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

令和　４ 年　 ６ 月 １９ 日現在

機関番号：１２１０２
研究種目：基盤研究(C)（一般）
研究期間：2018～2021
課題番号：１８Ｋ１１１５１

研究課題名（和文）電子指紋符号における不正者全員を特定する頑健なアルゴリズムの構築と同時容量の導出

研究課題名（英文）Construction of a Robust Algorithm for Identification of All Malicious Users of a Digital Fingerprinting Code and Characterization of the Joint Capacity

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）　　3,000,000円

研究成果の概要（和文）：電子指紋符号は，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る．電子指紋符号では，ディジタルコンテンツの中に，ユーザに１対１に対応する符号語を埋め込んで，悪意のある複数のユーザが結託して不正なコンテンツを生成しても，不正に加担したユーザの一部または全部を特定できるように設計する．本研究では，電子指紋符号のユーザ数と密接に関係するユニバーサル単純容量およびユニバーサル同時容量を解析した．電子指紋符号の問題をわずかに拡張することにより，これらの公式を得ることに成功した．これらはよく知られた形ではあるが，順定理と逆定理の証明を厳密に与えたことが既存研究とは大きく異なる．

研究成果の学術的意義や社会的意義
本研究で導出した電子指紋符号のユニバーサル単純容量およびユニバーサル同時容量の公式は，既存の文献の中にも現れている形ではあるが，既存の文献の中には容量の達成可能性および容量より大きいレートの達成不可能性の厳密な証明の記載はなく，真の意味での容量としての意味は確立されていなかった．本研究では，達成可能性および達成不可能性を厳密に証明したという点で，既存研究とは異なる．本研究の証明において鍵になったのは，電子指紋符号の問題の拡張の他，複数のスコア関数を用いた特定器の構成，仮説検定問題における等式，Sion のミニマックス定理などである．複数のスコア関数を用いた特定器は，実用的にも示唆を与え得る．

研究成果の概要（英文）：Digital fingerprinting codes are used to protect copyrights of digital contents from piracy. In a digital fingerprinting code, we embed a codeword corresponding to a user into a digital content. We need to design a digital fingerprinting code so that we can identify all or a part of malicious users who collude and generate a pirated copy. In this study we investigate the universal simple capacity and the universal joint capacity of a digital fingerprinting code, where these capacities are related to the number of users under which we can use the digital fingerprinting code reliably. We give explicit forms of the universal simple capacity and universal joint capacity under slight modification of the problem. Although the formulas themselves can be found in previous studies, we have given rigorous proofs of the direct parts and the converse parts.

研究分野：情報理論

キーワード：電子指紋符号　結託耐性符号　符号化定理　容量公式

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る．電子指紋符号では，ディジタルコンテンツの中に，ディジタルコンテンツを配信するユーザと１対１に対応する長さnの符号語を埋め込む．ユーザ集合の中に悪意をもつc人のユーザ（不正者グループ）を考え，不正者グループは上書きされた符号語が埋め込まれた海賊版コンテンツを生成する．特定者は，海賊版コンテンツから上書きされた符号語を抽出し，不正者グループのc人のメンバー全員を特定することを試みる．この問題設定において，符号語長nが十分大きいときに，不正者グループ全員の特定に失敗する確率P_nが無視できる大きさとなる方式を構築することが電子指紋符号の問題の基本問題となる．特に，ユーザ数をM_nとしたとき，$P_n \to 0$ $(n \to \infty)$のもとで， M_nは一般には符号語長nの指数関数のオーダで大きくなることが知られているが，その指数部のnの係数は電子指紋符号の容量と呼ばれている．

電子指紋符号に対する情報理論的な研究は Boneh と Shaw (1998) [1]に始まり，本研究の開始当初においても理論または計算機シミュレーションを用いた様々な研究が行われていた．特に，電子指紋符号の容量に関する研究が Moulin [2], Huang and Moulin [3], Laarhoven [4]などによって行われていた．[2] では様々な問題設定のもとで容量を達成する電子指紋符号の構成が議論されていたが，プレプリントは非常に読みにくい論文となっており，現在に至っても論文誌での公開はされていない．[3]は，[2]で与えられた容量公式は与えられたものとして，容量の実際の値の評価を行っている．[4]では，電子指紋符号の問題が２つの視点から整理され論じられている．１つ目は，特定者の立場から見たときに，不正者グループの(A)攻撃が既知であるか (B)未知であるかという視点，２つ目は，特定者が (i) ユーザごとに不正者グループに属するかどうかを判定するか，もしくは(ii)ユーザ集合のc人の部分集合全体を考えて，それぞれの部分集合に対して不正者グループかどうかを判定するか，という視点である．電子指紋符号の容量は，(A)(i)および(A)(ii)の視点から見る場合はそれぞれ「単純容量」「同時容量」と呼ばれ，(B)(i)および(B))(ii)の視点から見る場合はそれぞれ「ユニバーサル単純容量」「ユニバーサル同時容量」と呼ばれる．[4]では，(A)(i)の視点から，対数尤度比を用いた特定器が提案されているが，(A)(ii)への拡張は大雑把な議論がなされており，信頼性を欠くものとなっている．(B)(i)および(B)(ii)の視点は[4]ではほとんど論じられていない．

以上をまとめると，本研究の研究開始当初には，電子指紋符号の容量が４種類あること，それらの形のおよその想像はついていた．しかしながら，それらの容量公式が正しいことを示す厳密な証明は与えられていなかったといえる．

２．研究の目的

本研究では，４種類の電子指紋符号の容量を，情報理論の標準的な道具を用いながら，厳密な形で導出することを目的とした．電子指紋符号の容量の問題の難しさが何であるかを明らかにすること，および，電子指紋符号の容量公式の特徴づけを行うことも目的とした．

３．研究の方法

本研究では，M_n個の符号語を，ある確率分布P_Xに従って，成分ごとに独立に生成する状況を考える．電子指紋符号の容量公式を得るためには，C を容量としたとき，$R < C$を満たすRを任意に固定したとき，$M_n = 2^{nR}$人のユーザに対して特定失敗確率P_nが$P_n \to 0$ $(n \to \infty)$ を満たす特定器を構成する（順定理）ことに加えて，$P_n \to 0$ $(n \to \infty)$を満たすすべての特定器に対して$R \leq C$であること（逆定理）を示す必要がある．

本研究では不正者グループの人数を$c = 2$とし，(A)の不正者グループの攻撃モデルが既知の場合を考えた．本研究で考えた不正者グループの攻撃モデルは，[2][3][4]でも扱われている条件つき確率分布を用いるものである．攻撃に先立ち，不正者グループは，マーキング仮定と呼ばれる制約を満たす条件つき確率分布を任意に１つ選び固定する．不正者グループは，自分たちのもつ符号語の対応する成分に応じて，成分ごとに独立に，選んだ条件つき確率分布に従って上書きされた符号語を生成する．特定器は，確率分布P_Xに従って生成されたM_n個の符号語と，不正者グループが生成した上書きされた符号語から，不正者グループが任意に定めた条件付き確率が与えられるという仮定のもとで，２名の不正者グループを特定する．この状況において，まず(i)の単純容量および(ii)の同時容量を導出することを考えた．

次に，同じく不正者グループの人数を$c = 2$とし，(B)の状況，すなわち，特定器が，不正者グループが上書きされた符号語の生成に用いる条件つき確率分布を知ることができないという状況を考える．この場合において，ユニバーサル単純容量およびユニバーサル同時容量の導出を試みた．

最後に，不正者グループの人数を$c = 2$から増やし，一般化できるかどうかを考察した．

４．研究成果

(1) 電子指紋符号の単純容量Cの公式の導出を行った．具体的な容量公式は次の通りである．

$$C = \max I(X;Y)$$

ここに最大値は符号語生成のために用いる確率分布P_Xに関してとり，$I(X;Y)$は符号語の１シンボルXと上書きされた符号語の１シンボルYの間の相互情報量を表す．

順定理の証明には，[3]で提案されている対数尤度比に基づく特定器を用いる．逆定理の証明には，情報スペクトル理論[5]における仮説検定に関する不等式を用いる．逆定理の導出方法には新規性があり，不正者グループの特定器に対して，通常より少し強い性質を仮定する必要があった．この結果は文献[6]に示されている．

(2) 電子指紋符号のユニバーサル単純容量C_{univ}の公式の導出を行った．具体的な容量公式は次の通りである．

$$C_{univ} = \max \min I(X;Y)$$

ここに最大値は符号語生成のために用いる確率分布P_Xに関してとり，最小値は不正者グループが用いる条件つき確率分布全体(マーキング仮定を満たす条件付き確率分布全体)についてとる．$I(X;Y)$は(1)と同じである．

順定理の証明には，マーキング仮定を満たす条件つき確率分布全体の集合を離散化し，それぞれに対して対数尤度比を求めてそれらの最小値をとるという手法を用いる．逆定理の証明には，Sion によるミニマックス定理と，(1)の逆定理で得られた結果を用いる．順定理，逆定理とも新規性があるが，特に順定理の証明で用いた手法は新しい特定器を定義しており，興味深いものとなっている．この結果も文献[6]に示されている．

(3) 電子指紋符号の同時容量Cおよびユニバーサル同時容量C_{univ}の公式の導出を行った．具体的な形はそれぞれ次の通りである．

$$C = \max I(X\tilde{X};Y)/2$$

$$C_{univ} = \max \min I(X\tilde{X};Y)/2$$

ここに，最大値は符号語生成のための確率分布P_Xに関して，最小値はマーキング仮定を満たす条件つき確率分布全体についてとる，Xと$\tilde{X}$は確率分布P_Xに従う独立な確率変数，YはXと$\tilde{X}$を与えたときの上書きされた符号語の出力を表す．

導出の基本的な考え方は上記(1),(2)と同じであるが，順定理の証明においては２段階の不正者の特定が必要になる点で異なる．これらの結果は文献[7]で示された．

(4) 上記(1)～(3)の結果は，不正者グループの人数が$c = 2$の場合のものであるが，基本的な考え方はcの値には依存しない．一般に不正者グループの人数が$c \geq 2$人の場合，単純容量およびユニバーサル単純容量の公式に変化はなく，同時容量およびユニバーサル同時容量の公式は，それぞれ

$$C = \max I(X_1X_2\cdots X_c;Y)/c$$

$$C_{univ} = \max \min I(X_1X_2\cdots X_c;Y)/c$$

という形になる．ここに，$X_1, X_2, \ldots, X_c$は符号語生成に用いる確率分布P_Xに従う独立な確率変数である．順定理はc段階の特定器を用いることになるが，上記の公式を導くためにはマーキング仮定のもとでの相互情報量間に成り立つ不等式を示す必要がある．

(5) 本研究の副次的な成果であるが，電子指紋符号とも関係する視覚暗号の成果も得られた．具体的には，Ateniese らが提案した Extended Visual Cryptography Scheme (EVCS)[8]において，シェアが与えられたときの秘密情報の安全性を新たに定義し，その新しい安全性基準を満たす EVCS を構成した．この結果は文献[9]に記載されている．

<引用文献>

[1] D. Boneh and J. Shaw, ``Collusion-secure fingerprinting for digital data,'' IEEE Trans. Inf. Theory, vol. 44, no. 5, pp. 1897–1905, 1998.

[2] P. Moulin, ``Universal fingerprinting: capacity and random-coding.exponents,'' Proc. 2008 IEEE ISIT, Tronto, Canada, pp. 220–224, 2008.

[3] Y. W, Huang and P. Moulin, ``On the saddle-point solution and the large-collusion asymptotics of fingerprinting games,'' IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 160–175, 2012.

[4] T. Laarhoven, ``Asymptotics of fingerprinting and group testing: bounds from capacity-achieving log-likelihood decoders,'' EURASIP J. Inf. Security, 2016:3, 2016.

[5] 韓，情報理論における情報スペクトル的手法，培風館，1998.
[6] H. Koga, ``Coding theorems on the simple capacity for digital fingerprinting codes,'' Proc. ISITA 2020, pp.61–64, 2020.
[7] H. Koga, ``Coding theorems on digital fingerprinting coding under informed and uninformed setups,'' Proc. 2021 IEEE ITW, Kanazawa, REG-WE1.C, 2021.
[8] G. Ateniese, C. Blundo, S. A. De Santis and D. R. Stinson, ``Extended schemes for visual cryptography,'' Theor. Comput. Sci., vol.250, no.1-2, pp.143–161, 2001.
[9] K. Sekine and H. Koga, ``Optimal basis matrices of a visual secret sharing scheme with a meaningful shares and analysis of its security,'' IEICE Trans. on Fundamentals, vol. E104-A, pp.1235-1244, 2021.

５．主な発表論文等

〔雑誌論文〕　計5件（うち査読付論文　5件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Hiroki Koga	４．巻 -
２．論文標題 Coding Theorems on the Simple Capacity for Digital Fingerprinting Codes	５．発行年 2020年
３．雑誌名 Proceedings of 2020 International Symposium on Information Theory and its Applications	６．最初と最後の頁 61--65
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Yohei Ookawa and Hiroki Koga	４．巻 -
２．論文標題 An Ideal Secret Sharing Scheme Realizing an Access Structure Based on a Finite Projective Plane of Order 3	５．発行年 2020年
３．雑誌名 Proceedings of 2020 International Symposium on Information Theory	６．最初と最後の頁 852--856
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISIT44484.2020.9174121	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Hiroki Koga	４．巻 -
２．論文標題 A Lower Bound on the Joint Capacity of Digital Fingerprinting Codes Using Score Functions Based on Log-Likelihood Ratio	５．発行年 2018年
３．雑誌名 Proceedings of 2018 IEEE International Symposium on Information Theory	６．最初と最後の頁 1136--1140
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISIT.2018.8437922	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Hiroki Koga	４．巻 -
２．論文標題 Coding Theorems on Digital Fingerprinting Coding under Informed and Uninformed Setups	５．発行年 2021年
３．雑誌名 Proceedings of 2021 IEEE Information Theory Workshop	６．最初と最後の頁 REG-WE1.C
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ITW48936.2021.9611451	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 K. Sekine and H. Koga	4．巻 E104-A
2．論文標題 Optimal basis matrices of a visual secret sharing scheme with a meaningful shares and analysis of its security	5．発行年 2021年
3．雑誌名 IEICE Trans. on Fundamentals	6．最初と最後の頁 1235--1244
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020DMP0010	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計3件（うち招待講演　0件／うち国際学会　0件）

1．発表者名 古賀弘樹
2．発表標題 電子指紋符号の同時ユニバーサル容量の下界の導出
3．学会等名 第11回シャノン理論ワーウショップ
4．発表年 2019年

1．発表者名 古賀弘樹
2．発表標題 電子指紋符号の単純容量に関する符号化定理
3．学会等名 電子情報通信学会情報理論研究会
4．発表年 2019年

1．発表者名 關根達也，古賀弘樹
2．発表標題 混合型の攻撃に対する電子指紋符号の同時容量の評価
3．学会等名 電子情報通信学会情報理論研究会
4．発表年 2018年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関