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：「RFID とセンサネットワーク向け暗号基礎技術とそれを用いた構成要素の設計および安全性評価」
２．研究期間：平成 21 年１月～平成 25 年３月
３．支援額：　総額 19,521,499 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	渡辺　創	（独）産業技術総合研究所	研究グループ長
研究者	古原　和邦	同上	研究グループ長
研究者	萩原　学	同上	研究員
研究者	SeongHan Shin	同上	研究員
研究者	Miodrag Mihaljevic	同上	招聘研究員
研究者	花岡　悟一郎	同上	研究グループ長
参加研究者　のべ　15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	Sugata Gangopadhyay	IIT Roorkie	准教授
研究者	Subhamoy Maitra	ISI Kolkata	教授
研究者	Goutam Kumar Paul	Jadavpur University	助手
参加研究者　のべ3名			

５．研究・交流の目的
今や様々な機器に情報セキュリティ機能が必要となり、スマートメーターなど、非常に実装が制限された状況で、その回路規模や計算コスト等を最小限とすることが求められている。本プロジェクトの主目的は、RFID (Radio Frequency Identification) やセンサネットワーク／システムといった制限された演算能力しか使えない環境における、高い情報セキュリティ機能を実現するため、日本とインドの専門家を集約することにある。本研究は、特に単純なハードウェアのみの利用や低電力消費といった要求条件おいての実現を目指している。
プロジェクトの最終目標は、このような制限された環境において用いることのできる、基礎暗号技術や汎用部品の設計、およびにその安全性の評価を行うことである。

６．研究・交流の成果
６－１　研究の成果
ストリーム暗号と呼ばれる、本課題が対象とする場面で一般に利用される暗号の安全性評価について、インド側の数学的な boolean 関数の解析技術と、日本側のストリーム暗号

安全性評価技術、暗号設計技術を融合することで、k-normality と呼ばれる性質が、安全性指標として有用なものであることを示すことができた。本研究成果は共著のジャーナルペーパーとして出版された。安全性評価指標は、今後ストリーム暗号提案時に満たすべき要件として利用されると期待できる。

また、インド側のストリーム暗号解読技術と、日本側のストリーム暗号安全性評価技術、暗号設計技術を融合することで、欧州標準ストリーム暗号候補として提案された技術を含む、複数のストリーム暗号（LILI-128, Grain-v1）の安全性が、これまで知られていたよりも低いことを示すことができた。本研究成果は共著のジャーナルペーパーとして出版された。

その他、暗号理論や符号理論を融合した、計算量やメモリ利用量が少なく、高速で動作可能な暗号技術（エンティティ認証法等）を提案することができた。提案したエンティティ認証法等の暗号技術は、スマートグリッドで使用されるスマートメーター等、制限された実装環境での利用に最適であることから、これら機器での活用が期待される。

６－２　人的交流の成果

日本研究者のインド訪問では、先方機関所属の学生とも交流を行った。本課題に留まらない我々の研究成果を紹介し、本課題に関連する学生は当然として、本課題と関係しない研究をしている学生にも刺激を与えられたと考える。

本プログラムで採択されていた関連する 3 つのプロジェクトで、日印各訪問において相互に研究者が訪問しあい、自身の課題以外の研究者とも交流することができた。それにより、別の研究を行っている研究者からの意見を得ることができ、また別課題の話を聞くことで、互いの技術を組み合わせた新たな応用についても議論することができた。

研究期間中、インド側研究者の異動や留学があり、また日本側も震災の影響があったため、当初予定の交流は日数的には達しなかった。しかしながら、電子メールその他での連絡を密に行うことで訪問の不足を補い、共著論文や交流に感化された論文発表は十分できたと考える。

インド訪問では、IIT Roorkie 学長、ISI Kolkata 所長とも面談できた。本プログラム終了後の交流についても、肯定的な反応を得ることができた。

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	Mihaljevic, Gangopadhyay, Paul and Imai, Internal State Recovery of Keystream Generator LILI-128 Based on a Novel Weakness of the Employed Boolean Function, Information Processing Letters, Volume 112, Issue 21, pp. 805–810, 2012.	
論文	Mihaljevic, Gangopadhyay, Paul and Imai, Generic Cryptographic Weakness of k-normal Boolean Functions in Certain Stream Ciphers and Cryptanalysis of Grain-128, Periodica Mathematics Hungarica, vol. 65(2), pp. 39 – 61, 2012.	
論文	Mihaljevic, Gangopadhyay, Paul and Imai, Internal State Recovery of Grain-v1 Employing Normality Order of the Filter Function, IET Information Security, vol. 6, no. 2, pp.55 – 64, 2012.	

論文	Mihaljevic, Watanabe, Imai、A Low Complexity Authentication Protocol Based on Pseudorandomness, Randomness and Homophonic Coding、Proc. of 2010 International Symposium on Information Theory and its Applications、690-695、IEEE、2010	
論文	Mihaljevic, Imai, David, Kobara, Watanabe 、On Advanced Cryptographic Techniques for Information Security of Smart Grid AMI、Proceedings of the 7th Annual Cyber Security and Information Intelligence Research Workshop、ACM、2012	