システム情報工学研究科修士論文概要

年 度	平成 25 年度	学位名	修士(工学)
専 攻	知能機能システム 専攻	著者氏名	金井 紘平

指導教員氏名 古賀 弘樹

論文題目

電子指紋符号の不正検出力の向上に関する研究

論文概要

電子的コンテンツが普及した現在，そのコピーの不正配布・ダウンロードによって制作者の利益が損なわれている．電子的コンテンツに対する不正行為の対策として，それらにID情報を埋め込み不正者を特定可能にする電子指紋符号がある．電子指紋符号に対して不正者側がとれる対策として，結託攻撃と呼ばれるID情報の改ざん行為がある．結託攻撃は，複数の不正者が互いのコンテンツの比較によってID情報の一部を検出し，検出箇所を変更することで行われる．結託攻撃が行われた場合，不正コンテンツのID情報を調べても不正者を特定できず，さらには冤罪が発生する可能性もある．電子指紋符号はそのときでも，誤りなく不正者の何人かを特定できる検出器が設計できることが要求される．電子指紋符号の研究には2つの潮流があり，1つはTardosが与えた確率的な符号方式，もう1つは内符号と外符号の2つの符号を組み合わせた連接符号方式がある．本稿では，連接符号方式の1つであるBoneh-Shaw符号と，新たに与える確率的な電子指紋符号の2つを扱い，その不正検出力の評価をする．Boneh-Shaw符号は，BonehとShawにより与えられた内符号と，内符号を情報源とする一様ランダムな系列である外符号を組み合わせた連接符号であり，任意の数の不正者t人による結託攻撃に対して，不正者少なくとも1人を特定可能な不正検出器が与えられている．この検出器の問題点として，1人の特定しか保証していないことがある．そこで本研究では，不正者が2人の場合に，十分大きい符号語長において不正者全員を誤りなく特定できる不正検出器を提案する．また，Tardosが与えた確率的な電子指紋符号の方式は，符号語の各ビットを異なった確率分布に従って決定する．しかし，各ビットの従う確率分布を変化させることが，最適な方式なのかはわかっていない．そこで本研究では，Tardosによる符号を単純化した符号を考え，その生成方式の妥当性を検証する．具体的には，符号語の全てのビットが異なる2つの確率分布のどちらかに従って決定されるとし，2人の不正者グループが不正検出側にとって既知な２択の攻撃戦略をとる場合において，一定の条件下で符号語の各ビットが従う確率分布を変化させた符号生成が最適となることを示す．

審査日 平成 26 年 1 月 29 日

審査員	（大学名 職名）	（学位）	（氏名）
主査	筑波大学 准教授	博士(工学)	古賀 弘樹
副査	筑波大学 准教授	博士(工学)	掛谷 英紀
副査	筑波大学 准教授	博士(工学)	延原 肇