様　式　Ｆ－７－１

科学研究費助成事業（学術研究助成基金助成金）実施状況報告書（研究実施状況報告書）（平成２７年度）

1．機関番号　1 4 6 0 3　　2．研究機関名　奈良先端科学技術大学院大学

3．研究種目名　基盤研究(C)（一般）　　4．補助事業期間　平成２７年度～平成２９年度

5．課題番号　1 5 K 0 0 0 1 7

6．研究課題名　漏洩情報の量に基づくセキュリティ解析を可能とする情報量指標の開発

7．研究代表者

研究者番号	研究代表者名	所属部局名	職名
70263431	カジ　ユウイチ 楫　勇一	情報科学研究科	准教授

8．研究分担者

研究者番号	研究分担者名	所属研究機関名・部局名	職名

9．研究実績の概要

平成27年度の研究では，所期の研究実施計画に従い，多項分布のエントロピーの高精度近似式に関する研究に取り組んだ．多項分布のエントロピーを近似するにあたっては，Stirlingの公式により階乗計算を近似することが必要となる．Stirling近似を行った後，Bernstein多項式の計算を進めていくことになるが，予備的検討の段階ではBernstein多項式に関する知見がきわめて限られており，低次数で精度の劣るStirling近似の利用しか行うことができなかった．
平成27年度の研究では，Taylor級数展開と誤差項の関係に着目することにより，Bernstein多項式の具体的な算法に関して非常に大きな進展があった．これにともなって高次数・高精度のStirling近似の利用が可能となり，結果として，エントロピーの近似精度を飛躍的に向上させることができた．具体的には，漸近的領域，非漸近的領域のいずれにおいても有効な上界式および下界式を導出することに成功した．これまでの上界式，下界式の間には，多項分布のパラメータの一つに比例するギャップが存在していたが，本研究で導出した限界式の間にはギャップが存在せず，比較的小さなパラメータ値において，上界式と下界式が収束することが明らかとなった．一連の成果は，量的情報流解析によってサイドチャネル攻撃の脅威を分析するのにきわめて有用であり，工学的にも大きな貢献を与えるものと解釈することができる．
また，本研究に付随する研究課題として，ビットコインを用いた汎用的な計算方式に関する研究を行った．とくに，一連の計算から漏洩する情報の量と匿名性の関係について検討を行い，電子投票システム等への応用可能性について考察を行った．

10. キーワード

(1) 情報理論	(2) 情報セキュリティ	(3) エントロピー	(4) 多項分布
(5) 限界式	(6) 匿名プロトコル	(7)	(8)

11. 現在までの進捗状況

(区分) (1) 当初の計画以上に進展している。

(理由)

平成27年度の研究では，多項分布のエントロピーの近似の高精度化を目標としていた．数学的な検討の進展により，所期の目標は完全に達成しており，同時に，当初計画にはなかった匿名プロトコルに関する知見の獲得にも成功している．以上の状況より，当初の計画以上に進展していると判断することができる．

12. 今後の研究の推進方策　等

(今後の推進方策)

所期の研究計画にしたがい，情報量を評価するための新しい測度について検討を行う．smooth Renyiエントロピーに関する研究調査を中心に行う予定であるが，植松らによる最近の研究動向等も視野に入れつつ，同時に，情報セキュリティ分野との境界条件も考慮に入れて，新しい測度の検討を行う．
研究の遂行にあたっては，サイドチャネル攻撃等の標的とされやすい小規模簡易端末での計算行為にも着目し，実効性の高い情報測度の提案を目指すとともに，セキュアな計算の仕組みについても検討を行う．また，平成27年度の研究で明らかになったビットコイン基盤の汎用性に関する研究も進め，ブロックチェーンベースの計算から漏洩する情報の量についても議論を展開していくことを計画している．

(次年度使用額が生じた理由と使用計画)

(理由)

採録となった論文の掲載が想定より遅くなり，平成28年度となった．このため，平成27年度予算として計上していた別刷り印刷費用が未執行となり，平成28年度に繰り越された．

(使用計画)

繰り越し分については，当初の予定どおり，別刷り印刷費用に充当する．それ以外の部分については，所期の計画に従って使用する予定である．

(課題番号： 15K00017)

(注) ・印刷に当たっては、Ａ４判（縦長）・両面印刷すること。

13.研究発表（平成27年度の研究成果）

〔雑誌論文〕 計（3）件／うち査読付論文 計（3）件／うち国際共著 計（0）件／うちオープンアクセス 計（0）件

著者名	論文標題 【掲載確定】
Jason Paul Cruz, Yuichi Kaji	The Bitcoin Network as Platform for Trans-Organizational Attribute Authentication

雑誌名	査読の有無	巻	発行年	最初と最後の頁	国際共著
情報処理学会論文誌（トランザクション）数理モデル化と応用	有	9	2016	TBD	－

掲載論文のDOI（デジタルオブジェクト識別子）
なし

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

著者名	論文標題
熊谷一騎, 楫勇一	動的なセグメントを用いたフラッシュ符号の構成

雑誌名	査読の有無	巻	発行年	最初と最後の頁	国際共著
電子情報通信学会論文誌 A	有	8	2015	398-401	－

掲載論文のDOI（デジタルオブジェクト識別子）
なし

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

著者名	論文標題
Yuichi Kaji	Performance Evaluation of Index-Less Indexed Flash Codes for Non-Uniform Write Operations

雑誌名	査読の有無	巻	発行年	最初と最後の頁	国際共著
情報処理学会論文誌（トランザクション）数理モデル化と応用	有	8	2015	1-6	－

掲載論文のDOI（デジタルオブジェクト識別子）
なし

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

〔学会発表〕 計(6)件／うち招待講演 計(0)件／うち国際学会 計(3)件

発表者名	発表標題	
Yuki Takeda, Yuichi Kaji, Minoru Ito	On the Computational Complexity of the Solvability of Information Flow Problem with Hierarchy Constraint	
学会等名	発表年月日	発表場所
53rd Annual Allerton Conference on Communication, Control, and Computing (国際学会)	2015年09月27日～2015年09月30日	Monticello, IL, USA

発表者名	発表標題	
Yuichi Kaji	Bounds on the Entropy of Multinomial Distribution	
学会等名	発表年月日	発表場所
2015 IEEE International Symposium on Information Theory (国際学会)	2015年06月14日～2015年06月19日	Hong Kong, China

発表者名	発表標題	
Jason Paul Cruz, Yuichi Kaji	The Bitcoin Network as Platform for Trans-Organizational Attribute Authentication	
学会等名	発表年月日	発表場所
The Third International Conference on Building and Exploring Web Based Environments (国際学会)	2015年05月24日～2015年05月29日	Rome, Italy

発表者名	発表標題	
Jason Paul Cruz, Yuichi Kaji	E-voting System Based on the Bitcoin Protocol and Blind Signatures	
学会等名	発表年月日	発表場所
2016 暗号と情報セキュリティシンポジウム	2016年01月19日～2016年01月22日	ANAクラウンプラザホテル熊本ニュースカイ (熊本県熊本市)

発表者名	発表標題	
Yuichi KAJI	Converging Bounds of the Entropy of Multinomial Distributions	
学会等名	発表年月日	発表場所
第38回情報理論とその応用シンポジウム	2015年11月24日～ 2015年11月27日	下電ホテル（岡山県倉敷市）

発表者名	発表標題	
武田友希, 楫勇一, 伊藤実	階層制約のある情報フロー問題に関する計算理論的考察	
学会等名	発表年月日	発表場所
電子情報通信学会 情報理論研究会	2015年05月21日～ 2015年05月22日	京都市国際交流会館（京都府京都市）

〔図書〕 計（0）件

著者名	出版社	
書名	発行年	総ページ数

14.研究成果による産業財産権の出願･取得状況

〔出願〕 計（0）件

産業財産権の名称	発明者	権利者	産業財産権の種類、番号	出願年月日	国内･外国の別

〔取得〕 計(0)件

産業財産権の名称	発明者	権利者	産業財産権の種類、番号	取得年月日	国内･外国の別
				出願年月日	

15.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

国際研究集会名	開催年月日	開催場所

16.本研究に関連して実施した国際共同研究の実施状況

(1)国際共同研究: ー

17.備考