様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ６ 月　 １ 日現在

機関番号：１４５０１
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ００１８４

研究課題名（和文）サイバーフィジカル/IoTで用いられる軽量暗号の危殆化に関する研究

研究課題名（英文）Reserch on Compromising of Lightweight Encryption Used in Cyberphysical/IoT

研究代表者
森井　昌克（Morii, Masakatu）

神戸大学・工学研究科・教授

研究者番号：００２２００３８

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：サイバーフィジカルシステム（CPS）およびIoT(Internet of Things)を鑑みた現状のネットワーク暗号化システムに用いられる既存の軽量暗号を含む共通鍵暗号の安全性について評価し、その実装まで踏み込み、安全なシステムの構築に対して指針を与えた。具体的な成果として、ハードウェア向きの変形Feistel構造のブロック暗号であるHIGHTのベストアタック（現時点での、その解読計算量において最良の攻撃法）を提案し、ストリーム暗号として著名なSNOW 2.0に対する新たな攻撃法を提案した。暗号の実装における研究として、無線LAN暗号WPA2の脆弱性を中間者攻撃の実現から明らかにした。

研究成果の学術的意義や社会的意義
多様化した実社会の莫大なデータとサイバー空間が緊密に結合されたサイバーフィジカルシステム(CPS)において、それらビッグデータの解析により新たな価値を生み出し、新たな知の創造やサービスへ活用が、様々な競争力の源泉となり得る。このように収集されたデジタルデータには個人の位置情報や生体情報など多くのプライバシ情報が含まれうるため、データのセキュリティ・プライバシを守りながら収集・活用する技術が緊急の課題となっている。その基盤秘術が暗号であり、安全に実装、運用する技術が期待されている。本研究はその評価を行うとともに、安全な実装方法について指針を与えるものである。

研究成果の概要（英文）：This research evaluates the security of common key cryptography including the existing lightweight cryptography used in the current network encryption system considering cyber physical system (CPS) and IoT (Internet of Things), and gives a guideline for the construction of a secure system. As a concrete result, we proposed HIGHT's best attack (the best attack at the present time in terms of the amount of decoding calculations), which is a hardware-oriented block cipher with a modified Feistel structure, and a new attack method against SNOW 2.0, which is famous as a stream cipher. As a research on the implementation of cryptography, the vulnerability of WPA2, a wireless LAN cipher, was revealed from the realization of man-in-the-middle attacks.

研究分野：情報通信工学

キーワード：サイバーフィジカルシステム　IoT　共通鍵暗号　軽量暗号　解読　安全性評価　評価基準　暗号危殆化

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

サイバー空間でのネットワーク社会が現実化している一方、実社会（フィジカル）でも生活形態だけでなく、多彩な技術の上に社会が形成され、その多様化が進んでいる。その多様化した実社会の莫大なデータとサイバー空間が緊密に結合されたサイバーフィジカルシステム(CPS)において、それらビッグデータの解析により新たな価値を生み出し、新たな知の創造やサービスへ活用が、様々な競争力の源泉となり得る。このように収集されたデジタルデータには個人の位置情報や生体情報など多くのプライバシ情報が含まれうるため、データのセキュリティ・プライバシを守りながら収集・活用する技術が緊急の課題となっている。一方、データのセキュリティ・プライバシの基盤技術である暗号に関して、センサ等リソースの限られた環境に実装可能な軽量暗号技術が注目され、開発が進められるとともに、特にセンサ等、（末端）エンティティ側の暗号化とクラウド環境下での総合的な暗号利用に伴う、その実装方法の研究開発、特に IoT に伴う軽量暗号とその実装の安全性評価が求められている。

研究代表者は 1990 年代初頭からストリーム暗号について研究を行い、特に RC4 について WEP に採用される以前からその安全性について評価を行ってきた。特に 2008 年、WEP の鍵導出法として、暗号化された 4 万パケットを観測するだけで、瞬時に鍵を導出できる方法を開発し実証を行った。さらに WEP の後継の一つの方式である WPA-TKIP でも、その脆弱性を利用し､不正なパケットを受信させる攻撃が可能であることを示し､その具体的攻撃方法を提案した。また RC4 を用いた SSL/TLS において、実際用いられる Broadcast Setting と呼ばれる同報暗号化通信の脆弱性を世界に先駆けて示し、この結果は CRYPTREC（政府暗号評価機関）での RC4 の事実上排除を決定付けるに至った。合わせて SSL/TLS においては、そのクラウドでの使用時ではキャッシュタイミング攻撃が有効であることを示し、具体的な鍵回復方法を提案し、新たな実装方法によって深刻な脆弱性が生ずることを示した。

２．研究の目的

本研究では、サバーフィジカルシステム（CPS）および IoT(Internet of Things)を鑑みた現状のネットワーク暗号化システム、さらに IoT 機器自体での認証、データ秘匿に用いられる既存の軽量暗号を含む共通鍵暗号の安全性について評価するとともに、現在、事実上インターネット上のデータ保護を目的として多用されている SSH や TSL の安全性評価を行う。次に IoT で特に利用される軽量暗号の広いクラスで適用可能な解読手法を提案し、その提案を基に新たな評価指標を開発する。軽量暗号のクラスにおいてはその評価手法の確立は十分成熟した状況とは言えない。本研究では評価手法を与えるだけでなく、現実の実装を含めた、これからの通信環境や通信プロトコルをも考慮した脆弱性の評価を与えるところに独創性がある。特に Division Property と呼ばれる暗号解読手法を拡張した新たな解読手法とともに、それを元とした安全性評価基準を策定することは独創的かつ画期的な成果となり得る。また今後期待される CPS/IoT において暗号実装における指針を与えることとなり、懸念されている CPS/IoT のプライバシ、および安全性確保の解決に寄与する意義も多大と考えられる。

３．研究の方法

CPS/IoT で利用する暗号プリミティブだけでなく、その実装プロトコルまで踏み込んだ解析を行い、解読法および通信を阻害する方法、すなわち脆弱性を与える。さらにその解析を基に暗号システムの評価基準策定を行う。本方法は研究代表者の無線 LAN や SSL/TLS の脆弱性に対する研究業績を基に、クラウド環境やハードウェア環境での暗号システムに対する最近の研究業績を踏まえて、特に Division Property と呼ばれる新たな解読手法の概念を発展させるとともに、より有効な解読手法を導出し、共通鍵暗号一般の新たな評価基準として策定、整備する。すでに研究代表者は Division Property の拡張について斬新でかつ有効な結果を与えている。また長年にわたる暗号解析の知見を利用し、ISO 等で標準化されている共通鍵暗号についても過去の評価（解読）手法をまとめるとともに、その改良を試み、危殆化について評価する。具体的には

(1)　CPS/IoT で用いられる共通鍵暗号、特に軽量暗号の評価

研究代表者は RC4 だけでなく、様々な暗号についてその解読を試み、解読手法についても数多くの提案を行っている。特に Division Property を拡張した Bit-Based Division Property を開発し、軽量暗号への適用を試みている。これをさらに推し進めて様々な共通鍵暗号、特にストリーム暗号への適用方法を与える。また合わせて、この Division Property を含めて現在までに提案されている解読手法の整理を行い、特に幾つかの解読方法を見直すとともに、その実装や計算アルゴリズムにおいて最新の技術を導入し、現状におけるその事実上の解読限界を与える。

(2)　現状のネットワーク暗号化の安全性評価、その問題点の指摘

研究代表者はかつて RC4 を用いた SSL/TLS において、実際用いられる Broadcast Setting と呼ばれる同報暗号化通信の脆弱性を世界に先駆けて示した。本研究項目ではこの研究で積み重ねた TLS をはじめ各種のネットワーク暗号化における運用の知見により、現在、ファイル暗号化方

式として一般に利用されている幾つかの方式を対象にその脆弱性を明らかにする。

４．研究成果

主たる成果として、共通鍵暗号として電子政府推奨候補暗号の一つである Enocoro-128v2 に対して Cube 攻撃を適用し、その安全性の評価を行い、最良の解読法を与える。さらに WPA2/WPA3 無線 LAN 機器に対する脆弱性を指摘し、安全な運用法を与える。

(1) Enocoro-128v2 の Cube 攻撃に対する安全性評価

インターネットが広く普及した現在、通信の安全性を確保するための暗号技術はさらに重要度を増している。 その一方で、暗号アルゴリズムの安全性は計算機能力の向上や暗号解読手法の進歩にともなって次第に低下していく。このような暗号危殆化に対して、適切な対策を講じていくことは非常に重要な課題である。総務省及び経済産業省は、暗号危殆化対策の一環として、暗号技術検討会及び関連委員会（CRYPTREC）の活動を通して電子政府で利用される暗号技術の評価を行っており、2013 年に「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」を策定した。Enocoro-128v2 とは、この暗号リストの中で推奨候補暗号として名前が挙げられたストリーム暗号であり、国際規格 ISO/IEC29192-3 でも標準化されている。最適化問題において、目的関数と制約条件が線形関数で記述でき、各要素が整数に限定される問題を整数計画問題という。この解法アルゴリズムが整数計画法である。2011 年 Mouha らは Enocoro-128v2 の Active S-box 解析に整数計画法を利用する方法を提案した。それ以降、既存の暗号解読技術に整数計画法を適用する研究が進められてきた。2016 年には Xiang らによって Division Property を用いた Integral 攻撃に整数計画法が適用され、2017 年には藤堂らによって Cube 攻撃にも適用された。最新の研究では、この整数計画法を利用した Cube 攻撃によって、Trivium、Kreyvium、Grain-128aAcorn といったストリーム暗号の解読段数が更新されている。

本研究では、上記の手法でまだ評価がなされていない Enocoro-128v2 を対象とする。攻撃シナリオとして、鍵に依存しない特性を導出する識別攻撃と鍵そのものを導出する鍵回復攻撃の 2 種類を考える。また、攻撃者は初期化ベクトル（Initialization Vector）を自由に操作し、 対応するキーストリームを取得できる選択 IV 攻撃が可能であるものとする。まず、Enocoro-128v2 の構造に対して Division Property の伝搬ルールを適用し、それを整数計画モデルに置き換える。そして選択 IV 攻撃によって入出力の条件を付加した上で、整数計画ソルバーで解く。さらに入出力条件を変更することにより、攻撃可能な解読段数の最大値を探索する。その結果、鍵に依存しない識別攻撃では、21 段までは非乱数性を確認できたが、これは既存の安全性評価によって示された結果と同じだった。一方、鍵回復攻撃では、計算量 2120、28 選択 IV の 11 段鍵回復攻撃を発見した。これは既存研究では示されておらず、Enocoro-128v2 に対する Cube 攻撃の最良解析結果と言える。しかしながら、初期化フェーズとして用意されている 96 段と比べると明らかに少ない。従っ て、現時点において Enocoro-128v2 は Cube 攻撃に対し て十分な耐性を持つと言える。

(2) WPA2/WPA3 無線 LAN 機器に対する脆弱性とその対策

ホテルやカフェなどの商業施設、図書館や空港といった公共施設などで、無線 LAN を利用する機会が増えている。データの送受信に電波を使用する無線 LAN は盗聴が容易であり、安全なデータのやり取りには通信の暗号化が必要不可欠である。現在、無線 LAN のセキュリティプロトコル（暗号化方式）として広く使用されているのが WPA2 である。しかし WPA2 には脆弱性が発見されており、2018 年に WPA3 と呼ばれる新たなセキュリティプロトコルが発表された。2019 年に Vanhoef らによって WPA3 に対する攻撃である Dragonblood が提案された。Dragonblood は WPA3 の実装における脆弱性を利用した攻撃であり、サイドチャネル攻撃、ダウングレード攻撃および DoS 攻撃が提案されている。Dragonblood は WPA3 を利用しているクライアントに対してのみ攻撃可能であり、その実行難易度の高さと条件の厳しさから大きな影響は出ていない。しかし、今後も脆弱性が見つかる可能性は高く、 攻撃者が脆弱性を悪用する前に WPA3 だけではなく無線 LAN の各仕様についてその安全性を評価することが求められる。 我々は以前 CSA（Channel Switch Announcement）と 呼ばれる信号を利用した Dragonblood と異なるアプローチでの DoS 攻撃を提案した。CSA はアクセスポイントがチャネル（周波数）を切り替える際にクライアントに送信する信号である。この CSA を挿入した改ざんビーコンを送信し続けることでクライアントの通信を切断することに成功した。提案攻撃は Dragonblood に比較して、実現が容易であり、かつ広範囲に適用可能であるため深刻な攻撃であった。 本研究ではこの攻撃について詳細な検証実験を行い、クライアントの挙動について調査する。さらに実験の結果から、一部のクライアントに対してアクセスポイントと 接続したまま通信不可能にする攻撃や、通信速度を著しく低下させる攻撃を提案する。また攻撃対象を指定して DoS 攻撃を行う方法についても提案する。

結果として我々が以前提案したクライアントのチャネルを切り替えさせる信号である CSA を利用した DoS 攻撃についてより詳細な検証実験を行い、クライアントごとの挙動についても調査

し、その実験の結果から、一部の端末では CSA が無効となっており攻撃に失敗したものの、多くの端末で継続的な DoS 状態にすることに成功した。さらに最新のセキュリティプロトコルである WPA3 でも攻撃に成功したため、セキュリティプロトコルによらず攻撃は成功すると考えられる。攻撃者は攻撃対象のアク セスポイントのビーコンを受信できれば攻撃可能であるため、本攻撃は従来の無線 LAN に対する DoS 攻撃と比べても非常に有効的なものである。また、提案攻撃を改良し、攻撃者自身もチャネルを切り替えつつビーコンを送信し続ける方法を提案した。この手法では一部クライアントに対してアクセスポイントに接続させたまま、通信不可能にし、通信速度を著しく低下させることに成功した。従来の DoS 攻撃ではアクセスポイントと切断されてしまうため、被害者は異常に気付きやすく、モバイル機器であればアクセスポイントと切断されることで 携帯回線での通信が可能となるなど、いくつかの欠点があった。改良した手法ではアクセスポイントと接続したままであるためこれらの欠点がなく、一部のクライアントに対してより深刻な影響を与えることが可能となる。 最後にビーコンの宛先アドレスに攻撃対象となるクライアントの MAC アドレスを書き込むことで攻撃対象を指定する手法を提案した。実証実験の結果、Android スマートフォン以外では攻撃対象を絞った攻撃に成功した。 Android スマートフォンでは実装のバグにより宛先アドレスによらずビーコンを受け取ってしまうため攻撃対象を絞ることはできなかった。これらの結果から、我々が提案した攻撃は無線 LAN を利用する多くのクライアントに対して有効であるといえる。攻撃者は一部の端末を 除き攻撃対象を絞ったうえで通信速度の低下や通信の切断といった攻撃が可能となる。さらに、一部の端末ではアクセスポイントに接続したままで被害者に切断を気づかせることなく通信不可能にさせることも可能である。DoS 攻撃はパスワードを特定し、通信を復号するような攻撃に比べると影響が小さく軽視されがちである。しかし、DoS 攻撃によって通信を妨害しつつ Evil Twin 攻撃に繋げるなど他の攻撃と組み合わせることで 通信データの流出など大きな被害が出る可能性は常に存在する。また、本研究で提案した方法によって特定のクライアントのみ通信ができないようにさせることも可能であり、以前の提案手法に比べてより大きな被害が出ることも考えられる。したがって CSA の実装について今一度確認し、実装レベルで確実に対策していくことが求められる。

５．主な発表論文等

〔雑誌論文〕　計6件（うち査読付論文　6件／うち国際共著　1件／うちオープンアクセス　0件）

１．著者名 TAKITA Makoto、HIROTOMO Masanori、MORII Masakatu	４．巻 E101.A
２．論文標題 Coded Caching for Hierarchical Networks with a Different Number of Layers	５．発行年 2018年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 2037～2046
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E101.A.2037	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 WATANABE Yuhei、ISOBE Takanori、MORII Masakatu	４．巻 E101.A
２．論文標題 Cryptanalysis of Reduced Kreyvium	５．発行年 2018年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1548～1556
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E101.A.1548	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Subhadeep BANIK, Takanori ISOBE, Masakatu MORII	４．巻 EA100-A
２．論文標題 Analysis and Improvements of the Full Spritz Stream Cipher	５．発行年 2017年
３．雑誌名 IEICE Trans. Fundamentals	６．最初と最後の頁 1296-1305
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 FUNABIKI Yuki、TODO Yosuke、ISOBE Takanori、MORII Masakatu	４．巻 E102.A
２．論文標題 Improved Integral Attack on HIGHT	５．発行年 2019年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1259～1271
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1587/transfun.E102.A.1259	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Takada Masaru、Osada Yuki、Morii Masakatu	４．巻 1
２．論文標題 Counter Attack Against the Bus-Off Attack on CAN	５．発行年 2019年
３．雑誌名 2019 14th Asia Joint Conference on Information Security (AsiaJCIS)	６．最初と最後の頁 1～8
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/AsiaJCIS.2019.00004	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 瀧田 愼、大熊 浩也、森井 昌克	４．巻 J103-D
２．論文標題 二つの情報を出力するQRコードの構成―悪性サイトに誘導するQRコードの存在とその脅威―	５．発行年 2020年
３．雑誌名 電子情報通信学会論文誌D 情報・システム	６．最初と最後の頁 291～300
掲載論文のDOI（デジタルオブジェクト識別子） 10.14923/transinfj.2019JDT0003	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計18件（うち招待講演　0件／うち国際学会　6件）

１．発表者名 高田将，森井昌克
２．発表標題 ナップザックタイプ暗号に対する解読法の提案 ～ 部分和判定問題に基づくナップザック暗号の解読 ～
３．学会等名 電子情報通信学会　情報通信システムセキュリティ研究会　技術研究報告
４．発表年 2018年

１．発表者名 船引悠生，藤堂洋介，五十部孝典，森井昌克
２．発表標題 Enocoro-128v2のCube攻撃に対する安全性評価
３．学会等名 2019年暗号と情報セキュリティシンポジウム
４．発表年 2019年

１．発表者名
小家 武，五十部 孝典，藤堂 洋介，森井 昌克

２．発表標題
Type-1.x 一般化Feistel構造におけるブロックシャッフルの評価

３．学会等名
2019年暗号と情報セキュリティシンポジウム

４．発表年
2019年

１．発表者名
長濱 拓季，藤堂 洋介，草川 恵太，森井 昌克

２．発表標題
GLP署名の故障利用攻撃に対する安全性評価

３．学会等名
2019年暗号と情報セキュリティシンポジウム

４．発表年
2019年

１．発表者名
Makoto Takita, Masanori Hirotomo, Masakatu Morii

２．発表標題
Coded Caching in Multi-Rate Wireless Network

３．学会等名
2018 IEEE International Conference on Communications Workshops（国際学会）

４．発表年
2018年

１．発表者名
Y. Funabiki, Y. Todo, T. Isobe M. Morii

２．発表標題
Several MILP-Aided Attacks against SNOW 2.0

３．学会等名
The Seventeenth International Conference on Cryptology And Network Security（国際学会）

４．発表年
2018年

１．発表者名
M. Takita, H.Okuma, M. Morii

２．発表標題
A Construction of Fake QR Codes Based on Error-Correcting Codes

３．学会等名
The Sixth International Symposium on Computing and Networking（国際学会）

４．発表年
2018年

１．発表者名
窪田恵人，小家武，船引悠生，藤堂洋介，五十部孝典，森井昌克

２．発表標題
実環境を想定したWPA2に対するKRACKsの評価実験

３．学会等名
2018コンピュータセキュリティシンポジウム

４．発表年
2018年

１．発表者名
壇 慶人，瀧田 愼，仲野 有登，清本 晋作，森井 昌克

２．発表標題
LoRaWANに対するDoS攻撃の提案と対策

３．学会等名
2019年暗号と情報セキュリティシンポジウム

４．発表年
2019年

１．発表者名
Yuki Funabiki, Yosuke Todo, Takanori Isobe, Masakatu Morii

２．発表標題
Improved Integral Attack on HIGHT

３．学会等名
22nd Australasian Conference on Information Security and Privacy(ACISP2017)（国際学会）

４．発表年
2017年

１．発表者名
Yuhei Watanabe, Takanori Isobe, Masakatu Morii

２．発表標題
Conditional Differential Cryptanalysis for Kreyvium

３．学会等名
22nd Australasian Conference on Information Security and Privacy(ACISP2017)（国際学会）

４．発表年
2017年

１．発表者名
akeru Koie, Takanori Isobe, Yosuke Todo, Masakatu Morii

２．発表標題
Low-Data Complexity Attacks on Camellia

３．学会等名
Applications and Technologies in Information Security (ATIS2017)（国際学会）

４．発表年
2017年

１．発表者名
小家 武、五十部 孝典、藤堂 洋介、森井昌克

２．発表標題
一般化Feistel構造における最適なブロックシャッフルの評価

３．学会等名
2018年　暗号と情報セキュリティシンポジウム（SCIS2018）

４．発表年
2018年

１．発表者名
北川 理太、船引 悠生、藤堂 洋介、五十部 孝典、森井 昌克

２．発表標題
整数計画法を用いたXOR-SNOW 2.0に対する差分特性探索

３．学会等名
2018年　暗号と情報セキュリティシンポジウム（SCIS2018）

４．発表年
2018年

１．発表者名
船引 悠生、藤堂 洋介、五十部 孝典、森井 昌克

２．発表標題
SNOW 2.0に対する新たな線形近似探索手法と高速相関攻撃への応用

３．学会等名
2018年　暗号と情報セキュリティシンポジウム（SCIS2018）

４．発表年
2018年

１．発表者名
長濱 拓季、船引 悠生、藤堂 洋介、草川 恵太、森井 昌克

２．発表標題
整数計画法を用いた平文回復攻撃による二値行列LWE暗号の安全性評価

３．学会等名
2018年　暗号と情報セキュリティシンポジウム（SCIS2018）

４．発表年
2018年

１．発表者名
窪田 恵人,五十部 孝典,森井 昌克

２．発表標題
無線LAN機器に対するDoS攻撃の実装と評価

３．学会等名
コンピュータセキュリティシンポジウム2019

４．発表年
2019年

１．発表者名
森井昌克

２．発表標題
私見：情報理論からサイバーセキュリティへ

３．学会等名
電子情報通信学会研究報告情報セキュリティ（ISEC）（招待講演）

４．発表年
2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考