社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2003－ＣＳＥＣ－22　(33)
2003／7／18

符号の結託耐性に関する考察

吉岡　克成†　　四方　順司†　　松本　勉†

† 横浜国立大学 大学院環境情報研究院　〒240–8501 横浜市保土ヶ谷区常盤台 79–7
E-mail: †{yoshioka,shikata,tsutomu}@mlab.jks.ynu.ac.jp

あらまし　電子透かしを用いたコンテンツへのID情報付加やtraitor tracingのような有料TV放送などのデコーダに対するID情報付加は，複製に個体識別情報を付加する技術という意味でフィンガープリンティングとよばれる．フィンガープリンティングに対する脅威として，フィンガープリント入りの複製を複数集め，その比較を行うことで，ID情報の検出・改ざんを行う結託攻撃がある．このため，結託攻撃に対してなりすまし耐性や追跡性を有する結託耐性符号として，c-frameproof符号，c-secure frameproof符号，c-identifiable parent property符号などが多数提案されている．ここでcは，起こり得る結託の結託者数の最大値を意味している．しかし，これらの多くは組み合わせ論的性質に関して強い条件があるため，その構成を実際に行うにあたっては困難を伴う場合が多い．また，構成法が示されている場合でも，符号長が大きいなど実用的でないことが多い．本論文では，c-frameproof符号，c-secure frameproof符号，c-identifiable parent property符号の組み合わせ論的性質に関する条件をそれぞれ緩めた結託耐性の定義を新たに示した．また，c-frameproof符号の性質に関する条件を緩めた定義に関して，構成の容易なランダム符号がこの条件を満たす確率を近似的に見積もり，数値実験によりその検証を行った．

キーワード　フィンガープリンティング，電子透かし，traitor tracing，結託耐性符号

A Note on Collusion Security of Codes

Katsunari YOSHIOKA†, Junji SHIKATA†, and Tsutomu MATSUMOTO†

† Graduate School of Environment and Information Sciences, Yokohama National University
Tokiwadai 79–7, Hodogaya-ku, Yokohama, 240–8501 Japan
E-mail: †{yoshioka,shikata,tsutomu}@mlab.jks.ynu.ac.jp

Abstract　Fingerprinting, such as watermarking for digital contents or traitor tracing scheme for decoders of broadcast encryption, is a technique to add IDs to each copy of digital data in order to control their distribution. Collusion attacks, in which the attackers collect two or more fingerprinted data and compare them in order to detect and alter the assigned IDs, are considered to be a threat for the fingerprinting system. Therefore, several collusion secure codes, such as c-frameproof code, c-secure frameproof code and c-identifiable parent property code, have been proposed with the aim of enhancing collusion security to the system such as frameproof properties and traceability. Here, c indicates the maximum number of colluding users. However, the combinatorial conditions for these codes are rather harsh so that the constructions are complicated and the length of them may not be practical. In this paper, we relax the definitions of the collusion security for c-frameproof code, c-secure frameproof code and c-identifying parent property code, respectively. We then estimate the probability that randomly generated codes satisfy our relaxed condition derived from c-frameproof code. A numerical experiment is also done in order to support the adequacy of the estimation.

Key words　fingerprinting, watermarking, traitor tracing, collusion secure code

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元の特定を行うことが考えられている．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がコンテンツを復号し利用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元を特定することが考えられている(traitor tracing)．このように，コンテンツやデコーダに対して個体識別情報の付加を行う技術をフィンガープリンティングとよぶ．フィンガープリンティング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．

このため，結託攻撃に対してなりすまし耐性や追跡性を有する結託耐性符号が多数提案されている．これらの多くは組み合わせ論的性質に起因する制約が強いため，その構成を実際に行うにあたっては困難を伴う場合が多い(注1)．また，構成法が示されている場合でも，符号長が長いなど実用的でないことが多い．

本論文では，結託攻撃による"なりすまし"を防止する符号として，c-frameproof符号[1]とc-secure frameproof符号[6]，また，追跡性を有する符号としてc-identifiable parent property符号に注目し，これらの符号の組み合わせ論的条件を緩めた結託耐性の定義を行う．また，c-frameproof符号の性質に関する条件を緩めた定義に関しては，構成の容易なランダム符号がこの条件を満たす確率を近似的に見積もると共に，数値実験によりその考察の検証を行う．

1.1 関連研究

Boneh, Shawは論文[1]において，フィンガープリンティング対象ユーザ総数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．また，Stinson, Trung, Weiは論文[6]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．さらに，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．ここで，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)を新たに示している．そして，折原，水木，西関は論文[4]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．

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)．その後，Staddon, Stinson, Weiは論文[5]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符号とよんでいる．Staddonらはまた，Hollmann, Lint, Linnartzが論文[3]において示したidentifiable parent propertyをもつ符号(code with identifiable parent property，以下，c-IPP符号)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ている．

1.2 本論文の構成

2章では，準備として想定するフィンガープリンティングシステムと符号の関係について説明する．3章では，従来の結託耐性符号の組み合わせ論的条件を緩めた結託耐性符号の定義を新たに行う．4章では，ランダム符号の結託耐性に関する考察を行い，5章では，計算機による数値実験の結果により4章の考察の妥当性を検証する．最後に，6章では今後の課題を述べる．

2. 準　　備

本章では本論文において考えるフィンガープリンティングシステムとID情報の埋込に関して説明を行い，フィンガープリンティングと符号の関係を明らかにする．さらに，符号の結託耐性に関する定義を行う．

2.1 フィンガープリンティングシステム

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考える．デコーダ，コンテンツに付加されるユーザIDは集合$Q = \{1, 2, ..., q\}$の元がl個連結したもので，それぞれ$w^{(1)}, w^{(2)}, ..., w^{(n)} \in Q^l$とする．集合$F = \{w^{(1)}, w^{(2)}, ..., w^{(n)}\}$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$(l, n, q)$符号とよぶ．ここで$l, n, q$は正整数である．また本論文では，集合$Q^l$から$n$個の元を無作為に選ぶことで生成できる$(l, n, q)$符号をランダム$(l, n, q)$符号，または単にランダム符号とよぶこととする．

デコーダへのID情報付加(traitor tracing)，コンテンツへのID情報埋込の順に説明する．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とよぶ)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$DK_1, DK_2, ..., DK_l$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$K_{1,i}, K_{2,i}, ..., K_{q,i}$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lq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$K_{1,i}, K_{2,i}, ..., K_{q,i}$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．

(注1)：Separating Hash Family や Perfect Hash Family を利用する構成法が提案されている[5].

コンテンツへのID情報埋込では，$1, 2, ..., q$ のいずれかを示す電子透かしが各コンテンツに l 個埋込まれるものとする．

2.2 (l, n, q) 符号と結託攻撃

(l, n, q) 符号 $F = \{w^{(1)}, w^{(2)}, ..., w^{(n)}\}$ とその部分集合で b 個の元をもつ集合 C を考える．ここで，b は $1 \leqq b \leqq n$ を満たす整数とする．$u_1, u_2, ..., u_b$ を互いに異なる1から n までの整数であるとし，集合 C を次のように記述する．

$$C = \{w^{(u_1)}, w^{(u_2)}, ..., w^{(u_b)}\}.$$

この集合 C を結託とよぶ．ここで，$C \subset F \subset Q^l$ である．集合 Q^l の元を l-tuple とよぶ．また l-tuple x の i 番目のディジットを x_i と書く．したがって $x = x_1 x_2 \cdots x_l$ である．例として，$(3, 4, 3)$ 符号 $\{113, 211, 322, 233\}$ の符号語のうち，113, 211 が結託する場合を考える．このとき，結託者が所持しているデコーダに内蔵されている復号鍵のいずれを用いても海賊版デコーダを生成することが可能であるため，$\{113, 111, 213, 211\}$ の4種類の l-tuple に対応する海賊版デコーダが生成可能である．今 $F\epsilon S(C)$ を以下のように定義する．

$$F\epsilon S(C) = \{x \in Q^l | x_i \in \{w_i | w \in C\}, 1 \leqq i \leqq l\}.$$

また次の $desc(c, F)$ を定義する．ここで c は $1 \leqq c \leqq n$ を満たす整数とする．

$$desc(c, F) = \bigcup_{C \in \{C \subset F | \#C \leqq c\}} F\epsilon S(C).$$

集合 $F\epsilon S(C)$ は結託 C が生成できる全ての l-tuple の集合であり，$desc(c, F)$ は，符号 F について c 人以下の全ての結託が生成し得る l-tuple の集合である．集合 $C, F, F\epsilon S(C), desc(c, F), Q^l$ の関係を図1に示す．また，$desc(c, F)$ には次のような包含関係がある．

$$F = desc(1, F) \subsetneq desc(2, F) \subsetneq ... \subsetneq desc(n, F) \subset Q^l.$$

図2に $desc(c, F)$ の包含関係を示す．さらに，次の $par(c, x)$ を定義する．

$$par(c, x) = \{C \subset F | x \in F\epsilon S(C), \#C \leqq c\}.$$

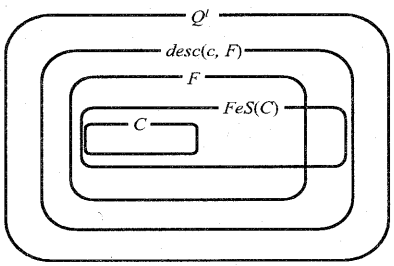

図1　各集合の関係

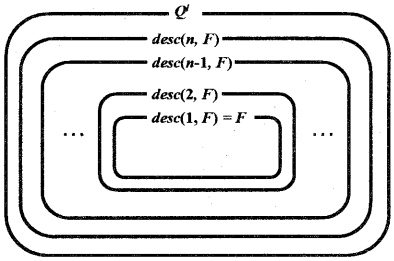

図2　$desc(c, F)$ の関係

3. 結託耐性の定義

論文[1]では，c 人以下のどのような結託によっても，その結託に属さないユーザ(潔白ユーザ)に割り当てられた符号語を生成することができない性質をもつ (l, n, q) 符号として c-frameproof 符号が定義されている．定義1に論文[1]で示された c-frameproof 符号の定義を示す．

[定義1][1]:　符号 F は (l, n, q) 符号であり，c は $1 \leqq c \leqq n$ を満たす整数とする．このとき全ての結託 $C \in \{C \subset F | \#C \leqq c\}$ について，$F \cap F\epsilon S(C) = C$ であるならば，F は c-frameproof 符号であるという．

ここで，個々の結託に対する (l, n, q) 符号 F の性質として定義2を示す．

[定義2]　符号 F は (l, n, q) 符号であるとし，$C \subset F$ とする．$F \cap F\epsilon S(C) = C$ であるならば，符号 F は結託 C に対して frameproof 性をもつという．

さらに，命題1に F が C に対して frameproof 性をもつための必要十分条件を示す．

[命題1]　符号 F は (l, n, q) 符号とし，結託 $C = \{w^{(u_1)}, w^{(u_2)}, ..., w^{(u_b)}\} \subset F$ とする．全ての $i \in \{1, 2, ..., n\} \backslash \{u_1, u_2, ..., u_b\}$ についてそれぞれ $w_j^{(i)} \notin \{w_j^{(u_k)} | 1 \leqq k \leqq b\}$ を満たす整数 j が少なくとも1つは存在することと，符号 F が結託 C に対して frameproof 性をもつことは同値である．但し，$1 \leqq j \leqq l$ である．

(証明) 全ての $i \in \{1, 2, ..., n\} \backslash \{u_1, u_2, ..., u_b\}$ について $w_j^{(i)} \notin \{w_j^{(u_k)} | 1 \leqq k \leqq b\}$ となる整数 j が存在すると仮定する．このとき，どの $i \in \{1, 2, ..., n\} \backslash \{u_1, u_2, ..., u_b\}$ についても，結託 C が有していないシンボルが第 j ディジットに存在するため，$w^{(i)} \in F\epsilon S(C)$ となることはない．したがって $F \cap F\epsilon S(C) = C$ となるため，F は C に対して frameproof 性をもつ．次に F が C に対して frameproof 性をもち，さらに $1 \leqq j \leqq l$ の全ての j について $w_j^{(i)} \in \{w_j^{(u_k)} | 1 \leqq k \leqq b\}$ となるような $i \in \{1, 2, ..., n\} \backslash \{u_1, u_2, ..., u_b\}$ が存在すると仮定する．このとき $\{w^{(i)} \cup C\} \subset F \cap F\epsilon S(C)$ となるため，F が C に対して frameproof 性をもつという仮定に反する．したがって，このような i は存在しない．よって命題が証明された．　□

次に，$C, D \subset F, C \cap D = \emptyset$ を満たす2つの結託 C, D を考える．$F\epsilon S(C) \cap F\epsilon S(D) = \emptyset$ のとき，この2つの結託は同一の l-tuple を生成することができないため，互いになりすます

事ができない．論文[6]では，互いに共通要素をもたない2つのc人以下の結託が互いになりすますことができない符号としてc-secure frameproof符号を定義している．定義3に論文[6]で示されたc-secure frameproof符号の定義を示す．

[定義3][6]: 符号Fは(l,n,q)符号であり，cは$1 \leqq c \leqq n$を満たす整数とする．このとき，$C,D \subset F$，$C \cap D = \emptyset$，$\#C, \#D \leqq c$を満たす全ての結託C,Dについて$FeS(C) \cap FeS(D) = \emptyset$であるとき，$F$は$c$-secure frameproof符号であるという．

次に個々の共通要素をもたない2つの結託C,Dに対する(l,n,q)符号Fの性質として定義4を示す．

[定義4] 符号Fは(l,n,q)符号であり，cは$1 \leqq c \leqq n$を満たす整数とする．このとき，$C,D \subset F$，$C \cap D = \emptyset$，$\#C, \#D \leqq c$を満たす2つの結託C,Dについて$FeS(C) \cap FeS(D) = \emptyset$であるとき，$F$は$C,D$に対してsecure frameproof性をもつという．

さらに，命題2に符号Fが結託C,Dに対してsecure frameproof性をもつための必要十分条件を示す．

[命題2] 符号Fは(l,n,q)符号とし，$C,D \subset F$，$C = \{w^{(u_1)}, w^{(u_2)}, ..., w^{(u_b)}\}$，$D = \{w^{(v_1)}, w^{(v_2)}, ..., w^{(v_d)}\}$，$C \cap D = \emptyset$とする．ここで$u_1, u_2, ..., u_b$は1から$n$までの互いに異なる整数であり，同様に$v_1, v_2, ..., v_d$も1から$n$までの互いに異なる整数であるとする．また$1 \leqq b, d \leqq n$である．このとき，$\{w_j^{(u_i)} | 1 \leqq i \leqq b\} \cap \{w_j^{(v_i)} | 1 \leqq i \leqq d\} = \emptyset$となる整数$j$が少なくとも1つは存在することと，符号$F$が結託$C,D$に対してsecure frameproof性をもつことは同値である．但し，$1 \leqq j \leqq l$とする．

(証明) $\{w_j^{(u_i)} | 1 \leqq i \leqq b\} \cap \{w_j^{(v_i)} | 1 \leqq i \leqq d\} = \emptyset$であると仮定する．このとき，$C$と$D$は第$j$ディジットにおいて共通のシンボルをもたないため，同様のl-tupleを生成することはできず，$FeS(C) \cap FeS(D) = \emptyset$となる．したがって$F$は$C$と$D$に対してsecure frameproof性をもつ．次にFがC,Dに対してsecure frameproof性をもち，さらに$1 \leqq j \leqq l$を満たす全てのjについて$\{w_j^{(u_i)} | 1 \leqq i \leqq b\} \cap \{w_j^{(v_i)} | 1 \leqq i \leqq d\} \neq \emptyset$であるとする．このとき，$\{x | x_j \in \{w_j^{(u_i)} | 1 \leqq i \leqq b\} \cap \{w_j^{(v_i)} | 1 \leqq i \leqq d\}, 1 \leqq j \leqq l\}$の元が必ず1つは存在する．これを$x$とすると，$x \in FeS(C) \cap FeS(D)$となるため，$F$が$C,D$に対してsecure frameproof性をもつという仮定に反する．したがって，$\{w_j^{(u_i)} | 1 \leqq i \leqq b\} \cap \{w_j^{(v_i)} | 1 \leqq i \leqq d\} \neq \emptyset$となる$j$が必ず存在する．よって命題が証明された． □

符号がなりすまし耐性を有していても，結託がどの符号語とも一致しないl-tupleを生成する場合は，不正者の追跡を行うことができない．論文[3]ではc人以下の結託によって生成されたどのl-tuple xに対してもxを生成した結託者のうち最低1人は追跡できる性質をもつ符号としてc-identifiable parent property符号(以降，c-IPP符号)が定義されている．論文[3]で示されたc-IPP符号の定義を以下に示す．

[定義5][3]: 符号Fは(l,n,q)符号であるとする．全てのl-tuple $x \in desc(c,F)$について，$\bigcap_{C \in par(c,x)} C \neq \emptyset$であるとき，$F$は$c$-IPP符号であるという．

個々のl-tuple $x \in desc(c,F)$に対する，(l,n,q)符号Fの性質として定義6を示す．

[定義6] 符号Fは(l,n,q)符号であるとする．あるl-tuple $x \in desc(c,F)$について，$\bigcap_{C \in par(c,x)} C \neq \emptyset$であるとき，$F$は$x$に対して$c$-IPP性をもつという．

4. ランダム符号の結託耐性

本章では，ランダム符号のframeproof性に関して考察を行う．具体的には，(l,n,q)符号Fがランダム(l,n,q)符号であるとき，Fが無作為に構成されるb人の結託Cに対してframeproof性を有する確率を導く．

まず，ある(l,n,q)符号$F = \{w^{(1)}, ..., w^{(n)}\}$とその部分集合である結託$C = \{w^{(u_1)}, ..., w^{(u_b)}\}$を考える．$1 \leqq j \leqq l$において次のように$M_j$を定義する．

$$M_j = \{w_j^{(u_i)} | 1 \leqq i \leqq b\} \tag{1}$$

M_jは結託Cの第jディジットで使われているシンボルの集合である．

今，集合Q^lから無作為にn個の元を選ぶことで符号Fが構成され，またb人の結託CはこのFから無作為にb個の符号語を選ぶことで構成される場合について考える．ここで以下の近似を考える．$1 \leqq i \leqq n$，$1 \leqq j \leqq l$，$1 \leqq k \leqq q$を満たす全ての整数i,j,kについて，

$$Pr[w_j^{(i)} = k] = 1/q \tag{2}$$

とする(注2)．今，結託はFから無作為にb個の符号語を選ぶことで構成されるので，$1 \leqq i \leqq b$，$1 \leqq j \leqq l$，$1 \leqq k \leqq q$を満たす全ての整数i,j,kについて

$$Pr[w_j^{(u_i)} = k] = 1/q \tag{3}$$

となる．さらに，$\#M_j$の期待値$E(\#M_j)$を考える．

$$E(\#M_j) = \sum_{m=1}^{min(q,b)} m \cdot Pr[\#M_j = m] \tag{4}$$

ここで，$min(q,b)$はq,bのうち，最小値をさす．

次に確率$Pr[\#M_j = m]$について考える．ここでmは$1 \leqq m \leqq min(q,b)$を満たす整数である．まず，$w_j^{(u_i)}$が1からqまでのいずれの値も取り得るとするとき$\#M_j = m$となるM_jの選び方の総数を$h(j,q,m,b)$とおく．例えば$\#M_j = 1$となるのは，$w_j^{(u_1)} = w_j^{(u_2)} = ... = w_j^{(u_b)}$の場合しかありえないから，$h(j,q,1,b) = q$である．一般に各$j$に対して以下が成り立つ．

$$h(j,q,m,b) = \begin{cases} q & (m = 1) \\ \binom{q}{m} \left\{ m^b - \sum_{i=1}^{m-1} h(j,m,i,b) \right\} & (m \geqq 2) \end{cases} \tag{5}$$

(注2)：式(2)で示される近似は，$w_j^{(i)}$の値が，各i，jにおいてそれぞれ独立に決定するという近似を同時に意味していることに注意する．

式 (3) が成り立つと仮定すると，

$$Pr[\#M_j = m] = h(j, q, m, b)/q^b \qquad (6)$$

となる．このとき，式 (6) は $j = 1, 2, ..., l$ について成り立つ．

今，ある潔白ユーザに割り当てられた符号語 w が結託 C によって生成可能であるとき，$1 \leqq j \leqq l$ について $w_j \in M_j$ である．式 (2) が成り立つと仮定すると，F のいずれの符号語のいずれのディジットも 1 から q までのシンボルを等確率でもつため，w が結託 C によって生成される確率は $\prod_{j=1}^{l}(\#M_j/q)$ となる．潔白ユーザは全部で $n-b$ 人存在するから，全ての結託ユーザに対してなりすましが出来ない確率，つまり符号 F が結託 C に対して frameproof 性を有する確率は，式 (2) が成り立つと仮定すると，

$$\left(1 - \prod_{j=1}^{l} \frac{\#M_j}{q}\right)^{n-b}$$

となる．また，式 (3) が成り立つと仮定するとき，上の確率の期待値は，

$$\left(1 - \prod_{j=1}^{l} \frac{E(\#M_j)}{q}\right)^{n-b} \qquad (7)$$

となる．さらに式 (2)，(3) が成り立つと仮定するとき，式 (6) より，$E(\#M_1) = E(\#M_2) ... = E(\#M_l)$ であるから，式 (7) は，

$$\left\{1 - \left(\frac{E(\#M_1)}{q}\right)^{l}\right\}^{n-b} \qquad (8)$$

と書くことが出来る．

5. 数値実験

本章では，4 章におけるランダム符号の frameproof 性に関する考察の妥当性を計算機による数値実験により検証する．まず，(l, n, q) 符号 F がランダム (l, n, q) 符号であり，F の部分集合である b 人の結託 C が無作為に構成される場合に，F が C に対して frameproof 性を有している確率を式 (8) を用いて計算し，これを理論値とする．次に，実際に計算機により実際に符号をランダムに構成し，さらに結託をランダムに構成した場合に，その frameproof 性を検査した実験値との比較を行う．

5.1 実験内容

$(l, n, q) = (30, 10, 7)$，$(30, 20, 7)$，$(30, 30, 7)$，$(30, 50, 7)$，$(30, 70, 7)$，$(30, 100, 7)$，$(30, 1000, 7)$ の場合(注3)についてそれぞれ，以下の手順で数値実験を行った．

(1) (l, n, q) 符号を 10 個ランダムに生成する．(注4)

(2) 手順 (1) において生成された各 (l, n, q) 符号に対してそれぞれ以下を行う．

(2-1) $2 \leqq b \leqq n$ ($n \leqq 50$ のとき) または，$2 \leqq b \leqq 50$ ($n > 50$ のとき) についてそれぞれ以下を行う．

(2-1-1) 無作為に b 個の符号語を選ぶ(注5)ことを 10000 回行い，10000 個の結託を生成する．

(2-1-2) 手順 (2-1-1) で生成した結託に対してそれぞれ各符号が frameproof 性をもっているかどうかを命題 1 に示す必要十分条件を用いて検査する．10000 個の結託のうちいくつの結託に対して frameproof 性を有しているかカウントする．

(3) 10 個の符号についてそれぞれ行ったカウントの平均を出す．これを 10000 で割ることで各 b においてこの 10 個の符号が frameproof 性を有している確率の平均値を計算する．

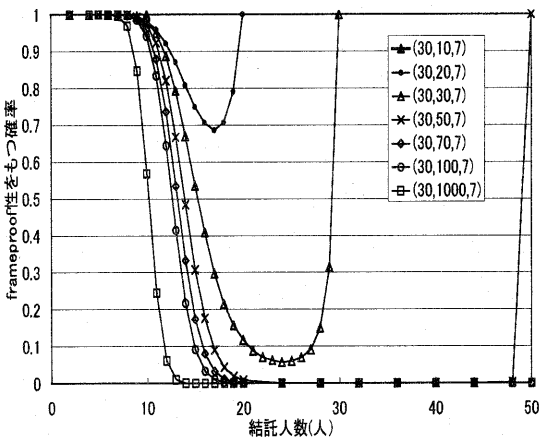

図 3 ランダム符号の frameproof 性 (数値実験結果)

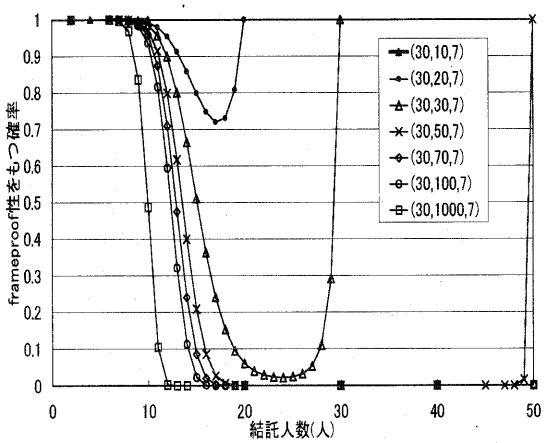

図 4 ランダム符号の frameproof 性 (理論値)

(注3)：traitor tracing において，シンボル数 q はヘッダサイズに依存した制限をもつ．また，電子透かしを用いたフィンガープリンティングにおいては生成できるバリエーションの数に対応するため，同様に制限があると思われる．今回の実験ではそれらを考慮して比較的小さい $q = 7$ を用いた．さらに符号語数 n に関しては数値実験に使用する計算機の能力の制限からフィンガープリンティングシステムとしては非常に小さい規模の 10 から 1000 の範囲についてのみ行った．

(注4)：符号の生成は C 言語の rand 関数を用いて 1 から q までの整数を生成することを繰り返し行うことで行った．この際，同様の符号語が重複して生成された場合は新たに符号語を生成し，重複がないようにした．また，生成された 10 個の符号は互いに異なっていることを確認した．

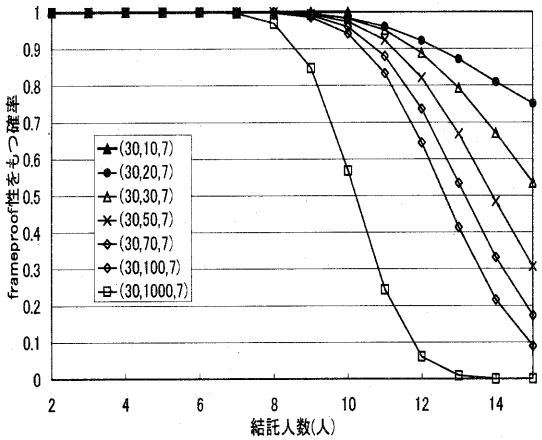

図 5　ランダム符号の frameproof 性 (数値実験結果)
図 3 の $2 \leqq b \leqq 15$ の範囲の拡大図

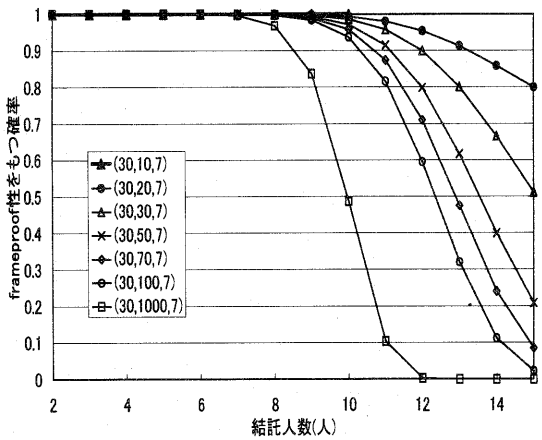

図 6　ランダム符号の frameproof 性 (理論値)
図 4 の $2 \leqq b \leqq 15$ の範囲の拡大図

5.2 実験結果

図 3 および図 5 に実験結果を示す．ここで横軸は結託人数 b であり，縦軸は各 b において frameproof 性を有している確率の平均値 (10 個の符号の平均値) であり，前節の手順 (3) で得られる実験値である．図 3 は実験を行った範囲全体である $2 \leqq b \leqq 50$ における実験結果である．一方，図 5 は図 3 の $2 \leqq b \leqq 15$ の範囲を拡大したものである．

5.3 理論値との比較

図 4 および図 6 に図 3 および図 5 の実験値に対応する理論値をそれぞれ示す．これは式 (8) から導出される．実験値と理論値は類似しており，このパラメータにおいて，式 (2), (3) に示した近似が有効であることを示しているといえる．また，実験値，理論値ともに結託人数 b が 8 人から 10 人を超えると frameproof 性をもつ確率が低下を始めていることが分かる．

6. おわりに

本論文では，c-frameproof 符号，c-secure frameproof 符号，c-identifiable parent property 符号に対して，これらの符号の組み合わせ論的条件を緩めた結託耐性の定義を行った．また，構成の容易なランダム符号の frameproof 性について，理論的な考察を行い，計算機による数値実験との比較を行った．今後の課題としては，c-secure frameproof 符号と c-identifiable parent property 符号に関しても同様の考察を行い，ランダム符号の結託耐性に関する考察を進めたい．

文　献

[1] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," IEEE Trans. Information Theory Vol. 44, pp.1897–1905, 1998.

[2] B. Chor, A. Fiat and M. Naor, "Tracing traitors," Advances in Cryptology - Crypto'94, LNCS Vol.839, pp.480–491, 1994.

[3] H. D. L. Hollmann, J. H. van Lint, J-P. Linnartz and L. M. G. M. Tolhuizen, "On codes with the identifiable parent property," J. Combinatorial Theory A82, pp.121–133, 1998.

[4] S. Orihara, T. Mizuki and T. Nishizeki, "New security index for digital fingerprinting and its bounds," IEICE Trans. Vol.E86-A, No.5, pp.1156–1163, 2003.

[5] J. N. Staddon, D. R. Stinson and R. Wei, "Combinatorial properties of frameproof and traceability codes," IEEE Trans. Information Theory, Vol. 47, pp.1042–1049, 2001.

[6] D. R. Stinson, Tran 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.

(注5)：符号の生成と同様に rand 関数を用いた．しかし結託に関しては重複を許すこととした．