様式 C-19

科学研究費補助金研究成果報告書

平成２３年　５月２３日現在

機関番号：１２１０２
研究種目：基盤研究(C)
研究期間：2008～2010
課題番号：20500004
研究課題名（和文）　確率的符号器をもつ情報理論的に安全な暗号システムにおける符号化定理
研究課題名（英文）　Coding Theorems for Information-Theoretically Secure Systems with Stochastic Encoders
研究代表者
古賀　弘樹（KOGA HIROKI）
筑波大学・大学院システム情報工学研究科・准教授
研究者番号：20272388

研究成果の概要（和文）：
本研究は，確率的符号器をもつ情報システムについて深く考察し，特に敵対者からの攻撃に対して理論的に安全な情報システムに対して新たな知見を得た．本研究では，一般情報源をもつシャノンの暗号システムに対して，符号器が確率的な場合にも有効な新しい形の符号化定理を導出した．また，シェアの改ざんを試みる不正な参加者のもとでも安全性が保証される(n,n)しきい値法を提案し，その安全性を理論的に示した．さらに，有限射影平面に基づく電子指紋符号を解析し，すべての不正者が特定されるための条件を考察した．

研究成果の概要（英文）：
In this study we analyzed information systems with stochastic encoders and developed new results. First, we established novel coding theorems for Shannon's cipher system with a general source, where an encoder of the system can be stochastic. We also proposed a new simple n-out-of-n threshold scheme that is secure against a substitution attack by shareholders. In addition, we considered a digital fingerprinting code for copyright protection using a finite projective plane and obtained conditions under which all the malicious users are identifiable from a pirated content.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,100,000	330,000	1,430,000
2009 年度	1,000,000	300,000	1,300,000
2010 年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,100,000	930,000	4,030,000

研究分野：情報理論
科研費の分科・細目：情報学・情報学基礎
キーワード：情報理論的安全性，確率的符号器，秘密分散法，電子指紋

１．研究開始当初の背景

(1) 極めて広いクラスの情報源・通信路の符号化を扱う「情報スペクトル的手法」の立場は，新しい情報理論的な視点として定着していた．多くの既知の符号化定理の拡張ができることは分かっていたが，新しい符号化定理への発展が期待されていた．

(2) 確定的(deterministic)でない，確率的(stochastic)な符号器を用いると，従来の結果を含む一般的な符号化定理が得られる場合があることが，研究代表者によ

って示されていた．確率的符号器に対する符号化定理は，確率的下極限などの情報スペクトル的手法で導入された概念を用いるが従来議論されていなかった．

(3) 最も基本的な共通鍵暗号系であるシャノンの暗号システムでは，秘密情報が，無記憶性などを仮定しない一般的な情報源から出力される場合は，順定理と逆定理の間にギャップがあり，最適性に関する議論が残っていた．

(4) 敵対者がいる場合の秘密分散法，電子指紋符号など，より詳細な性能解析が求められながらも，十分な知見が得られていない興味深い問題があった．これらの問題の中で使う符号器は，一様乱数を用いるので一種の確率的符号器とみなすことができる．

２．研究の目的

確率的符号器をもつ情報システム，特に敵対者からの攻撃に対して理論的に安全な情報システム，対して深く考察し，新しい形の符号化定理など，新たな知見を得て将来的な応用につなげることが本研究の目的である．前述の共通鍵暗号システムは，従来型の符号化定理では最適性が保証できない端的な例であり，最適性を保証できる新しい形の符号化定理の導出を目指す．

さらに本研究では，確率的符号器をもち，理論的に安全性を保証する必要がある情報システムを考察する．具体的には，敵対者がいる場合の秘密分散法，不正者の結託のもとでも安全な電子指紋符号に対して，ある与えられた安全性規範を満たし効率のよい最適な方式を構成することも併せて目的とした．

３．研究の方法

共通鍵暗号システムに対しては，1(1)で述べた情報スペクトル的手法の立場からアプローチする．確率的符号器を，与えられた入力に対して複数の符号語を出力できる条件つき確率分布として捉え，符号語のレート，鍵のレートに関する符号化定理を述べる．

敵対者のいる秘密分散法に対しては，従来の Shamir のしきい値法をもとにした方式でなく，新たな方式を考える．具体的には，符号器と復号器が鍵を共有できる状況を考え，不正者の分散情報の改ざんの成功確率が小さいことが保証される方式を導出する．

電子指紋符号の問題では，有限射影平面として知られる離散構造に基づく符号を考える．有限射影平面に基づく符号では，符号語が一種の対称性をもつため解析がしやすい．本研究では，不正者の攻撃の制限としてよく用いられる「マーキング仮定」のもとで，構成した符号が不正者全員を特定できるための必要条件，十分条件について考察を行う．

４．研究成果

(1) 共通鍵暗号システム

無記憶性，マルコフ性などの仮定のない，一般情報源に対する固定長符号化の問題を考察した．符号器は，情報源から出力される長さ n の系列を，確率的符号器を用いて符号語に変換し，復号器は送られてきた符号語から情報源出力を復元する．本研究では，復号誤り確率が n→∞のもとでゼロに収束するという要請のもとで，任意の確率的符号器と決定的復号器に対して成り立つ不等式を導出した．得られた不等式の特別な場合として，符号語のレートに関する既存の逆定理が導ける．

この結果は,一般的な情報源から秘密情報が出力されるシャノンの暗号システム（共通鍵暗号システム）に対しても拡張できる．実際，復号誤り確率が n→∞のもとでゼロに収束し，さらに，ある安全性基準を満たす任意の確率的符号器と決定的復号器が満たすべき不等式を２つ導出した．不等式は符号語（暗号文）のレート，および鍵のレートにそれぞれ関連し，例えば無記憶情報源から秘密情報が出力される状況では，２つの不等式はそれぞれ暗号文のレートおよび鍵のレートの下界を与える．逆に，か靴的な符号化の一種である Homophonic Coding と呼ばれる手法を用いると，２つの不等式が等号で満たされることがわかる．

(2) 秘密分散法

(k,n)しきい値法では，１個の秘密情報を n 個の分散情報（シェア）に符号化する．k-1 個のシェアからは秘密情報に関する知識は全く得られないが，任意の k 個のシェアから秘密情報が完全に復元される．通常，(k,n)しきい値法は有限体上のランダムな k-1 次式を生成して構成されることが多いが，この多項式を用いる方式はシェアの改ざんに弱いことが知られていた．

本研究では，秘密分散法の符号器と復号器が共通の一葉乱数をもつことができれば，シェアの改ざんを高い確率で検出できる(n,n)しきい値法が構成できることを示した．特に，n=2 の場合には，S を秘密情報とするとき，２つのシェア X,Y は

$$X = U^{-1}(S-E), Y = V^{-1}E$$

により生成される，U,V は符号器と復号器で共有する一様乱数であり，有限体の非ゼロ元に値をとる(-1 は逆元を表す)，E は符号器だけが利用できる乱数である．復号時は

$$UX + VY \in \Sigma$$

が成り立つかどうかで改ざんの有無を判定する．ここにΣは秘密情報が値をとる集合である．この方式で改ざんを検出できない確率が $(|\Sigma|-1)/(|C|-1)$ となることを理論的に

示すことができる．CはX,Yが値をとる集合であり，$|\ |$は要素の個数を表す．

同じ方式はnが３以上の場合にも容易に拡張することができる．この場合もシェアの改ざんが検出できない確率は$(|\Sigma|-1)/(|C|-1)$に一致する．すなわち，シェアが値をとるアルファベットのサイズが，秘密情報のアルファベットのサイズよりも十分大きければ，提案方式は不正なシェアの改ざんに対して安全であるといえる．

(3) 電子指紋符号

電子指紋符号は，インターネット等を通じて配信される動画や音楽などの有償コンテンツの不正配信を抑止するための技術である．コンテンツの配信者は，コンテンツを購入するユーザと１対１に対応する符号語を埋め込む．他方，複数の悪意のあるユーザは，符号語が埋め込まれたコンテンツを加工し，自分たちが特定されないように不正なコンテンツ（海賊版）を生成する．電子指紋符号は，このような結託攻撃に対しても耐性をもつように設計する必要がある．

本研究では，マーキング仮定として知られる不正のモデルのもとで，有限射影平面に基づく電子指紋符号の性質を解析した．最初に，悪意のある結託ユーザの数が２の場合を考察し，海賊版を生成したユーザが２名とも特定される場合を，有限射影平面の性質を用いて特徴づけることに成功した．具体的には，L_1,L_2を結託ユーザの符号語に対応する有限射影平面の直線とし，wをマーキング仮定のもとで結託ユーザによって書き換えられた符号語，B_wをwに対応する有限射影平面の点の集合であるとすると，２つの関係式

$|B_w \cap L_1| \geq 3$　かつ　$|B_w \cap L_2| \geq 3$

が成り立つとき，結託ユーザは二人とも特定できる．また，

$|B_w \cap L_1| = 2$　かつ　$|B_w \cap L_2| = 2$

であれば，２名の結託ユーザの候補が３個に絞られることもわかった．

本研究ではまた，この結果を結託ユーザの数が３以上の場合への拡張を考えた．特に，結託ユーザの数が既知のときには，すべての結託ユーザが海賊版から特定されるための十分条件を与えることができた．また，この十分条件が必要条件にもなる場合があることも考察した．

(5) 新しい情報理論的な量とその性質

情報源の固定長符号化の問題は，通常，復号誤り確率がブロック長とともに漸近的にゼロに収束するという要請のもとで，達成可能な符号語のレートを求める問題として定式化される．特に，無記憶性などの仮定のない一般情報源の符号化を考えるときには，達成可能なレートの下限はスペクトル上エントロピーレート$\overline{H}(X)$に一致することが知られている．この$\overline{H}(X)$は，情報源の自己情報量の分布を考えたときの右端としての意味をもつ．

本研究では，自己情報量スペクトルの右端と左端に別の定義を与えた．実際，右端には$\overline{H}(X)$のほかに$\overline{H}^*(X)$の定義が可能であり，左端としては，通常の$\underline{H}(X)$のほかに$\underline{H}^*(X)$が定義できる．本研究では，これらの４つの量の大小関係を明らかにするとともに，$\overline{H}^*(X)$と$\underline{H}^*(X)$が様々な場面で有用であることを明らかにした．

実際，$\overline{H}^*(X)$は復号誤り確率が可算無限回任意にゼロに近づくときの達成可能な符号化レートの下限になる．また，ゼロ次のsmooth Renyiエントロピーを用いて表すこともできる．さらに自己情報量の分布の幅の上界と下界が，これら４個の量を用いて書けることを示した．本研究ではまた，自己情報量の分布の幅が固定長の最悪冗長度の最小値に等しいことを示した．

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５件）

① Hiroki Koga and Yusuke Minami, “A Digital Fingerprinting Code Based on a Projective Plane with Identifiability of All Malicious Users,” IECIE Trans. Fundamentals, vol. E94-A, pp. 223-232, 2011, 査読有.

② Hiroki Koga, “Two Generalizations of a Coding Theorem for a (2,2)-Threshold Scheme with a Cheater,” Proc. 2010 International Symposium on Information Theory and its Applications, Taichung, pp. 678-683, 2010, 査読有.

③ Hiroki Koga, “A Simple Secret Sharing Scheme Using a Key and its Security against Substitution of Shares,” Proc. International Symposium on Information Theory, pp. 2483-2487, Austin, 2010, 査読有.

④ Hiroki Koga, ``New Coding Theorems for Fixed-Length Source Coding and Shannon’s Cipher System with a General Source,” Proc. International Symposium on Information Theory and its Applications, Auckland, pp. 251-256, 2008, 査読有.

⑤ Yi Jin and Hiroki Koga, “Basic Properties of Complete Complementary Codes Using the DFT Matrices and

Kronecker Products, ”Pro. International Symposium on Information Theory and its Applications, Auckland, pp. 887--892, 2008, 査読有.

〔学会発表〕(計7件)

① 古賀弘樹, 有村光晴, 岩田賢一, “情報スペクトルの幅と固定長符号の最悪冗長度,” 電子情報通信学会情報理論研究会, IT2010-83, 大阪大学, 2011年3月3日.
② 古賀弘樹, “４種類の確率的極限と情報源符号化,” 電子情報通信学会情報理論研究会, IT2010-60, 国際奈良学セミナーハウス, 2011年1月18日.
③ Hiroki Koga, “On the Necessary Conditions for Identification of all the Malicious Users by a Digital Watermarking Code Based on a Projective Plane,” 第33回情報理論とその応用シンポジウム予稿集, pp. 426-431, 信州松代ロイヤルホテル, 2010年12月1日.
④ 古賀弘樹, AND攻撃に耐性をもつ結託耐性符号の容量について,” 電子情報通信学会情報理論研究会, IT2009-110, 信州大学, 2010年3月5日.
⑤ 南佑典, 古賀弘樹, ”BIBDを用いた結託耐性符号の基礎的性質,” 第32回情報理論とその応用シンポジウム予稿集, pp. 532-537, 山口湯田温泉ホテルかめ福, 2009年12月3日.
⑥ 古賀弘樹, “情報スペクトル的手法の発展とその秘密分散法への応用,” 電子情報通信学会情報理論研究会, IT2009-47, 山口湯田温泉ホテルかめ福, 2009年12月1日(招待講演).
⑦ 南佑典, 古賀弘樹, “不正者全員を特定できるアフィン平面を利用した結託耐性符号の一構成法,” 2009年暗号と情報セキュリティシンポジウム, 1D1-1, 大津プリンスホテル, 2009年1月20日.

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
古賀　弘樹 (Koga Hiroki)
筑波大学・大学院システム情報工学研究科・准教授
研究者番号：20272388

(2)研究分担者
(　　)

研究者番号：

(3)連携研究者
(　　)

研究者番号：