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：数理科学的手法による暗号アルゴリズムの設計解析とネットワークセキュリティ強化評価
２．研究期間：平成２０年１２月～平成２５年３月
３．支援額：　総額　17,281,000　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	櫻井　幸一	九州大学 大学院 システム情報科学研究院	教授
研究者	竹内　純一	九州大学 大学院 システム情報科学研究院	教授
研究者	堀　良彰	九州大学 大学院 システム情報科学研究院	准教授
研究者	西出　隆志	九州大学 大学院 システム情報科学研究院	助教
研究者	福島　和英	KDDI研究所 情報セキュリティグループ	研究員
研究者	安田　貴徳	九州先端科学技術研究所 情報セキュリティ研究室	研究員
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	Bimal ROY	インド統計研究所・応用統計課	所長
研究者	Rana BARUA	インド統計研究所・応用統計課	教授
研究者	Avishek ADHIKARI	コルコタ大学・純粋数学部門	講師
研究者	Sushmita RUJ	インド統計研究所・応用統計課	研究員
研究者	Rishiraj BHAT TACHARYA	インド統計研究所・応用統計課	研究員
参加研究者　のべ　　5　　名			

５．研究・交流の目的

暗号アルゴリズムの設計と解析、およびネットワークセキュリティでも数理解析的手法を必要とされる分野に焦点をあてた研究を行う。日本側は、暗号アルゴリズムの設計や実装をはじめとする情報セキュリティ技術で先行しており、実際のシステムのモデル化を通じて、多様な環境における最適な暗号通信方式の確立を担当する。片やインド側は、伝統的に数理統計をはじめとする理論解析の強みを生かし、日本側の設計した方式の安全性評価や、ネットワークにおける不正な攻撃者の挙動データの解析を行う。日印それぞれの強みを生かし、連携・補完する形で交流を行い、単独では得られない研究成果を得ることを目的とする。

６．研究・交流の成果

６－１　研究の成果

当初設定した主要研究サブテーマ３つ　(A)暗号アルゴリズムの解析[A1:ストリーム暗号の新構造の解析､A2:多変数多項式暗号系の安全性],(B)暗号プロトコル[鍵管理構造の解析と最適化],(C)ネットワークセキュリティ[C1.統計に基づくインシデント検出　C2.人工知能応用による情報セキュリティ技術]に関して、期待以上の成果が出た。

共同研究・共著論文作成の上で、設定したモデルにおける条件のミスをインド側研究員 Adhikari より指摘を受けて修正を行った。この論文は INTRUST という国際会議に共著論文として発表した。この共同研究は、インド側研究員の一人 Adhikari 博士が、数週間九州大学に滞在しての結果である。幸い大学のゲストハウスもキャンパスの近くにあり、論文投稿前は、ほぼ徹夜での議論でもあった。いかにインターネットが発達しても、こうした滞在交流型の共同研究でなければ、なしえなかった成果である。
また当初設定の研究サブテーマ以外でも、九大側博士学生の研究テーマに対して、インド側訪問研究員のアドバイスと討論により、共同研究が実現できた。

また、提案暗号 K2 の国際標準化を行い、KDDI 研究所は自社の携帯システムへの展開を行った。量子解読に耐えうる次世代暗号として注目されている多変数多項式暗号系は、中国･台湾･フランス､そして日本の研究グループは精力的であり､昨年度､九大数理 IMI-GOE の支援のもとで、集中ワークショップを開催した。現在も、下名の博士研究員が、国立台湾大に 3 ヶ月滞在し、共同研究を進めている。ネットワークセキュリティは、Practice という総務省 project に発展的に展開している。ここでは、ボットネットによる攻撃の予知・即応が課題であり、本研究でのアルゴリズムを実装し、評価している。

６－２　人的交流の成果

日印相互の研究者の多くは、本プロジェクトで初めてお互いの国に滞在し、共同研究やワークショップを実施するという貴重な体験の機会を得た。学術研究交流に加えて､文化交流のきっかけともなった。
また、日本側研究代表者・櫻井の研究室には、中国からの留学生も在籍しており、インド側からの研究者との交流も行えた。実際に、共同研究の成果として、共著論文を数件作成することに成功した。
インド側研究者を通じて、それまで交流のなかった、日本側研究者とも交流・共同研究が開始できた。

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	Liang Zhao,Avishek Adhikari, Di Xiao, Kouichi Sakurai, On the security analysisof an image scrambling encryption of pixel bit and its improved scheme basedon self-correlation encryption. Communications in Nonlinear Science and Numerical Simulations. Volume 17, Issue 8, pp.3303-3327. Elsevier press. August 2012,	共著
論文	Dong Hao, Avishek Adhikari, Kouichi Sakurai: Mixed-Strategy Game Based Trust Management for Clustered Wireless Sensor Networks. INTRUST 2011: 239-257	共著
論文	Liang Zhao, Takashi Nishide, Avishek Adhikari, Kyung-Hyune Rhee and Kouichi Sakurai: Cryptanalysis of Randomized Arithmetic Codes Based on Markov Model. Inscrypt'11, LNCS, Springer, 2011	共著

論文	Takashi Nishide, Shinichi Yoshinaga, Rishiraj Bhattacharyya, Mridul Nandi, Bimal Roy, and Kouichi Sakurai: New Multiple Encryption for Making Double Encryption Secure against Meet-in-the-Middle and Related-Key Attacks, WISA2011.	共著
論文	Liang Zhao, Avishek Adhikari, Kouichi Sakurai: A New Scrambling Evaluation Scheme Based on Spatial Distribution Entropy and Centroid Difference of Bit-Plane. Proc. of the IWDW 2010	共著