戦略的国際科学技術協力推進事業（日本－インド研究交流）

１．研究課題名：「動的かつ階層的な暗号鍵割当方式の安全性証明と学際評価」
２．研究期間：平成２０年１２月～平成２５年３月
３．支援額：　総額　　18,850,000 円
４．主な参加研究者名：
日本側（研究代表者を含め６名までを記載）

	氏名	所属	役職
研究代表者	松浦 幹太	東京大学 生産技術研究所	准教授
研究者	細井 琢朗	東京大学 生産技術研究所	技術職員
研究者	北川 隆	東京大学 生産技術研究所	特任研究員
研究者	松田 隆宏	東京大学 生産技術研究所	博士課程学生
研究者	ジェンジャラサックル・ボンコット	東京大学 生産技術研究所	修士課程学生
研究者	市川 顕	東京大学 生産技術研究所	修士課程学生
参加研究者　のべ９名			

相手側（研究代表者を含め６名までを記載）

	氏名	所属	役職
研究代表者	Anish Mathuria	デルバニ・アンバニ情報通信研究所　情報通信技術部	教授
研究者	Manik Lal Das	デルバニ・アンバニ情報通信研究所　情報通信技術部	助教授
研究者	Naveen Kumar	デルバニ・アンバニ情報通信研究所　情報通信技術部	Research Associate（博士課程学生）
研究者	Murali Medisetty	デルバニ・アンバニ情報通信研究所　情報通信技術部	Undergraduate Project Assistant（学部学生）
研究者	Anil Kuma Mundra	デルバニ・アンバニ情報通信研究所　情報通信技術部	Junior Research Fellow（修士課程学生）
研究者	Pooja Hegde	デルバニ・アンバニ情報通信研究所　情報通信技術部	Junior Research Fellow（修士課程学生）
参加研究者　のべ７名			

５．研究・交流の目的
本研究は、暗号利用の核となる鍵割当方式に高度な利便性、安全性、社会受容性を与えることを目的とする。具体的には、日本側の安全性証明技術およびセキュリティ経済学理論とインド側の鍵割当方式技術を、それぞれ発展させた上で、組み合わせる。インド側技術で鍵割当方式を動的かつ階層的にし、利便性を高める。両国技術の連携で体系的な安全性評価を行い、安全性を高める。さらに日本側の理論で同方式の経済学的意義などを明らかにし、社会受容性を高める。
本共同研究で日印が交流を通じて相互的に取り組むことで、包括的かつ厳密な評価を伴う情報セキュリティ技術の健全な普及が期待される。

６．研究・交流の成果

６－１　研究の成果

日本側が担当した情報セキュリティ経済学では、トップコンファレンス（WEIS: Workshop on the Economics of Information Security）採択論文の発展版が掲載される編纂書籍に、本研究期間中に２件論文が掲載された。インド側と共著のジャーナル論文に貢献した学際評価では、鍵割当方式に対して脆弱性低減だけではなく脅威低減（不正抑止力としての効果）も含めた総合的な効果が重要という観点で研究を進め、有用な知見が得られた。具体的には、体系的な設計と安全性評価によって高いレベルの品質保証が実現すると、鍵割当方式を用いたアプリケーションシステムのセキュリティに投資するための最適戦略が単純になる（対象とする脆弱性に関して単調増加な投資を考えればよい）という利点があることが分かった。学際評価を含む鍵割当方式の論文は、本研究代表者の知る限り、世界初である。

日本側が担当した暗号理論（証明可能安全性）の研究では、レベルの高い成果が多数得られた。主要な成果として、公開鍵暗号の識別不可能性を破ろうとする攻撃者に許される準備・学習行為の順序や並行性等を体系化した安全性モデルを構築した。そのモデルに基づいて、CPA-to-CCA2 問題という重要な未解決問題における世界記録を達成する成果をあげ、論文が一流の国際会議に採録された。日本側の基礎研究から、同じく暗号理論分野で一流と見なされている国際会議に採択された成果が、他にも３件出ている。

６－２　人的交流の成果

本研究では、日本側の研究者（大学院学生）が多くの賞を受賞した（学内の主要な表彰２件を含めて７件)。トップコンファレンスあるいはそれに準じる国際会議での学生の発表も５件に達した。これらが、国際交流プロジェクトを体験する中から生まれたことは、国際感覚のある優れた人材の育成という意味で、将来の交流につながるといえる。また、日本側からもインド側からも、本研究に従事して卒業した後に、当該分野で競争力のある海外の主要大学や主要企業に進む学生が輩出された。より広く世界を経験することは、長い目で見ればまた巡り巡って両国の交流の発展にもつながると期待される。インド側では、日本側の影響を受けて、情報セキュリティ研究への取り組みをより多角的に行うようになりつつある。

他の２つの日印プロジェクトと合同の日印ワークショップを４回開催した。これによって、人的交流は量的に倍増した。人材育成の質の観点で、日本側インド側双方の研究者にとって、効果も倍増した。また、これらのワークショップに参加した全ての組織が、最終回のワークショップの際に行われた協議で、日印両国の暗号と情報セキュリティ分野におけるさらなる研究交流と持続的発展を考えることで合意した。さらに、当該分野への貢献として、インドで開催される主要国際会議への日本人委員の協力なども進んでいる。

７．主な論文発表・特許等（５件以内）

※相手側との共著論文についてはその旨備考欄に記載

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	備考
論文	Kanta Matsuura: "Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model ," Managing Information Risk and the Economics of Security, Springer, pp.99-119, 2009.	
論文	Takahiro Matsuda, Kanta Matsuura: Parallel Decryption Queries in Bounded Chosen Ciphertext Attacks, Lecture Notes in Computer Science, vol.6571, pp.246-264, 2011.	

論文	Takahiro Matsuda, Kanta Matsuura: On Black-Box Separations among Injective One-Way Functions, Lecture Notes in Computer Science, vol.6597, pp.597-614, 2011.	
論文	Anil Mundra, Anish Mathuria, Naveen Kumar, Takahiro Matsuda, Kanta Matsuura: Two Views on Hierarchical Key Assignment Schemes, 日本セキュリティ・マネジメント学会誌, Vol.25, No.3, pp.40-51, 2012.	共著
論文	Bongkot Jenjarrussakul, Hideyuki Tanaka, Kanta Matsuura: "Sectoral and Regional Interdependency of Japanese Firms under the Influence of Information Security Risks," Economics of Information Security and Privacy, Springer (in press)	