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

平成　２９　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：　2014～2016
課題番号：　２６３３０１５５

研究課題名（和文）サイバーフィジカルで用いられる軽量暗号の評価と実装に関する研究

研究課題名（英文）On the analysis and implementation of light weight cryptography in cyber phisical system

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）　　3,700,000円

研究成果の概要（和文）：我々が世界で初めて開発した現実的な計算量で解けるRC4の平文回復攻撃を拡張し，さらに効率よく平文を回復する方法を提案した．これはSSL/TLSの安全性評価につながっている．さらにSSL/TLSでの実装方式として使われるOpenSSLにおいてのキャッシュタイミングアタックについて考察し，特にクラウド環境での利用における脆弱性の存在を与えた．次に量子コンピュータに耐性のある公開鍵暗号として期待されている高密度ナップザック暗号について評価し，効率的な暗号解読手法を提案した．また本研究の中心テーマである軽量暗号の評価として，CAESARプロジェクトへの提案を含むいくつかの暗号方式の安全性評価を行った．

研究成果の概要（英文）：First, we propose a new full plaintext recovery attack. Our proposed attack can recover all plaintext bytes from 233 ciphertexts. Secondly, we propose the interaction between processes running on the different VMs as an alternative means of getting accurate clock cycles. We also cover POODLE attack. It's a kind of Man-in-the-middle attack against SSLv3.0, allowing to extract secure HTTP cookies. We prove the feasibility of this attack with a practical experiment. Thirdly, we propose an attack on high-density knapsack cryptosystem. This attack uses pseudo intermediary plaintext that is not the solution for subset sum problem. We remark about the knapsack cryptosystem the attack is effective. Finally, we propose a new method to find conditional differential characteristics on NLFSR-based stream ciphers. We apply our technique to Grain v1. We show the conditional differential distinguisher on Grain v1 up to 114 rounds and have 240 weak keys.

研究分野：　工学

キーワード：　共通鍵暗号　軽量暗号　サイバーフィジカル　IoT　ネットワークセキュリティ　解読　安全性評価　公開鍵暗号

１．研究開始当初の背景

IT（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 IT 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と考えられている．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と特にその安全性評価が求められている．

２．研究の目的

本研究では，まず CPS を鑑みた現状のネットワーク暗号化システムである SSH や SSL/TLS の安全性について評価するとともに, CPS でも多用化される無線通信システムでの暗号化について，特にその安全性について評価し，現実的な改善策，および安全性確保のために指針を与える．また今後提案される次世代暗号についても評価を行う。具体的には次の通りである．

(1) 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

サーバ・ブラウザ間暗号通信の標準プロトコルである SSL/TLS は現在，もっとも利用されているインターネット暗号化通信システムと言っても過言ではなく, SSL/TLS に基づいたセキュリティシステムは数多く存在し，実際に稼働している．しかしながら最近になって, BEAST あるいは Lucky Thirteen と呼ばれる攻撃，すなわち SSL/TLS にとっての脆弱性が指摘されている．この脆弱性を回避する方法として, RC4 と呼ばれるストリーム暗号を利用する方式が推奨された．研究代表者はこの RC4 を利用した SSL/TLS においてさえ，世界に先駆けて脆弱性を指摘し，実際に暗号を解読，すなわち暗号文を平文に戻す方法を提案した．本研究項目では脆弱性があるものの，暫定的な処置等がとられ，実際に利用され続けている SSL/TLS についてその安全性評価を行う．

(2) CPS で用いられる高速軽量暗号の評価（無線 LAN プロトコルからの展望）

CPS においては各種センサを有機的に接続することから，その活用はネットワークに依存する．特に無線による接続がその中心となり得る．研究代表者は無線 LAN 暗号システムである WEP および WPA-TKIP の脆弱性については多大な業績を残している。これらの業績に基づき，無線 LAN プロトコルだけでなく，RFID 等を含む近距離無線通信システムでの暗号化についてその評価を行うとともに，その安全性を確保するための指針を与える．

(3) CAESAR プロジェクトで応募される暗号の評価

2013 年から CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness の開催され，2014 年 1 月に候補暗号の提案締切が設定されている．本項目ではこの CAESAR に提案される Authenticated Encryption と呼ばれる暗号モードおよび方式の評価，ならびにそれに用いられる暗号プリミティブの評価を行い，暗号の国際標準化等に貢献する．

３．研究の方法

SSL/TLS 全般の脆弱性について，特に利用する暗号プリミティブの脆弱性だけでなく，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を与える．本方法は研究代表者が 2013 年に提案した SSL/TLS の平文解読方法の原理を従来の攻撃法との関連で拡張することによって行う．さらに CPS を鑑みた高速軽量暗号を、その無線通信システムでの実装を含めて解析し、安全性評価を行う。以下，具体的に研究項目毎に説明する．

(1) 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 RC4 を用いた SSL/TLS の脆弱性を指摘し, Broadcast Setting での環境下で，実際に暗号文を平文に復号出来得ることを示した．さらにその改良を行い，より少ない平文量で，かつ信頼性高く確実に復号でき得るように改良を行った．これをさらに押し進め，SSL/TLS の実際のプロトコルおよびデータ（パケット）構造を利用することによって，さらに少ない平文量および計算量で精度を高くして復号出来る方法を開発する．また，既存の BEAST や Lucky Thirteen 等との攻撃手法（脆弱性）の関係を明確にする．そして RC4 を利用した SSL/TLS の解読法の改良を進めると同時に，SSL/TLS 全般について，その脆弱性評価を行い，通信システムとしての運用を阻害する脆弱性を含めて議論し，その具体的事例を示すとともに，その現実的可能性を指摘する．特に最終年度ではその脆弱性が起こりえる必要十分条件を示すとともに，回避手法や改良法についてまとめる．

(2) CPS で用いられる高速軽量暗号の評価（無線 LAN プロトコルからの展望）

すでに研究代表者らは WEP および WPA-TKIP 等の脆弱性を指摘するだけでなく，RAKAPOSHI 等, 軽量暗号の解析も進めている．平成 26 年度は，さらなる WPA-TKIP の脆弱性および WPA2 等の脆弱性を評価するとともに，

その上での認証を含めた暗号プロトコルの脆弱性について検証する．また WEP や WPA-TKIP を利用する場合の安全性の正確な評価と，一定の安全性を得るための現実的改良方法を与える．さらに実際に利用されている RFID 等の暗号システムの安全性について評価する．さらに脆弱性を中心としたその問題点を克服する方法，特に暗号システムの適用，運用方法を与えるとともに，具体的な軽量暗号の適用による CPS でのモデル化を行い，実装も交えての安全性評価を行う．

(3) CAESAR プロジェクトで応募される暗号の評価

AES（プロジェクト）や e-STREAM，あるいは SHA-3 以上に CAESAR プロジェクトでは暗号プリミティブが提案されると予想される．平成 26 年度では応募された暗号プリミティブおよびその利用モードについて整理検討するとともに，研究代表者らの RAKAPOSHI 等，軽量暗号の解析を踏まえて、提案者らの評価符が妥当か否か，評価実験を含めて検証する．さらに具体的な脆弱性を指摘するとともに，特に暗号プリミティブに関してはその解読法の提案を試みる．

４．研究成果

研究の方法で述べた研究項目毎にまとめる．なお、先の研究方法での研究項目（２）と（３）は，同じ軽量暗号の評価となることから項目（２）でまとめて報告する．

(1)　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

①RC4 に対する平文回復攻撃の改良

Broadcast Setting の RC4 における最初の平文回復攻撃は FSE 2001 で Mantin らによって提案された．この攻撃は，RC4 から生成される擬似乱数列(キーストリーム)の 2 バイト目に偏り（bias）があることを利用し，異なる鍵で暗号化された 256 個以上の暗号文から平文の 2 バイト目をランダム探索より高確率で復元する．その後，FSE 2011 では Maitra らによって攻撃対象を平文の先頭の 2～255 バイト目まで拡張できることが示され，FSE2013 では五十部らによって全ての平文バイトを攻撃対象とできる攻撃法が提案された．五十部らの攻撃では，RC4 のキーストリームの初期のバイトにだけ生じる bias (short-term bias) とキーストリームの任意の位置のバイトで生じる bias(long-term bias) を組み合わせて使っており，その long-term bias は知られている中で最も強力な ABSABbias を用いている．五十部らの攻撃は，2^{32} 個の暗号文から平文の先頭 257 バイトの各バイトをそれぞれ確率 0.8 以上で復元でき，2^{34} 個の暗号文から平文の先頭 1000 テラバイト全体を確率 0.97 程度で復元できる．USENIX Security 2013 で AlFardan らは bias の利用方法を改善した平文回復攻撃を提案した．AlFardan らの一つ目の攻撃では shortterm bias についてキーストリームの各バイトで複数の bias を有効に扱えるようにする．具体的には，平文復元アルゴリズム中のカウントアップ手法に対してキーストリームの出力の生起確率を使った重み付けを施している．この攻撃は，2^32 個の暗号文から平文の先頭 256 バイトの各バイトを確率 0.96 以上で復元できる．また AlFardan らは，FSE2000 で Fluhrer と McGrew によって発見された long-term bias (FM00 bias)を利用し，short-term bias の場合と似たカウントアップ手法によって平文を復元する攻撃も提案している．ただし，この AlFardan らの二つ目の攻撃は特殊な条件を満たす平文への攻撃であり，五十部らの攻撃とは直接比較することはできない．しかしながら，平文バイトを復元できる確率が概ね１になるための暗号文のデータサイズが Broadcast Setting で言えば 2^{34} 個の程度の暗号文に相当するため，五十部らの攻撃と近い能力を有していると思われる．さらに AlFardan らの二つ目の攻撃に含まれるカウントアップ手法や FM00 bias は五十部らの攻撃で使っている技術とは独立しており，これらを併用すれば平文回復攻撃の成功確率を向上させられると考えられる．五十部らの攻撃で成功確率が概ね 1 になる暗号文数である 2^{34} という数は，現実の環境で影響が生じるかどうかのボーダーライン周辺にあると考えられる．そのため，従来の手法の組み合わせによってその値がどれだけ減少するかを明らかにすることは，RC4 を継続使用した場合に 258 バイト目以降の平文情報が実際に漏洩するかを考える上での重要な判断材料となる．そこで，本研究では，まず初めに五十部らの攻撃の ABSAB bias を用いたアルゴリズムを AlFardan らの攻撃のようなカウントアップ手法を利用できるように変形する．次に，FM00 bias にも同様のカウントアップ手法を適用した上で ABSAB bias と併用するように改良した平文回復攻撃を提案する．さらに計算機実験により，Broadcast Setting において提案手法は 2^33 個の暗号文から平文バイトを概ね確率１で復元でき，五十部らの攻撃の半数まで必要な暗号文数を削減できていることを明らかにした．

②OpenSSL キャッシュタイミング攻撃の実現性について

Bernstein は 2005 年に暗号化に AES を用いた場合，キャッシュによる時間差を利用し，鍵を取得するキャッシュタイミング攻撃を提案した．2011 年には SSLv3.0 および TLSv1.0 に対する攻撃として BEAST(Browser Exploit Against SSL/TLS)が提案された 2012 年の CRIME(Compression Ratio Info-leak Made Easy/Compression Ratio Info-leak Mass Exploitation)，2013 年の BREACH(Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext)はともに SSL/TLS のデータ圧縮機能を利用した攻撃として報告された．2013 年には MAC の計算速度の違いを利用した Lucky13 が提案された．

2014 年に発表された POODLE(Padding Oracle On Downgraded Legacy Encryption) は，SSLv3.0 のプロトコル上の欠陥を利用した攻撃である．SSL/TLS においてブロック暗号を用いて暗号化を行うとき，平文のサイズをブロック長の倍数にあわせるためにパディングという処理を行う．SSLv3.0 の仕様では，パディングしたバイトの中身は確認しない．SSLv3.0 は TLS 以前に開発されたプロトコルであるが，互換性を維持するために数多くの機器でサポートが続いている．攻撃者はこの状況を悪用し通信を改竄することで，SSLv3.0 を用いた通信を強制することができる．またブロック暗号の特性によりブロックの境界線を移動させて，攻撃を効率よく行えるようにする．結果として攻撃者は暗号化された HTTP リクエストを復号することができる．POODLE はプロトコルの仕様そのものを利用した攻撃であり，SSLv3.0 においては現実的な対抗策は無いと言われている．本研究ではこれらの攻撃のうち，Bernstein のキャッシュタイミング攻撃のクラウド環境下での実現性について検証した．クラウド環境とはソフトウェアやハードウェア資源をネットワークを通じて利用可能な環境の事であり，コストや保守管理の点で優れているため，企業などで導入が進んでいる．このクラウド環境を支える仮想化技術は，一台の PC 内に複数の VM を動作させて処理を行っている，この特性を利用し Bernstein の攻撃がより現実的に実行できることを示した．

③高密度ナップザック暗号に対する攻撃

高密度ナップザック暗号は低密度攻撃に耐性を持つ一方，複雑な構成をとるため，低密度なナップザック暗号とは異なる脆弱性を抱える可能性がある．これは密度 1 を基準として高密度な暗号では部分和問題の解が複数生じるためである．低密度な暗号では平文を部分和問題の解とすることが一般的だが，高密度な暗号では平文の衝突が生じるためこのような構造をとることができない．そのため，高密度な暗号を実現するために何らかの前処理が必要となる．そのような前処理の一つに平文を中間平文に写像することが挙げられる．この写像は拡大写像と捉えることができ，中間平文を部分和問題の解とすることで高密度ナップザック暗号を実現することができる．中間平文を用いる暗号システムは，平文から一意に中間平文を導出される場合と，平文から複数の中間平文が導出される場合の二種類に分類できる．筆者らはこれら二種類の中間平文を用いて構成されるナップザック暗号に対する攻撃をそれぞれ提案した．中間平文が一意に決定される場合は平文の一部を推定することで中間平文を多量に決定し，元の平文を導出することができる．また，中間平文が複数存在する場合は中間平分偽造攻撃が有効である．中間平文偽造攻撃は正規の中間平文と同様の働きをすることができる擬似中間平文を用いて平文を解読する．擬似中間平文は部分和問題よりも容易な問題である整数部分和問題の解を求めることで導出することができる．本研究では中間平文偽造攻撃に耐性を持つ暗号システムについて考察することで，中間平文偽造攻撃がどのような構造を持つナップザック暗号に対して有効であるのかを示した．中間平文が複数存在する場合でも擬似中間平文が満たすべき条件により擬似中間平文を生成できる確率を低くすることができる可能性があることを示し，中間平文偽造攻撃に対して耐性を持つために中間平文を導出するアルゴリズムが満たすべき条件を示した．

(2) CPS で用いられる高速軽量暗号の評価(無線 LAN プロトコルからの展望)

①ブロック暗号構造に対する汎用解析手法の提案と Kuznyechik の解析

Eurocrypt2001 で Biryukov と Shamir は SASAS 構造に対する汎用解析手法を提案しており，これは 2.5 段 SPN 構造に対する汎用解析手法と考えられる．また S-box の入出力ビット長やブロック長を制限することにより SASAS 解析は近年改良されている．本稿では，現実的な構造を用いたブロック暗号に注目し，その汎用解析手法を提案する．SASAS 解析では SPN 構造の非線形関数および線形関数の全てが攻撃者にとって秘密であることが想定されている．しかしながら，多くの現実的な暗号は秘密のラウンド鍵の排他的論理和と公開情報である非線形関数と線形関数から構成される．本研究では，そのような構造を持つブロック暗号に対する汎用解析手法を考える．ここで解析技術として，Eurocrypt2015 で提案された Division Property の伝搬および CANS2014 で提案された FFT 鍵回復技術を併用する．本研究で示す手法は汎用解析手法でありながらロシアの国家標準規格で標準化されている 256 ビット鍵 128 ビットブロック暗号 Kuznyechik の最良攻撃手法になる．Kuznyechik の既存最良解析手法は信学会論文誌で提案されており，5 段までが中間一致攻撃を用いることで解析されている．一方で，本稿で示す汎用解析手法は 6 段の Kuznyechik を解析することが可能となる．

②NLFSR 型ストリーム暗号に対する条件付差分特性の解析

Grainv1 は eSTREAM においてハードウェア暗号の一つに選択されている．Grain v1 に対する様々な解析が行われてきた．Preneel らは AFRICACRYPT2008 において関連鍵攻撃を提案した．Lee, Jeong, Sung, Hong は関連鍵の脆弱性を用いて鍵回復攻撃を示した．しかし，この攻撃は 80 ビットのキーストリームが必要である．Asiacrypt2010 において，条件付差分解読法と呼ばれる新しい攻撃手法が Knellwolf, Meier, Naya-Plasencia により提案された．条件付差分解読法では初めに鍵の初期化処理における差分の拡散を解析し，条件付差分特性を得る．得られた特性を用いて識別攻撃を構成する．彼らは NLFSR 型の暗号

である KATAN, Grain v1, Grain-128 に攻撃を適用した．彼らは Grain v1 について 2^27 個の選択 IV を用いた 97 段と 2^{35} 個の選択 IV を用いた 104 段の識別攻撃を示した．2014 年に Banik は同様の手法を用いて 105 段の識別攻撃を示した．この攻撃は Sarkar によって改良され，106 段の識別攻撃が示された．この攻撃は 2^{23} 個の選択 IV で成立するが，IV の自由に変更できる範囲を全て利用している．本研究では条件付差分特性を探索する新しい手法を提案する．一般的に NLFSR 型ストリーム暗号は鍵の初期化処理の巻き戻しが可能である．既存の手法では順方向の鍵初期化処理のみを解析し，1 ビットの差分が IV に入力された場合の条件付差分特性を探索している．本研究では，より効果的な条件付差分特性を取得する手法を提案した．鍵初期化処理を二つに分割し，順方向と逆方向の両方における差分の拡散を利用する．ある 1 ビットの差分が存在する状態を中間状態と仮定する．順方向の解析において，中間状態とキーストリームとの間の差分特性を得る．逆方向の解析において中間状態と初期の状態との間の条件付差分特性を構成する．結果として，IV に複数ビットの差分が存在する場合の条件付差分特性を得ることができる．提案手法を Grain v1 に適用し，条件付差分特性を得る．結果として Grain v1 において 2^{30} 個の選択 IV から 107 段の識別攻撃が得られる．107 段の識別攻撃に利用するキーストリームの差分の偏りについて理論的な確認を行った．また実験的にも提案する識別攻撃の有効性を確認した．

③Integral Attack に対する SPECK32 の安全性評価

SIMON と SPECK は 2013 年に NSA が提案した軽量ブロック暗号である．これらの仕様書には安全性評価に関する記述が無いため，これらの暗号を利用する前に安全性評価が必要である．SIMON に対して線型解読法，差分解読法など様々な攻撃に対する安全性評価が行われた．しかし，SPECK は差分解読法に対する評価やサイドチャネル攻撃に対する評価が行われたが，未だ十分な安全性評価がなされたとは言えない．本研究では Integral Attack に対する SPECK の安全性評価を行う．SPECK は様々なブロック長と鍵長をサポートするが，本稿の評価対象は最もブロック長が短い，ブロック長 32bit，鍵長 64bit の SPECK32 とする．Integral Attack はブロック暗号に対して有効な攻撃手法であり，Integral Attack において攻撃者は Integral Distinguisher を用いて鍵回復攻撃を行う．Integral Distinguisher は以下のような性質を持つ．平文の特定のビットを固定し，そのとき考えられる全ての平文を r 段暗号化して得られた暗号文を全て XOR したものを考える．このとき暗号化に用いた鍵によらず計算結果の特定のビットが必ずゼロになる場合がある．この性質を満たすかどうかを調べることで鍵回復攻撃が実行可能である．Integral Distinguisher は平文のどのビットを固定するかで特徴づけられる Distinguisher の候補について全数探索を行うことで，証明では立証困難なものも含めて Distinguisher を発見することが可能である．また，Distinguisher が存在しないことを示すことが可能である．網羅的に Distinguisher を探索した既存研究として Wang らの成果がある．Wang らは Distinguisher の候補から網羅的に探索することで SIMON32 の 15 段の Distinguisher を発見した．しかし，Wang らが探索したのは候補の一部であり，探索しなかった候補の中により段数の多い Distinguisher が存在する可能性がある．Wang らが全数探索を行わなかった理由として，計算量の問題が考えられる．Distinguisher の候補の数はブロック長に依存し，Wang らの単純なアルゴリズムではブロック長が 32bit であっても計算量が膨大で全数探索は実行不可能である．そこで本研究では全数探索の計算量の削減手法を提案し，これを用いて SPECK32 と SIMON32 の Distinguisher の全数探索を行う．提案手法では，メモリを活用して単純なアルゴリズムの全数探索における冗長な暗号化を削減する．また，高速フーリエ変換を応用し XOR の計算量を削減する．提案手法はブロック暗号の構造に依存しないため，いかなるブロック暗号に対しても有効である．全数探索の結果から，SPECK32 に対して 6 段の Distinguisher が存在し，7 段以上の Distinguisher が存在しないことを示した．また，SIMON32 に対して 16 段以上の Distinguisher が存在しないことを示す．発見した SPECK32 の Distinguisher を用いて SPECK32 に対して鍵回復攻撃を構成する．鍵回復攻撃の構成においてはと同様に Partial-Sum，Meet-in-the-Middle Match を用いて計算量を削減する．その結果から，選択平文攻撃 (CPA) の条件で 8 段の SPECK32 が Integral Attack により攻撃可能，選択暗号文攻撃 (CCA)の条件で 11 段の SPECK32 が攻撃可能であることを示した．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 9 件）

① Atsushi Nagao, Toshihiro Ohigashi, Takanori Isobe, and Masakatu Morii, "Expanding Weak-key Space of RC4," IPSJ Journal of Information Processing, 査読有, vol.22, 2014, 357-365.

② Toshihiro Ohigashi, Takanori Isobe, Yuhei Watanabe, and Masakatu Morii, "Full Plaintext Recovery Attacks on RC4 Using Multiple Biases," IEICE Trans. Fund., 査読有, vol.E98-A,

2015, 81-91.
③ Sho Sakikoyama, Yosuke Todo, Kazumaro Aoki, and Masakatu Morii, "How Much Can Complexity of Linear Cryptanalysis be Reduced?," Information Security and Cryptology - ICISC 2014, LNCS, 査読有, vol. 8949, 2015, 117-131.
④ Sho Sakikoyama, Yosuke Todo, Kazumaro Aoki, Masakatu Morii, "Efficient Implementations for Practical Linear Cryptanalysis and Its Application to FEAL-8X," IEICE Trans. Fundamentals, 査読有, vol.EA99-A, 2016, 31-38.
⑤ Yosuke Todo and Masakatu Morii, "Bit-Based Division Property and Application to Simon Family," FSA2016, LNCS, 査読有, vol.9665, 2016,1-15.
⑥ Shohei Kakei, Masami Mohri, Yoshiaki Shiraishi, and Masakatu Morii, "SSL Client Authentication with TPM," IEICE TRANSACTIONS on Information and Systems, 査読有, Vol. E99-D, 2016, 1052-1061.
⑦ Yosuke Todo and Masakatu Morii,” Compact Representation for Division Property,” CANS2016, LNCS, 査読有, vol 10052, 2016
⑧ Yuhei Watanabe, Takanori Isobe, Toshihiro Ohigashi, and Masakatu Morii, "How to Efficiently Exploit Different Types of Biases for Plaintext Recovery of RC4," IEICE Trans. Fundamentals, 査読有, vol.E100-A, 2017, 803-810.
⑨ Yuhei Watanabe, Takahiro Iriyama, and Masakatu Morii, "Proposal of WEP Operation with Strong IV and Its Implementation," IPSJ Journal of Information Processing, 査読有, vol.25, 2017, 288-295.

〔学会発表〕(計 13 件)
① 草薙祥広, 長尾篤,森井昌克, "高密度ナップザック暗号に対する攻撃," コンピュータセキュリティシンポジウム(CSS2014), 2014 年 10 月, 札幌.
② 大東俊博, 渡辺優平, 森井昌克, "RC4 に対する平文回復攻撃の改良," コンピュータセキュリティシンポジウム(CSS2014), 2014 年 10 月, 札幌.
③ 先小山翔, 森井 昌克, "Integral Attack に対する SPECK32 の安全性評価," 暗号と情報セキュリティシンポジウム(SCIS2015), 2015 年 1 月, 小倉.
④ 飯塚大貴, 藤堂洋介, 森井昌克, "Simon48 に対する Integral 攻撃," 暗号と情 報セキュリティシンポジウム(SCIS2015), 2015 年 1 月, 小倉
⑤ 古川凌也, 伊沢亮一, 森井昌克, 井上大介, 中尾康二, "メモリ空間における 暗号化/復号関数の位置特定に関する検討," 信学技報, ICSS, 2015 年 6 月, 福岡.
⑥ 長谷川淳, 渡辺優平, 森井昌克, "OpenSSL における CREAM 脆弱性について," 信学技報, ICSS, 2015 年 6 月, 福岡.
⑦ 渡辺優平, 入山敬大, 森井昌克, "WEP の安全な運用方法とその実装について," 第 14 回情報科学技術フォーラム(FIT2015), 2015 年 9 月, 松山.
⑧ 長谷川淳, 渡辺優平, 森井昌克, "OpenSSL キャッシュタイミング攻撃の実現性について," 第 14 回情報科学技術フォーラム(FIT2015), 2015 年 9 月, 松山.
⑨ 古川凌也, 伊沢亮一, 森井昌克, 井上大介, 中尾 康二, "難読化コードに対する暗号関数特定手法の提案," コンピュータセキュリティシンポジウム(CSS2015), 2015 年 10 月, 長崎.
⑩ 藤堂洋介, 森井昌克, "ブロック暗号構造に対する汎用解析手法の提案と Kuznyechik の解析," 2016 年暗号と情報セキュリティシンポジウム(SCIS2016), 2016 年 1 月, 熊本.
⑪ 渡辺優平, 藤堂洋介, 森井昌克, "NLFSR 型ストリーム暗号に対する条件付差分特性の解析," 2016 年暗号と情報セキュリティシンポジウム(SCIS2016), 2016 年 1 月, 熊本.
⑫ 入山敬大, 渡辺優平, 森井昌克, "RC4 における Mantin らの弱鍵を用いた攻撃の改良," 2016 年暗号と情報セキュリティシンポジウム(SCIS2016), 2016 年 1 月, 熊本.
⑬ 草薙祥広, 森井昌克, "解読可能な高密度ナップザック暗号のクラス――現実的なパラメータを有するナップザック暗号は解読できる――," 2016 年暗号と情報セキュリティシンポジウム(SCIS2016), 2016 年 1 月, 熊本.

〔図書〕(計 0 件)

〔産業財産権〕

○出願状況 (計 0 件)

○取得状況 (計 0 件)

〔その他〕

６．研究組織
(1) 研究代表者
森井 昌克 (Masakatu Morii)
神戸大学・大学院工学研究科・教授
研究者番号：00220038