様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　２０　日現在

機関番号：　１２１０２
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３０００３

研究課題名（和文）不正者全員を特定できる電子指紋符号の容量公式の導出および特定アルゴリズムの開発

研究課題名（英文）Developments of the Capacity Formula and Identification Algorithms for a Catch-All Digital Fingerprinting Code

研究代表者

古賀　弘樹（KOGA, Hiroki）

筑波大学・システム情報系・教授

研究者番号：２０２７２３８８

交付決定額（研究期間全体）：（直接経費）　　3,100,000円

研究成果の概要（和文）：電子指紋符号は，ディジタルコンテンツの著作権を保護し海賊版の流通を抑止するための技術である．本研究では，自分たちのディジタルコンテンツから海賊版を生成する不正者を全員特定できる電子指紋符号を考え，情報理論的な立場からその同時容量の特徴づけを行なった．特に，電子指紋符号が２値でc人の不正者がインタリーブ攻撃として知られる攻撃を行なった場合の電子指紋符号の同時容量について詳細に解析し，同時容量に関する上界と下界の高次の項の特徴づけに成功した．また，不正者が２名の場合には，スコア関数に基づく不正者特定アルゴリズムを提案し，同時容量の下界を得た．

研究成果の概要（英文）：Digital fingerprinting codes are used for protecting digital contents from piracy. In this study we consider digital fingerprinting codes that can identify all the malicious users who generate an illegal copy from their contents and characterize the joint capacity from an information-theoretic viewpoint. We analyze the joint capacity of binary digital fingerprinting codes against the interleaving attack of c malicious uses in detail. We succeeded in obtaining higher orders of upper and lower bounds of the joint capacity as a function of c.
In addition, for the case of c=2 we propose an algorithm for identification of all the malicious users based on a score function. This algorithm leads to a lower bound of the joint capacity.

研究分野：　情報理論

キーワード：　電子指紋符号　結託体制符号　容量公式　不正者特定　電子透かし　コンテンツ保護

１．研究開始当初の背景

電子指紋符号(Digital Fingerprinting Code)は，ライセンスのあるディジタルコンテンツの不正配信を抑止するための技術であり，情報理論的な立場からの研究が Boneh と Shaw (1998) 以降発展してきている．M 人のユーザに対する電子指紋符号の問題は，通常次の形に定式化される．

(1) コンテンツ供給者は，各ユーザの ID 情報に１対１に対応する符号語を生成し，その符号語を埋め込んだディジタルコンテンツを各ユーザに配信する．
(2) 悪意のある一部のユーザ（不正者グループ）は結託して，自分たちのもつディジタルコンテンツから不正なコンテンツを生成し，海賊版として配信する．
(3) コンテンツ供給者は，海賊版コンテンツを見出したときには，その海賊版コンテンツから抽出される符号語を用いて，生成に関わった不正者グループの一部または全部を，高い確率で特定する．

コンテンツ供給者が海賊版コンテンツから抽出する符号語から不正者グループを特定できるためには，海賊版コンテンツから抽出する符号語と，不正者グループのメンバーに対応する符号語の間には相関がなければならない．通常は不正者グループの攻撃に「マーキング仮定」という制約を入れて，これらの間に相関があるようにする．

上記(2)においては，不正者グループは，自分たちが海賊版を生成したことをできるだけ知られないように行動する．逆にコンテンツ供給者は，不正者グループの攻撃に対して，不正者グループのメンバーの一部または全部が特定できるような符号語生成と不正者特定のアルゴリズムをもつ必要がある．理想的には，マーキング仮定を満たす範囲内のあらゆる攻撃に対して，コンテンツ供給者は不正者を特定ができるようにしたい．

既存の電子指紋符号の研究の多くが，不正者グループの少なくとも１人を特定することを目的としており，不正者グループ全員を特定することを意図した理論的な研究はほとんどなかった．一方，研究代表者は，2011 年に有限射影平面に基づく電子指紋符号を用いれば，適当な条件のもとで不正者グループ全員を特定できることを示していた．

また，電子指紋符号では，不正者グループの人数の上界を既知としたときに，不正者全員を特定できるための容量（同時容量）を求めることは重要である．電子指紋符号の容量が C のとき，符号語長 n を十分大きくすると，その電子指紋符号はユーザ数 2^{nC} 以下で使うことができる．不正者グループの攻撃に対するできるだけ一般的な条件のもとで同時容量を求めることは課題の１つであった．

２．研究の目的

本研究では，電子指紋符号の同時容量の公式を導出し，特徴づけすることを目標とした．特に，インターリーブ攻撃として知られる攻撃は，同時容量 C_{int} が不正者数を c とするとき $1/c^2$ のオーダーで減少することが知られていたが，c が十分大きいときに $C_{\mathrm{int}} \approx 1/(2c^2 \ln 2)$ もしくは $C_{\mathrm{int}} \approx 1.1604/(2c^2 \ln 2)$ を満たすという相反する２つの結果が公表されていた．数値的には後者が正しいように見えるが，後者の導出には不自然な仮定と数値的な最適化が必要であった．本研究では，インタリーブ攻撃 C_{int} の上界と下界を c の関数として導出し，c が小さい場合であっても精度のよい近似を与えることを目標とした．

３．研究の方法

(1) 符号の生成

$n \geq 1$ を任意の整数として，$U_n = \{1,2,...,M_n\}$ をユーザ全体の集合とする．コンテンツ供給者は，ユーザ j に対して n ビットの符号語 $X^{(j)}$ を生成し，ユーザ j に配信するディジタルコンテンツに埋め込む．ここに，符号語 $X^{(j)}$ の各成分は，１となる確率が w となるように独立に生成する．

(2) 不正者グループの攻撃

c 人の不正者グループを考える．不正者グループは，自分たちに配信されたコンテンツを持ち寄り，結託して海賊版コンテンツを生成する．海賊版コンテンツから抽出される n ビットの符号語を Y と書く．Y の各成分は，成分ごとに独立に，ある条件つき確率分布に従って生成される．条件となるのは，不正者グループに対応する符号語の同じ成分である．この条件つき確率分布が不正者の攻撃を決定する．本研究ではインターリーブ攻撃を考えるので，この条件つき確率分布は，不正者グループに対応する符号語の該当する成分の１の個数で決定する．

(3) 電子指紋符号の同時容量

不正者特定器は，各ユーザのコンテンツに埋め込まれた符号語と不正者数 c を既知として，海賊版コンテンツから抽出した符号語から c 人を不正者グループのメンバーとして出力する．このときの誤り確率を P_n とおく．P_n が $n \to \infty$ で漸近的に 0 になるという条件のもとでのユーザ数の指数部 $\log M_n / n$ の上限を w に関して最大化したものをを同時容量と定義する．

本研究では，インターリーブ攻撃に対する同時容量 C_{int} の上界と下界を c の関数として評価することが目的になる．

４．研究成果

我々は次の成果を得た．

定理１：インターリーブ攻撃の同時容量の下界は次式で与えられる．

$$C_n \geq 1/(2\ln 2\cdot c^2)+1/(12\ln 2\cdot c^2\ln c)$$
$$+1/(12\ln 2\cdot c^2\ln^2 c)+o(1/c^2\ln^2 c)$$

定理１の導出にはテイラー展開および２項分布の平均まわりのｋ次モーメント(k≧1)の間の関係式を利用する．

定理１は，３つの性質(A) $s(c)/c\in(0,1)$，(B) $c\to\infty$において$s(c)/c\to 0$，(C) $c\to\infty$において$s(c)\to\infty$，を満たす関数$s(c)$を利用して次の形に拡張することができる．

系１：インターリーブ攻撃の同時容量の下界は次式で与えられる．

$$C_n \geq 1/(2\ln 2\cdot c^2)+1/(12\ln 2\cdot c^2 s(c))$$
$$+1/(12\ln 2\cdot c^2 s^2(c))+O(1/c^2 s(c)^2)$$

$s(c)=(\ln c)^{\alpha}$とした場合の同時容量の下界を図１に示す．赤線はc^2C_{int}を表しており，青はその極限値である 1.1604 を表す．c が小さい場合であっても，α を適当に選ぶことによって，よい近似が得られていることが確認できる．

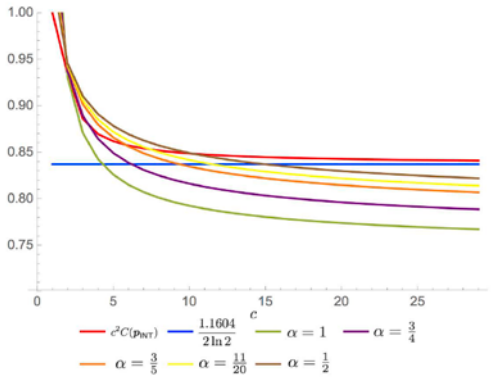

図１　同時容量（青）と下界

数式処理ソフトウェア Mathematica を使うと，下界のより高次の項まで求めることができる．具体的には次の下界を得た．

$$C_n \geq 1/(2\ln 2\cdot c^2)+1/(12\ln 2\cdot c^2 s(c))$$
$$+1/(12\ln 2\cdot c^2 s^2(c))$$
$$+19/(120\ln 2\cdot c^2 s^3(c))$$
$$+9/(20\ln 2\cdot c^2 s^4(c))$$
$$+863/(504\ln 2\cdot c^2 s^4(c))$$
$$+o(1/c^2 s^5(c))$$

$s(c)=(\ln c)^{3/4}$とした場合の 2≦c≦100 の下界の振舞いを図２に，$s(c)=(\ln c)^{1/2}$とした場合の 2≦c≦1000 の下界の振舞いを図３にそれぞれ示す．

上界については次の形を得た．

定理２：$\varepsilon>0$と$\eta>0$を任意に小さい定数とする．c が十分大きいとき，次式が成り立つ．

$$C_{\mathrm{int}} \leq 1/(2\ln 2\cdot c^2)$$
$$+(1+\eta)(\ln c)^{(1+\varepsilon)/2}/(2\ln 2\cdot c^2)$$
$$+(1+\eta)^2(\ln c)^{(1+\varepsilon)}/(2\ln 2\cdot c^2)$$
$$+\cdots$$

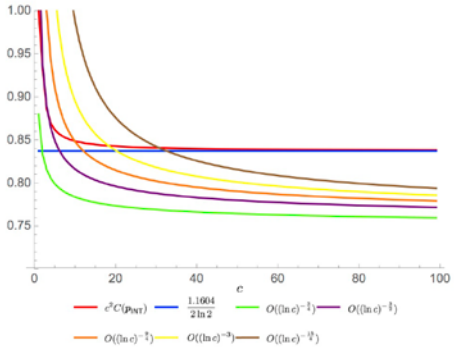

図２　下界の漸近的な振舞い(2≦c≦100)

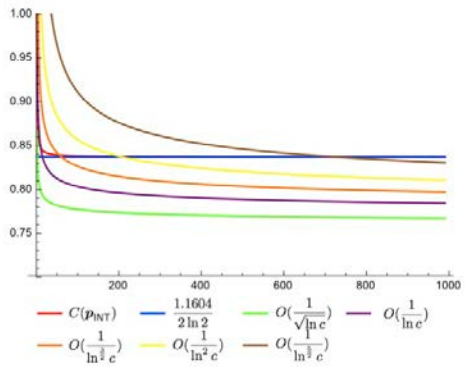

図３　下界の漸近的な振舞い(2≦c≦1000)

定理２の証明には，同時容量を達成する w の値を c の関数として見積もる必要があり，証明の中では$w=\Omega(c(\ln c)^{(1+\varepsilon)/2})$であることを用いている．

以上が主たる研究成果であり，下記５の雑誌論文[2]で公開したものである．この他の成果として，雑誌論文[1]では不正者グループが AND 攻撃を行う場合に，誤り確率が 0 に真に等しい場合の同時容量の上界と下界を評価している．学会発表[1]では，c=2 の場合にスコア関数に基づく不正者グループの特定アルゴリズムを提案し，同時容量の下界を求めている．雑誌論文[3]では，関連する研究として，近年提案された Guessing Secrecy という規範のもとでの暗号システムの安全性を議論した．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　３　件）

[1] S. Kamiya and H. Koga, “New Fundamental Properties on a Secret-Key Cryptosystem under Guessing Secrecy Criteria,” Proceedings of the 2016

International Symposium on Information Theory and Its Applications, pp. 350-354, Monterey(USA), 2016. （査読あり）
http://ieeexplore.ieee.org/document/7840443/

[2] H. Koga and K. Itabashi, “A Higer Order Analysis of the Joint Capacity of Digital Fingerprinting Codes against the Interleaving Attack,” Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security, pp.23-28, Vigo (Spain) 2016. (査読あり)
DOI: 10.1145/2909827.2930788

[3] H. Koga, “On the Capacity and the Zero-Error Capacity of k-Resilient AND Anti-Collusion Codes,” Proceedings of the 2014 IEEE Information Theory Workshop, pp.178-182, Hobart(Austoralia), 2014.(査読あり)
DOI: 10.1109/ITW.2014.6970816

〔学会発表〕(計 4 件)

[1] 神谷, 古賀, “平文と鍵の推測確率を考慮した共通鍵暗号システムの基本的性質,” 信学技報 IT2015-123, pp.137-142, 電気通信大学（東京都・調布市), 2016.

[2] 古賀, 板橋, “インターリーブ攻撃に対する電子指紋符号の同時容量の評価,” 信学技報 IT2015-124, 電気通信大学（東京都・調布市), 2016.

[3] 武井, 古賀, “JPEG 画像の消失部分を復元できる電子透かしの提案と性能評価,” 信学技報 IT2015-39, pp.31-36, 白山菖蒲亭（石川県・加賀市), 2015.

[4] 古賀, 板橋, “連続分布に基づき符号語が生成される電子指紋符号の容量の下界について,” 信学技報 IT2015-1, pp.1-6, 京都国際交流会館（京都府・京都市）, 2015.

６．研究組織
(1)研究代表者
古賀　弘樹（KOGA, Hiroki）
筑波大学・システム情報系・教授
研究者番号：20272388