（様式４）

二国間交流事業 共同研究報告書

令和３年６月 11 日

独立行政法人日本学術振興会理事長 殿

［日本側代表者所属機関・部局］
兵庫県立大学大学院 応用情報科学研究科
［職・氏名］
准教授 五十部 孝典
［課題番号］
JPJSBP 120197735

1. 事 業 名 相手国:インド (振興会対応機関:DST)との共同研究

2. 研究課題名

（和文） ストリーム暗号に対する暗号学的安全性評価手法の開発

（英文）) Cryptanalytic study on Stream ciphers

3. 共同研究実施期間 2019 年 6 月 1 日 ～ 2021 年 5 月 31 日 (2 年 ヶ月)

4. 相手国側代表者(所属機関名・職名・氏名【全て英文】)

Indian Institutes of Technology Madras, Associate Prof. Santanu Sarkar

5. 委託費総額(返還額を除く)

本事業により執行した委託費総額		1,930,000 円
内訳	1年度目執行経費	980,000 円
	2年度目執行経費	950,000 円
	3年度目執行経費	円

6. 共同研究実施期間を通じた参加者数(代表者を含む)

日本側参加者等	6 名
相手国側参加者等	3 名

＊ 参加者リスト(様式 B1(1))に表示される合計数を転記してください(途中で不参加となった方も含め、全ての期間で参加した通算の参加者数となります)。

7. 派遣・受入実績

	派遣		受入
	相手国	第三国	
1 年度目	0	0	2(2)
2 年度目	0	0	0(0)
3 年度目	0	0	0(0)

＊ 派遣・受入実績(様式 B1(3))に表示される合計数を転記してください。

派遣:委託費を使用した日本側参加者等の相手国及び相手国以外への渡航実績(延べ人数)。

受入:相手国側参加者等の来日実績(延べ人数)。カッコ内は委託費で滞在費等を負担した内数。

8. 研究交流の概要・成果等

(1)研究交流概要(全期間を通じた研究交流の目的・実施状況)

- **研究交流の目的**

本研究交流では、共通鍵暗号技術であるストリーム暗号に関して以下の2点を研究目的とする.

(1) 強力な攻撃方法である高速相関攻撃とキューブ攻撃に対する安全性評価手法の開発

(2) 実際のストリーム暗号への(1)で開発した安全性評価手法の応用

インド側の代表者である Sarker 准教授は，ストリーム暗号の解析技術のエキスパートであり，これまで多くの解析実績がある．特に数学科のバックグラウンドがあるため，理論的解析に非常に明るい．今回のプロジェクトにおいて，特に（1）の段階では，高速相関攻撃とキューブ攻撃の手法を一般化し，評価手法を確立する際には，代数次数の正確な見積もり手法が求められる．これには，高度な代数学の知識が求められるため,Sarker 准教授の知識やスキルを用いる必要がある.一方,日本側の研究代表者は,これまで様々な共通鍵暗号の設計や解析をしてきた実績があり，ストリーム暗号の構造面からアプローチを行い評価手法の確立を目指す．具体的には，さまざまなストリーム暗号の構造と安全性の関係を明らかにし，どの構造に対しても評価できるような評価フレームワークの作成を行う．Sarker の代数評価の理論研究と組み合わせることにより，一般化が可能であると考えられる．(2)の段階では，評価手法の最適化と実際のストリーム暗号の応用を行うが，実際の解析では，計算機実験や理論値の見積もり等で様々な専門性を有した多くの人的リソースが必要であるため，インド，日本の合同チームで行うことが重要である．以上より，それぞれ独立に行っていた場合にはできない成果を得ることができる.

- **研究交流の実施状況**

2019 年度は計画通り,目的(1)のストリーム暗号に対して,新たに提案された強力な攻撃(高速相関攻撃とキューブ攻撃)の一般化を行い,安全性を厳密に評価する手法の確立を目指して研究を行った.具体的には,代数構造に基づく攻撃の一般化を行うため,さまざまな暗号アルゴリズムに対してキューブ攻撃を適用し,その効果の確認を行った.インド側の研究者の Santanu Sarkar 教授とはテレカンやメールなどで議論を進め,研究に対するフィードバックを得た.またインド側の研究者2名が 11 月に来日した際に,ストリーム暗号を含む共通鍵暗号のディスカッションを行い,その議論をもとにいくつかの追加の研究成果も得た.具体的には,ブロック暗号の設計技術，ストリーム暗号の差分解析に関しての結果を得た.これらの成果は国際論文誌に2件採択され[研究実績 1,2],国内学会でも3件の口頭発表[研究実績 3,4,5]を行った.

2020 年度は,目的(2)の研究を実施した.具体的には,昨年度行ったストリーム暗号の安全性を厳密に評価する手法を,実際のストリーム暗号 KCipher-2 に適応し，安全性厳密な評価を実施した.研究の実施方法であるが,コロナのため実際にインドへの訪問や招聘は行うことはできなかったので,テレカンやメールを中心に細目に連絡を取りながら進めた.前年度,一度直接ディスカッションが日本でできたため,ある程度背景等も共有できており,スムーズに研究を進めることができた.また,追加の研究内容として,実際のストリーム暗号アルゴリズムの新規設計も実施した.これらの成果は国際論文誌に 2 件採択され[研究実績 6, 8],国内学会でも 1 件の口頭発表[研究実績 7]を行った.国際論文誌の 1 件は Sarker 教授との共著論文である.

2021 年度は,目的 2 を継続し,ISO 標準のストリーム暗号 KCipher-2，SNOW-3G，Rasta に対する安全性解析を実施した.研究の進め方は 2020 年度に引き続き,テレカンとメールをベースに交流を進めながら実施した.これらの成果は,国際会議に 1 件採択され[研究実績 9],一件は現在国際会議に投稿中である.

(2)学術的価値(本研究交流により得られた新たな知見や概念の展開等、学術的成果)

目的(1)に対する研究

最も大きな成果としては，キューブ攻撃の新しいアルゴリズムを開発である。これは，MILP(混合線形計画法)と呼ばれる solver を利用する方法により開発を行い，結果として，Subterranean-SAE と呼ばれる軽量暗号に対して適用し，新たな安全性評価結果を得ることで有効性を確認した．結果としては，設計者は Trivial な攻撃はできないと主張していた nonce misuse と呼ばれる仮定において，Practical な攻撃が可能であることを示し(図1)，その結果は共通鍵暗号分野のトップジャーナル TOSC に採録された [研究実績 1]．またハッシュ関数 RIPEMD への適用結果も TOSC に採録され，学術的に高い評価を得た[研究実績 2].

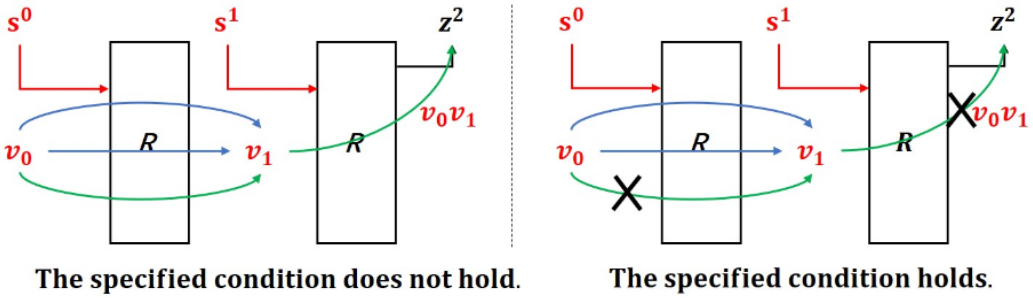

図1：Subterranean-SAE に対する攻撃

目的(2)に対して

既存のストリーム暗号の評価として，ISO 標準の KCipher-2 の安全性評価を実施した．混合整数計画法を暗号解析に用いることでより詳細な安全性評価を可能とした．技術的に難しい点は，Kcipher-2 の内部構造を，解析手法毎にうまくモデリングすることである．既存研究の効率のよりモデリング手法をうまく適応するとともに，KCipher-2 独自の Dynamic feedback 構造に対して初めて効率的なモデリング手法を考案した．その結果，

A)　Kcipher-2 が差分攻撃に対して十分な安全性評価を有していることと

B)　Integral 攻撃に対しての安全性の lower bound の見積もり

に成功した．これらは KCIpher-2 に対する初めての詳細な安全性評価結果であり，それぞれ国内会議で発表し，のちに国際ジャーナルに採録された．[研究業績 6,7,9]．これらの結果自体は，インド側との共同成果ではないが，定期的に内容のディスカッションを実施し，情報共有やディスカッションを行いながら進めた成果である．さらにこの成果を発展させて，ストリーム暗号 Rasta に対して代数的解析を Sarker 教授と実施し，脆弱性の発見に成功し，Rasta の安全性の正確な bound の導出に成功した．本研究成果は，暗号分野のトップカンファレンス ASIACRYPT へ投稿中である．

追加の結果(暗号の設計技術)

当初の目的に加え， IoT デバイスハードウェアで向けにハードウェアで軽量に実装可能な軽量暗号の設計を行った．通常ストリーム暗号は，安全性を確保するために，鍵のサイズの内部状態が必要となり，状態保持のために多くのレジスタが必要であり，軽量化は難しいと考えられてきた．このボトルネックを解消するために，我々は Double Key Filter と呼ぶ新しい構造を考案し，安全性を保ったまま内部状態を鍵長と同等程度に削減することに成功した．日本とインド側の役割分担としては，日本側が基本的な構造を考えて，インド側が安全性を評価した．安全性評価結果を受けながら，構造の改良を進めることでより安全で，効率的な構造を開発することができ

た. 結果は論文としてまとめて, 国際暗号学会の共通鍵暗号のトップジャーナルに投稿し, 無事採録された[研究業績 8]. その他, ブロック暗号に対する新しい設計手法も考案し発表した[研究業績 2,3].

(3)相手国との交流(両国の研究者が協力して学術交流することによって得られた成果)
学術交流によって, 1 件の共著論文がと共通鍵暗号分野のトップジャーナル ToSC に採択された[研究業績 8]. また, 別の1件の結果も国際会議に投稿中である. 共著論文ではないが, 学術交流でのディスカッションによっての 4 件の国際ジャーナル[研究業績 1,2,6,9], 4 件の国内発表の結果を得た[研究業績 3,4,5,7].

(4)社会的貢献(社会の基盤となる文化の継承と発展、社会生活の質の改善、現代的諸問題の克服と解決に資する等の社会的貢献はどのようにあったか)
本研究は, 情報セキュリティのコア技術であるストリーム暗号の研究である. これらの暗号技術は, IoT, Society 5.0 において基盤技術であり, ユーザのプライバシーや個人情報を保護に大きく貢献するものである. 特に本研究では, 新しく開発した安全性評価手法により, ISO 標準のストリート暗号 KCipher-2, 3/4G 標準の SNOW-3G など広く使われている暗号アルゴリズムに対して厳密な安全性評価結果を得ることができた. さらに, 既存の暗号の安全性評価のみではなく, 解析技術をベースとして新たな IoT 用のストリーム暗号技術 Atom を開発した. Atom のハードウェア規模は同じ安全性レベルを有するストリーム暗号では世界最小であり, IoT 等のハードウェア規模の小さいデバイスでも安全性を確保可能となった.

(5)若手研究者養成への貢献(若手研究者養成への取組、成果)
本研究プロジェクトでは, 6 名の若手研究者とともに実施し, 若手研究者には積極的に共同研究に参加してもらった. 定期的な打ち合わせでは, 若手研究者に最新の研究成果を発表してもらうことにより, 英語でのプレゼンテーションスキルの向上と, ディスカッションを通じた新たな知見の獲得を計った, また, 共同での論文執筆の経験や国際共同研究の進め方, スケジューリング等を身につけてもらった. 結果として, 多くの査読付き論文誌の採録に繋がり, 若手育成の観点でも大きな成果を挙げることができた.

(6)将来発展可能性(本事業を実施したことにより、今後どの様な発展の可能性が認められるか)
本研究を通じたす将来の発展としては, 本プロジェクト後も Sarker 教授との共同研究は継続していく予定である. 実際, 本プロジェクトで開発した暗号解析手法をベースに新たな暗号解析や軽量暗号の設計を行っている. また本プロジェクトを通じて, インドの暗号コミュニティとの繋がりもでき, 9 月からインドからの博士研究者2名を雇用予定であり, 益々今後インドの暗号コミュニティとの交流はより強くなることが期待できる.

(7)その他(上記(2)～(6)以外に得られた成果があれば記載してください)
特になし