令和元年度 情報工学コース卒業研究報告要旨

楫 研究室	氏　　名	蒲　浩 輝
卒業研究題目	多項分布のエントロピーに対する上界式の改善	

情報理論は幅広い分野で利用されている基礎理論であるが，近年特に，サイドチャネル攻撃と呼ばれる不正行為のリスクを評価するのに情報量の概念が有用であることが指摘されている．暗号システムにおけるサイドチャネル攻撃とは, 暗号を処理する装置が発する電磁波や熱, 電力量や処理時間の違いなどを物理的に観測してシステム内部の状態や動作を推定し，暗号解読の手がかりを得ようとする攻撃手法のことである. サイドチャネル攻撃のうち, 処理時間の違いをもとに秘密鍵の情報を取得しようとする攻撃手法のことをタイミング攻撃という. タイミング攻撃は比較的容易に実行可能であるため, どのようなシステムでもタイミング攻撃の対象となる可能性がある. 特に，定期券や電子マネーとしても使用される IC カード等のシンプルなシステムでは処理時間が外部から明確に観測される可能性も高く，タイミング攻撃の脅威が深刻となりうる．一方，未知・未発見のタイミング攻撃を具体的に想定し，安全性評価を行うことは非常に困難である．より包括的に，どれだけの秘密鍵情報が処理時間から漏洩しているかを定量的に見積もる，いわゆる情報理論的安全性の評価が重要となる．

タイミング攻撃による漏洩情報量は，多項分布に従う確率変数のエントロピーにより上界が与えられる．しかし，多項分布のエントロピーの計算公式は知られておらず，また，定義式に従ってエントロピーを計算することも，サイドチャネル攻撃を想定した大きなパラメータに対しては事実上不可能である．そのため本論文では，実際に計算可能な，多項分布のエントロピーの限界式の導出を行う．多項分布のエントロピーの限界式の計算方法についていくつかの関連研究が行われている．その中で [楫 16] はスターリングの公式とテイラー級数展開を利用することで，エントロピーの上界式と下界式を導き出している．漸近的には同一の値に収束する上界式と下界式が与えられているが，非漸近的な領域では，上界と真値との間に若干の乖離が見られる．その理由は様々に推測されるが，本研究では，既存研究で採用されている「$1/x$ の多項式上界の精度」に着目した．エントロピーの上界式の導出の過程では，二項分布に従う確率変数 X に対し，$1/X$ の期待値 $E[1/X]$ を計算する必要がある．既存研究では，$1/x$ のテイラー級数展開から $1/x$ の上界となる多項式を導出し，$E[1/X]$ の上界を導き出しているが，得られた上界多項式はテイラー級数の展開点付近でのみ良い精度を持つため，期待値の計算過程で多くの誤差を生み出してしまう．本研究では，上界多項式を導き出して期待値を計算するのではなく，$E[1/(X+1)]$ を正確に計算する公式を最初に導出し，$E[1/(X+1)]$ を使って $E[1/X]$ を上から抑えるアプローチを取る．この改良に基づいてエントロピーの上界式を導き出し，非漸近的な領域において，既存研究よりも優れた特性を持つことを実験的に示す．