ソフトウェアの科学的構築法に関するワークショップ型研究
共同研究における水平分業モデルのケーススタディ

研究代表者　小川瑞史　北陸先端科学技術大学院大学　特任教授
共同研究者　高野明彦　国立情報学研究所　教授

Abstract

現在、計算機科学において、理論的成果と現実問題の要請が乖離した状況が続いている。その有益な融合をはかるためには、理論から応用にいたる異分野間の横断的な理解および信頼感の醸成の場が強く求められている。本提案では、ワークショップ形式の相互啓発の機会を通し、（1）各関連分野における成果・問題点の相互理解、（2）相互の信頼感の醸成、を行い（3）実際に共同研究を推進する（具体的な想定する研究テーマについては研究実施方法の項を参照)。この過程において、分野横断的なテーマの共同研究の水平分業のモデル(共同研究の芽を育む機会の設定法や効率的な共同研究の推進法)を探る。

研究成果概要

本提案ではワークショップ形式の相互啓発の機会を通し、(1) 各関連分野における成果・問題点の相互理解、(2) 相互の信頼感の醸成を行い (3) 実際に共同研究を推進する（具体的な研究テーマについては研究の内容の項を参照)。この共同研究過程のケーススタディを行い、共同研究の水平分業モデルを探ることを目的とした。

今年度の研究成果としては、部分的には既に開始していた以下の二項目の共同研究

＊ NTTで開発中の時刻認証システムのセキュリティモデルの検証（NTT、工学院大学と共同）
＊ 量子計算機向け情報のコーディング法（大阪大学と共同）

について研究を進めた（いずれも異分野間における問題の提起に対する証明の請負という水平分業として遂行された)。

前者は、公開鍵暗号に基づく時刻認証 (rfc-3161など) の長期安全性を補完するイベント順序認証を行うセキュリティモデルの基本的性質の形式的証明を行ったものである。イベント順序認証は、Merkle木と呼ばれる二分木にハッシュ関数を組み合わせたデータ構造の漸増的構成と適宜ルートハッシュ値を公知情報とすることでなされる。この方式はNTTで開発されたが、その基本的性質のうち、特に自己検査を行うSanity検査の正当性の証明は本共同研究で初めて与えた（査読付国際会議(1)、海外論文誌投稿準備中)。

後者は、パスカルの三角形に基づく古典的数え上げ符号（Cover 1973）に対し、パスカル三角形の一般化により、1ビットの符号長のコストのもとで符号中の1の個数を抑えることができることを示した。符号中の1の個数を抑えることは量子計算機では重要な効率化となる。本手法は大阪大学で提案していたが、方式の妥当性を示す上記評価の証明は本共同研究で初めて与えた（口頭発表(2)、IEEE Transaction on Information Theory 投稿中)。

今年度の活動として、3回のコアメンバー・ミーティング、および定理証明に関する試験的な非公

開ワークショップを1回開催した。(その他、個別のメンバー間での研究交流は随時行った。)これらの活動の内容は、

＊ 第一回コアメンバー・ミーティング(JAIST、H17年8月22～23日)
討議内容：定理証明系Isabelle/HOLによるOpen Induction(小川)、ESC/Java紹介(中島)、GETAによる連想検索技術とその実装(高野)

＊ 第二回コアメンバー・ミーティング(工学院大学、H17年10月12日)
討議内容：組込みOSの現状と展望(小野)

＊ 第三回コアメンバー・ミーティング(NII、H18年2月17日)
討議内容：GETAによる連想検索と非同期web処理(高野)、プッシュダウンモデル検査によるJavaの関数間解析(小川)

である。(小野がH17年4月にNTTから工学院大学に移籍したため、第二回は工学院大学で開催した。)定理証明に関するワークショップは、本研究課題の遂行につれ、定理証明系に関する強化が必要であると判断し、試験的に組織横断的(筑波大学、京都産業大学、AIST, NTTも含む12名)な非公式な形式で開催(JAIST, H17年11月28～29日)したものである。具体的な問題に対するさまざまなアプローチを俯瞰する非常に有効な機会であることが確認されたため、来年度以降、このワークショップは年1回程度、定期的に開催を計画している。

その他、関連する活動として、チュートリアル・講習会として以下のものを行った。

＊ プラットフォームOS(小野)、電子情報通信学会・先端オープン講座の一環として 春季H17年7月2日および秋季11月19日の2回開催。内容は、Linux 上の組込みシステム開発経験(NTTの無線LANサービスM-fletsなど)に基づく組込みシステムの実装デザイン法についての講習である。

＊ 汎用連想計算エンジンGETAによる情報の発見(西岡真吾、高野のNIIにおける共同研究者)、JAIST情報科学科研究セミナーの一環として、H18年1月26日に開催。内容は連想検索エンジンGETAの効率的な実装法についてのチュートリアルである。

論 文 発 表 等

[査読付国際会議:]

(1) Mizuhito Ogawa, Eiichi Horita, Satoshi Ono, Proving Properties of Incremental Merkle Trees, Proceedings of the 20th International Conference on Automated Deduction, CADE-20, Springer LNAI 3632, pp.424-440, 2005.

(2) Isao Sasano, Mizuhito Ogawa, Zhenjiang Hu, *Maximum Marking Problems with Accumulative Weight Functions,* Proceedings of International Colloquium on Theoretical Aspects of Computing, ICTAC05, Springer LNCS3722, pp.562-578, 2005.

[口頭発表]

(1) Guoqiang Li, Bochao Liu, Xin Li, Mizuhito Ogawa, Type-directed Trace Analysis of Security Protocols in Process Calculus, 第22回日本ソフトウェア科学会大会(2005. 9. 14 東北大学)

(2) Masahiro Kitagawa, Akira Kataoka, Mizuhito Ogawa, Logarithmic Width Enumerative Coding, 第28回情報理論とその応用シンポジウムSITA2005 (2005. 11. 22 リーザンシーパーク谷茶ベイ)

開催した会議、イベント、メディア発表、特許等

[コアメンバー・ミーティング]（小川，小野，中島，高野によるワークショップ）

(1) 平成17年8月22～23日(北陸先端科学技術　大学院大学)

(2) 平成17年10月12日（工学院大学）

(3) 平成18年2月17日（国立情報学研究所）

その他，メンバー間での個別の研究交流を4回（JAIST→NII 7/10-11, 9/5-6, 1/16-17，およびJAIST→工学院大学 12/9-10）を行った．

[チュートリアル・講習会]

(1) 小野諭，組込み型コンピュータのソフトウェア技術　第3回：プラットフォームOS，電子情報通信学会・先端オープン講座（春季H17年7月2日および秋季11月19日の2回，機械振興会館）

(2) 西岡真吾，汎用連想計算エンジンGETAによる情報の発見、第13回JAIST情報科学科研究セミナー（H18年1月26日，JAIST招聘）

[非公開ワークショップ]

(1) 定理証明と証明系ワークショップ（H17年11月28日～29日，JAIST）