様 式 Ｃ－７－１

平成２０年度科学研究費補助金実績報告書（研究実績報告書）

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）　　4. 研究期間　平成２０年度　～　平成２２年度

5. 課題番号　2 0 5 6 0 3 5 6

6. 研究課題名　次世代型グループ情報共有・流通のセキュリティ基盤に関する研究

7. 研究代表者

研究者番号	研究代表者名	所属部局名	職名
7 0 2 6 3 4 3 1	ﾌﾘｶﾞﾅ　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（所属研究機関名については、研究代表者の所属研究機関と異なる場合のみ記入すること。）

研究者番号	研究分担者名	所属研究機関名・部局名	職名
	ﾌﾘｶﾞﾅ		
	ﾌﾘｶﾞﾅ		
	ﾌﾘｶﾞﾅ		
	ﾌﾘｶﾞﾅ		
	ﾌﾘｶﾞﾅ		

9. 研究実績の概要

（下欄には、当該年度に実施した研究の成果について、その具体的内容、意義、重要性等を、交付申請書に記載した「研究の目的」、「研究実施計画」に照らし、600 字～800 字で、できるだけ分かりやすく記述すること。また、国立情報学研究所でﾃﾞｰﾀﾍﾞｰｽ化するため、図、ｸﾞﾗﾌ等は記載しないこと。）

本研究課題では，大規模グループ鍵の更新手法に関する研究，自律分散グループ鍵に関する研究の二つの具体的課題を設定し，研究活動を行っている．

このうち，大規模グループ鍵に関する平成20年度の研究では，鍵更新の際の効率悪化を長期にわたって抑制する方式の開発を行った．開発方式では，ユーザの集合とユーザに割り当てる鍵の関係を木構造により決定し，情報源符号化等でしばしば用いられるハフマン符号化アルゴリズムを用いることにより，木構造の断片化を抑制する方式を採用している．計算機実験により，提案手法が従来法に比して，どの程度の効率改善を実現するか評価を行った．

自律分散グループ鍵に関する研究では，とくに，ユーザの権限失効についての研究に注力して研究を行った．研究代表者が以前取り組んでいた時間限定鍵の概念を拡張し，これを時間制約のあるアクセス制御の実現に適用できないか検討を行った．時間限定鍵の利用によって，いったん発行した鍵の追跡管理が不要となるため，とくにユーザ数が多い場合，あるいは，ユーザとの通信が保証されない場合等，現実のサービスにおいてしばしば発生する局面において，当該アプローチが有効である旨の結論を得た．その一方，時間限定鍵の実現に必要となる要素技術の開発については，当該年度内に完了できていない部分が残っている．問題点を明確化し，今後の研究計画の中に適切に位置付けて継続検討を行う予定である．

※　成果の公表を見合わせる必要がある場合は、その理由及び差し控え期間等を記入した調書(A4 判縦長横書１枚)を添付すること。

10. キーワード

(1)　情報セキュリティ	(2)　暗号鍵	(3)　グループ通信
(4)　LKH 法	(5)　マルチキャスト通信	(6)　放送暗号
(7)	(8)	

（裏面に続く）

11.研究発表（平成２０年度の研究成果）

〔雑誌論文〕　計（２）件

著者名	論文標題			
H. Mohri, R. Matsumoto, Y. Kaji	Key Predistribution Schemes for Sensor Networks Using Finite Plane Geometry			
雑誌名	査読の有無	巻	発行年	最初と最後の頁
IEICE Transactions on Information Systems	有	E91-D	2008	1416-1423

著者名	論文標題			
K. Sugiyama, Y. Kaji	On the Minimum Weight of Simple Full-Length Array LDPC Codes			
雑誌名	査読の有無	巻	発行年	最初と最後の頁
IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	有	E91-A	2008	1502-1508

著者名	論文標題			
雑誌名	査読の有無	巻	発行年	最初と最後の頁

〔学会発表〕計（９）件

発表者名	発表標題		
T. Sakamoto, T. Tsuji, Y. Kaji	Group Key Rekeying Using the LKH Technique and the Huffman Algorithm		
学会等名	発表年月日	発表場所	
2008 International Symposium on Information Theory and Its Applications	2008.12.8	Auckland, New Zealand	

発表者名	発表標題		
R. Aoyama, Y. Kaji	Improvement of the Forced-Convergence Decoding for LDPC Codes		
学会等名	発表年月日	発表場所	
2008 International Symposium on Information Theory and Its Applications	2008.12.9	Auckland, New Zealand	

発表者名	発表標題		
Y. Kaji	On the Number of Minimum Weight Codewords of SFA-LDPC Codes		
学会等名	発表年月日	発表場所	
2009 International Symposium on Information Theory	2009.6.29	Seoul, Korea	

発表者名	発表標題		
Y. Kaji	On the Error Performance and Parameter Choices of the Array-Type LDPC Codes		
学会等名	発表年月日	発表場所	
Tenth International Symposium on Communication Theory and Applications	2009.7.16	Ambleside, UK	

発表者名	発表標題	
坂本，楫	α分木ハフマン法を用いたグループ鍵管理方式	
学会等名	発表年月日	発表場所
コンピュータセキュリティシンポジウム2008	2008年10月	沖縄県宜野湾市

発表者名	発表標題	
坂本，楫	ハフマン法を用いたグループ鍵管理方式の詳細な性能検証	
学会等名	発表年月日	発表場所
2009年 暗号と情報セキュリティシンポジウム	2009.1.22	滋賀県大津市

発表者名	発表標題	
野末，楫	視覚型秘密分散共有を利用したフィッシング対策認証方式	
学会等名	発表年月日	発表場所
2009年 暗号と情報セキュリティシンポジウム	2009.1.23	滋賀県大津市

発表者名	発表標題	
Y. Kaji	On the Code Rate and Code Performance of SFA-LDPC Codes	
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	2009.9.30	東京都千代田区

発表者名	発表標題	
杉山，楫	SFA-LDPC符号の低重み符号語の個数について	
学会等名	発表年月日	発表場所
第32回情報理論とその応用シンポジウム	2009.12.2	山口県山口市

〔図　書〕　計（0）件

著者名	出版社	
書名	発行年	総ページ数

12. 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

13. 備考

※　研究者又は所属研究機関が作成した研究内容又は研究成果に関するｗｅｂページがある場合は、ＵＲＬを記載すること。
