0, 1); c)である．一方，追跡アルゴリズム T が確定的アルゴリズムであるとき，F が TS(A(0, 1); c)ならば，F は IPP(A(0, 1); c)である.

(証明)まず, F が IPP(A(0,1); c)ならば, F が TS(A(0,1); c)であることを示す．F が IPP(A(0, 1); c)であるとする．定義3 より，全ての $x \in$ desc(A(0, 1); c, F)に対して,

$$w \in \bigcap_{C \in \mathrm{par}(\mathrm{A}(0,1);c,x)} C \quad (7)$$

を満たす $w \in F$ が必ず1 つは存在する．ここで x を入力とし w を出力する追跡アルゴリズム T(x) = w を考える．式(7)は全ての $x \in$ desc(A(0, 1); c, F)に対して成り立つ．よって全ての $C \in \{C \subset F \mid \#C \leq c\}$，全ての $x \in$ FeS(C; 0, 1)に対して，T(x) ∈ C となっており．F は TS(A(0, 1); c)である.

次に F が TS(A(0,1); c)であるならば F が IPP(A(0,1); c)であることを示す．F が TS(A(0, 1); c)であるとする．ある l-tuple $x \in$ desc(A(0,1); c, F)について par(A(0,1); c, x) = $\{C_1, C_2, \ldots, C_k\}$ であるとする. 整数 k は1 以上とする．このとき定義5b より，T(x) ∈ C_i (i = 1, 2,…, k)となる確定的追跡アルゴリズム T が存在する．よって,

$$\mathrm{T}(x) \in C_1 \cap C_2 \cap \ldots \cap C_k = \bigcap_{C \in \mathrm{par}(\mathrm{A}(0,1);c,x)} \neq \phi \quad (8)$$

となる．式(8)は全ての $x \in \mathrm{desc}(\mathrm{A}(0,1); c, F)$ に対して成り立つので，F は IPP(A(0, 1); c)である． □

次に IPP(A(0, 1); c)と SS(A(0, 1); $c, g/s$)の関係について，以下の定理を示す．

定理2 $1 \le g \le c$ とする．また，全ての $x \in \mathrm{desc}(\mathrm{A}(0,1); c, F)$に対して，

$$\#\left(\bigcap_{C \in \mathrm{par}(\mathrm{A}(0,1);c,x)} C\right) \ge g \tag{9}$$

が成り立つとする．このとき，F は IPP(A(0, 1); c)かつ SS(A(0, 1); $c, g/g$)である．

(**証明**) 全ての $x \in \mathrm{desc}(\mathrm{A}(0,1); c, F)$ に対して，式(9)が成り立つとする．F が IPP(A(0, 1); c)であることは定義3より明らかである．そこで F が SS(A(0, 1); $c, g/g$)であることを示す．全ての $x \in \mathrm{desc}(\mathrm{A}(0,1); c, F)$について，par(A(0, 1); c, x)は，$S \subset \bigcap_{C \in \mathrm{par}(\mathrm{A}(0,1);c,x)} C$ かつ $\#S = g$ なる S を考えることにより，[g / g]-detectable であり，$\mathrm{detect}(\mathrm{par}(\mathrm{A}(0,1); c, x)) = [g/g]$である．一方，全ての $x \in \sum_0^l \setminus \mathrm{desc}(\mathrm{A}(0,1); c, F)$ については，全ての $C \in \{C \subset F \mid \#C \le c\}$について $x \notin \mathrm{FeS}(C; 0, 1)$となるため，$\mathrm{detect}(\mathrm{par}(\mathrm{A}(0,1); c, x)) = [\infty/\infty]$となる．よって

$$[g/g] = \min\{\mathrm{detect}(\mathrm{par}(\mathrm{A}(0,1); c, x)) \mid x \in \textstyle\sum_0^l\}$$

である．したがって F は SS(A(0, 1); $c, g/g$)である． □

定理3 F **が** SFP(A(0, 1); c)であるとき，F の安全度は少なくとも[1 / c]である．

(証明) F が SFP(A(0, 1); c)であるとする．$x \in \mathrm{desc}(\mathrm{A}(0,1); c, F)$とする．このとき，par(A(0, 1); c, x) の元の数が k 個で，par(A(0, 1); c, x) = $\{C_1, C_2, \ldots, C_k\}$であるとする．$F$ は SFP(A(0, 1); c)なので，$1 \le i \le k, 1 \le j \le k, i \ne j$ について，$C_i \cap C_j \ne \phi$ である．ここで，$C_1, C_2, \ldots, C_k$ のうち元の数が c であるものが必ず1つは存在する．一般性を失うことなく，これを C_1 とし，C_1 を改めて S とおく．このとき，$2 \le i \le k$ について，$\#(C_i \cap S) \ge 1$ である．つまり，par(A(0, 1); c, x)は，[1 / c]-detectable である．よって，$x \in \mathrm{desc}(\mathrm{A}(0,1); c, F)$ に対して，

$$\mathrm{detect}(\mathrm{par}(\mathrm{A}(0,1); c, x)) \succcurlyeq [1/c]$$

となる．また，$x \in \sum_0^l \setminus \mathrm{desc}(\mathrm{A}(0,1); c, F)$ については，全ての $C \in \{C \subset F \mid \#C \le c\}$について $x \notin \mathrm{FeS}(C; 0, 1)$となるため，

$$\mathrm{detect}(\mathrm{par}(\mathrm{A}(0,1); c, x)) = [\infty/\infty]$$

である．よって

$$\min\{\mathrm{detect}(\mathrm{par}(\mathrm{A}(0,1); c, x)) \mid x \in \textstyle\sum_0^l\} \succcurlyeq [1/c].$$

したがって，F の安全度は少なくとも[1 / c]である． □

図4に符号クラス間の関係を示す．

TA(A(0,1); c)

⇩

IPP(A(0,1); c) ⇔ TS(A(0,1); c)

⇩

SFP(A(0,1); c) ⇨ SS(A(1,2); c, 1 / c)

⇩

FP(A(0,1); c)

図4．符号クラス間の関係

5． おわりに

結託耐性符号のモデル化を行い，各想定モデルにおける符号間の関係を解析した．今後の課題として，更なる符号クラス間の関係，特に A(0, 1)以外の feasible set における関係を明らかにしたい．また，各符号クラスの存在条件と構成法も明らかにしたい．

参考文献

[1] D. Boneh and J. Shaw, “Collusion-secure fingerprinting for digital data,” IEEE Transactions on Information Theory 44 (1998), pp.1897- 1905.

[2] B. Chor, A. Fiat and M. Naor, “Tracing traitors,” Advances in Cryptology-Crypto’94, LNCS 839 (1994), 480-491.

[3] H. Guth and B. Pfitzmann, “Error- and collusion-secure fingerprinting for digital data,” Information Hiding ’99, Springer, Lecture Notes in Computer Science, Vol. 1768, pp.134-145, 2000.

[4] H. D. L. Hollmann, J. H. van Lint, J-P. Linnartz and L. M. G. M. Tolhuizen, “On codes with the identifiable parent property,” Journal of Combinatorial Theory A82(1998) pp121-133. 1998.

[5] H. Muratani, “A collusion-secure fingerprinting code reduced by Chinese remaindering and its random-error resilience” Proceedings of the Fourth Information Hiding Workshop, IHW 2001, LNCS, vol.2137, Springer-Verlag, pp.303-315, 2001.

[6] R. Safavi-Naini and Y. Wang, “Collusion secure q-ary fingerprinting for perceptual content,” Security and Privacy in Digital Rights Management (SPDRM'01), Lecture Notes in Computer Science, Vol. 2320, pp. 57-75, 2002.

[7] J. N. Staddon, D. R. Stinson and R. Wei, “Combinatorial properties of frameproof and traceability codes,” IEEE Trans. Information Theory, Vol. 47, 1042-1049, 2001.

[8] D. R. Stinson, T. van Trung, and R. Wei, “Secure frameproof codes, key distribution patterns, group testing algorithms and related structures,” J.statist. Plann. Inference, 86(2), pp.595-617, 2000.

[9] K. Yoshioka and T. Matsumoto, “Random-error-resilient tracing algorithm for a collusion-secure fingerprinting code,” IPSJ Journal Vol. 43 No.8, pp.2502-2510, 2002.

[10] 折原 慎吾, 水木 敬明, 西関 隆夫, “電子透かしの安全性,” 信学技報 COMP2002-3, pp.17-21, 2002.