戦略的国際科学技術協力推進事業
日本－フランス研究交流
研究課題「暗号と理論：計算機によって検証された安全性証明」

研究終了報告書

研究交流期間　平成20年2月～平成23年3月

研究代表者：今井 秀樹　（印）
（独立行政法人産業技術総合研究所
情報セキュリティ研究センター、研究センター長）

１．研究・交流の目的

本研究はセキュリティプロトコルの自動安全性証明法の研究および開発を目的とする。具体的には日本側の暗号理論に基づくセキュリティ科学技術と、フランス側の論理学に基づいた計算機科学技術を組み合せ、計算量理論上で厳密に定義された仮定に基づいて記号レベルで安全性証明を行うための、理論構築と技術開発を行う。

本共同研究で日仏が交流を通じて相互的に取り組むことで、学術界および産業界において、コストと安全性が適切に判断された暗号技術やプロトコルが用いられるようになるばかりでなく、情報社会の安心と安全を達成する多くの技術のための基本的かつ本質的な開発ツールを提供されることが期待できる。

２．研究・交流の方法

研究計画時の交流計画は以下の通り。
日本側が主体となる研究交流活動：

- 日本側研究者のフランス側への短中期（２ヶ月程度）の訪問
  特に産総研情報セキュリティ研究センターでプロトタイプを開発するに当たっては、開発者のフランス側への訪問が不可欠である。最初の訪問は 2008 年春を予定している。
- 各年度において、フランス側学生の受け入れ（それぞれ 5 ヶ月程度）
  学生の交換は連携において非常に有効な活動であるため、受入経費を計上している（フランス側の研究者の来日についてはフランス側で計上）。産総研としても、“Ecole Normale Superieure(s)” から学生を受け入れるのはこのプログラムによってのみである。
- 2010 年東京でのワークショップ開催
  本プログラム参加者のみによるクローズドで比較的小規模な国際会議である。これにより、研究交流成果の仕上げを行う予定である。

フランス側が主体となる研究交流活動:

- フランス側研究者の日本側への短中期（2 ヶ月程度）の訪問
  プロジェクトの最終的な目標に向けた共同研究が目的である。最初の訪問は、2008 年 2 月よりを予定している。
- 2009 年パリでの小規模なワークショップの開催

相互訪問で行われる共同研究は、暗号技術や暗号プロトコルの安全性の、記号としての抽象化とソフトウェアプロトタイプの開発における健全性に関する基礎的な研究である。

交流の結果、日、仏で合計 2 回開催されたワークショップでは、日仏以外の多数の参加者を多数集めることができた等、活発かつ予定以上の規模で開催できた。フランス側の学生も本プログラムを含め様々な方法を用い、産総研で受け入れることができた。一方、日本側からフランスにもプロジェクトメンバーの学生を送り、現地での共同研究に参加させることができた。

３．研究・交流実施体制

３．１　日本側

氏名	所属	役職	学位	役割
（リーダー） 今井　秀樹	独）産業技術総合研究所 情報セキュリティ研究センター	研究センター長	博士	プロジェクト統括
（研究者） 渡邊　創	同上	副研究センター長	博士	プロジェクト副統括、分野融合の推進研究
（研究者） 花岡　悟一郎	同上	主任研究員	博士	暗号の情報論的・計算量的安全性理論
（研究者） 大塚　玲	同上	主任研究員	博士	分野融合の推進研究
（研究者） 大岩　寛	同上	研究員	博士	ソフトウェアセキュリティ
（研究者） Affeldt Reynald	同上	研究員	博士	暗号技術の形式的検証
（研究者） Nowak David	同上	研究員	博士	暗号技術の形式的検証
（研究者） Comon-Lundh Hubert	同上	招聘研究員	博士	暗号技術の形式的検証
（研究者） 古原　和邦	同上	主幹研究員	博士	暗号の計算量的安全性理論
（研究者） 萩谷　昌己	東京大学大学院理工学系研究科	教授	博士	暗号技術の形式的検証
（研究者） 川本　裕輔	Ecole Normale Superieure de Cachan	ポスドク	博士	暗号技術の形式的検証
（研究者） 岡本　龍明	NTT 情報流通プラットフォーム研究所	特別研究室長 フェロー	博士	分野融合の推進研究
（研究者） 塚田　恭章	NTT コミュニケーション科学基礎研究所	主任研究員	博士	暗号技術の形式的検証
（研究者） 櫟　粛之	NTT コミュニケーション科学基礎研究所	主任研究員	博士	暗号技術の形式的検証
（研究者） 櫻田　英樹	NTT コミュニケーション科学基礎研究所	研究主任	修士	暗号技術の形式的検証

（研究者） 真野　健	NTT コミュニケーション科学基礎研究所	主任研究員	修士	暗号技術の形式的検証
（研究者） 岡田　光弘	慶應義塾大学文学部哲学専攻	教授	博士	暗号技術の形式的検証
（研究者） 田辺　良則	東京大学大学院情報理工学系研究科	教授	博士	暗号技術の形式的検証

３．２　相手国側

氏名	所属	役職	学位	役割
（リーダー） Goubault-Larrecq, Jean	CNRS, ENS-Cachan, INRIA , Laboratoire Specification et Verification	Professor	Ph. D	Formal methods security
（研究者） S. Kremer	CNRS, ENS-Cachan, INRIA, Laboratoire Specification et Verification	Charge de recherches	Ph.D	Formal methods Security／**サブリーダー**
（研究者） B. Blanchet	CNRS, LIENS	charge de recherches	Ph. D	Formal methods security
（研究者） H. Comon-Lundh	CNRS, Ecole Normale Superieure de Cachan, LSV	professor	Ph. D	Formal methods security
（研究者） V. Cortier	CNRS, LORIA	chargee de recherches	Ph. D	Formal methods security
（研究者） C. Fournet	Microsoft Research, Saclay	researcher	Ph.D	Formal methods security
（研究者） Y. Lakhnech	CNRS, Univ. J. Fourier	professor	Ph. D	Formal methods security
（研究者） D. Pointcheval	CNRS, LIEN	Directeur de recherches	Ph.D	cryptology

４．研究成果

４．１　研究成果の自己評価

□　計画以上の成果がでた　　■　計画通りの成果がでた

□　計画とは異なるが有益な成果がでた　□　計画ほどの成果はでなかった

□　いずれでもない

４．２　研究成果の自己評価の根拠

本研究交流により、例えば以下のような研究成果が得られた。

- H. Comon-Lundh（日本側）、Veronique Cortier（フランス側）による”Computational Soundness of observational equivalence”なる論文は、2008 年の ACM Conference on Computer and Communication Security で発表された。本会議は情報セキュリティに関するトップの会議であり、その成果は本交流によって得られたものである。具体的には、本成果は、形式検証の研究者であった H. Comon-Lundh 教授が日本に滞在し、産総研のプロジェクトメンバーの暗号理論研究者との議論によってまとめられたものであり、これまでの本分野（暗号技術の安全性の形式的検証）では達成できていなかった、厳密な計算量理論的安全性の検証を実現するためのフレームワークとなる、基本的な理論成果である。
- R. Affeldt（日本側）、H. Comon-Lundh（日本側）による “Verification of Security Protocols with a Bounded Number of Sessions Based on Resolution for Rigid Variables” なる論文は、H. Comon-Lundh 教授が 2 年にわたり日本に滞在し、日本側メンバーとの共同研究で得られた成果である。現実のシステムにおけるセキュリティプロトコルの通信では、一般に同じプロトコルが複数同時に実行されているが、本論文ではそのような状況を可能な限り現実的な状況下で形式化し、その上でプロトコルの安全性を検証する方法を提案している。本成果により、個々のセキュリティプロトコル実行の安全性検証では捉えきれなかった、実際の計算機上での実行におけるプロトコルの脆弱性を見つけること、あるいは安全性を証明することが可能となった。
- R. Affeldt, D. Nowak, Kiyoshi Yamada（全員日本側）による”Certifying Assembly with Formal Security Proofs: the Case of BBS”なる論文は、2011 年に Science of Computer Programming に掲載される予定の、疑似乱数生成器のソフトウェア実装のセキュリティ検証を行った論文である。ソフトウェア実装が、情報セキュリティに関係する数学的な性質まで詳細に検証された初の論文であり、本分野においても非常に重要な成果であると言える。

今や社会のインフラとなっている情報システムは、決済等で金融機関とセキュリティ技術によって接続されるなど、非常に複雑なものとなっている。一方でシステムの脆弱性を攻撃されることにより起きたサービス停止や情報漏えい等の事故が多数報告され、大きな社会問題となっている。本交流で得られた成果により、情報システムの安全性を計算機によって保証する手法に関し、基礎的な理論整備が大きく進められたと言える。また上でも紹介したように、疑似乱数生成器といった小規模なプロトコル部品については、ソフトウェア実装の安全性証明までが可能となった。

今後さらにツール、検証ライブラリを整備することで、まずは情報システムのセキュリティ的な急所部分の安全性検証が、詳細かつ現実的な設定で可能となると考えられる。さらに研究が進むことで、情報システム全体の安全性検証法が確立できると期待される。

４．３　研究成果の補足

５．交流成果

５．１　交流成果の自己評価

□　計画以上の交流成果がでた　　■　計画通りの交流成果がでた
□　計画ほどの交流が行われなかったが成果はでた
□　計画ほど交流成果がでなかった
□　いずれでもない

５．２　交流成果の自己評価の根拠

2009 年 4 月 6 日～9 日に伊豆熱川で開催した、「暗号の計算論的・記号的安全性証明に関するスプリングスクール」では、日仏を中心に、米国や他の欧州諸国からトップの研究者を講師として招待、第一線の研究者や学生も参加し、合計 64 名の参加者を集めることができた。結果としてスプリングスクールでは、本分野の世界のトップが一堂に会することができ、本分野ではこれまでにもなかった最高レベルの研究集会となった。集会の成果については、産総研情報セキュリティ研究センターの Web ページで、発表資料や参加した日独伊の学生によってまとめられた報告書:”Computational and Symbolic Proofs of Security – a short report”が公開されている。

続いて 2010 年 4 月 12 日～16 日にフランスバルビゾンでも「Computational and Symbolic Proofs of Security (CosyProofs) 2010」でも同様のスプリングスクール＆ワークショップを開催した。前半は、フランスで以前より開催されていたスプリングスクールプログラムと共催で本分野の講習を行い、後半は、世界各国から論文募集をし査読を経た最新成果の論文発表を行った。前回から 1 年を経て研究交流が進んだ結果の発表もあり、この分野の進歩が感じられる会となった。

この交流により、日仏両研究チームの共著論文といった日仏の交流だけでなく、産総研と NTT、東大など、日本国内での交流も進めることができた。

５．３　交流成果の補足

2010 年度の活動において、4 月にフランスでワークショップ開催中にアイスランドの火山噴火が起こり、日本側研究者が帰国できなくなった。そのため予定外の出費があったため、同年度最後すなわちプロジェクト最終時に日本で開催する相談を始めていたワークショップ開催が不可能となった。研究成果としては特に増えるものではないが、やはり研究交流の締めという意味では残念な結果となってしまった。

６．主な論文発表・特許出願

論文 or 特許	・論文の場合：　著者名、タイトル、掲載誌名、巻、号、ページ、発行年 ・特許の場合：　知的財産権の種類、発明等の名称、出願国、出願日、 出願番号、出願人、発明者等	特記 事項
論文	Hubert Comon-Lundh, Veronique Cortier, Computational Soundness of observational equivalence, Proceedings ACM Computer and Communication Security (CCS'08), 2008	
論文	Reynald Affeldt, Hubert Comon-Lundh, Verification of Security Protocols with a Bounded Number of Sessions Based on Resolution for Rigid Variables. In Formal to Practical Security, Lecture Notes in Computer Science, Vol.5458, pp.1-20, 2009	
論文	Reynald Affeldt, David Nowak, Kiyoshi Yamada, Certifying Assembly with Formal Security Proofs: the Case of BBS, Science of Computer Programming, Elsevier, 2011 (to appear)	