科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　　３　日現在

機関番号：　１４５０１
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５６０４５５

研究課題名（和文）実装を考慮したストリーム暗号の安全性評価に関する研究

研究課題名（英文）On the anaysis of stream cipher and its implementation

研究代表者
森井　昌克（Morii, Masakatu）

神戸大学・工学（系）研究科（研究院）・教授

研究者番号：００２２００３８

交付決定額（研究期間全体）：（直接経費）　　4,000,000円、（間接経費）　　1,200,000円

研究成果の概要（和文）：本研究ではWPA-TKIPの脆弱性、およびWEP鍵導出の考察、さらにその対策法について研究を進めた。WPA-TKIPでは具体的な脆弱性を指摘した。WEPにおいては申請者らがかつて提案した現実的な解読法を改良した。また、RC4に対する、世界で初めての現実的な計算量によるで平文回復攻撃を提案した。さらにSSL/TLSでのRC4の利用を想定して、実際に利用されている環境下での特定部分の平文を回復する方法を提案し、評価を行った。加えて提案した安全なWEP鍵運用方法について考察し、その現実的な実装方法を与えた。

研究成果の概要（英文）：Stream cipher is a widely-used in secured protocols. Especially, RC4 is adopted in a lot of standard protocols such as WEP, WPA and SSL/TLS as a standard encryption algorithm. We present the evaluation of these protocols based on the stream cipher. Firstly, we proposed practical plaintext recovery attacks on RC4 in SSL/TLS in the broadcast setting, independently. We give an active attack, which is a method to slide the position of a target plaintext byte into later byte of the plaintext. Our attack injects any bytes into the head of the plaintext by using malicious JavaScript. It causes improvement in probability for recovering a lot of plaintext bytes. Secondly, we propose a secure WEP operation against key recovery attacks. The proposed method requires for attackers at least 100,000 packets to recover the WEP key. At last, we propose an executable attack in a real environment without requiring the man-in-the-middle attack on WPA-TKIP.

研究分野：　工学

科研費の分科・細目：　通信・ネットワーク工学

キーワード：　ストリーム暗号　解読　無線LAN　RC4　WEP　WPA-TKIP　SSL-TLS　脆弱性

１．　研究開始当初の背景

ストリーム暗号はその高速性と回路規模に優れることから近年，大きく注目されている．しかしながら研究が進んでいる共通鍵ブロック暗号ほど研究が進展しているとは言えない．最近，共通鍵ブロック暗号との類似性から，その安全性評価を行う研究を含め，新たな取り組みが見られるものの共通鍵ブロック暗号ほど安全性評価基準が整備されていないのが現状である．その実装においても，インターネットで利用されるIEEE802.11x系の無線LAN暗号化方式であるWEPではRC4と呼ばれるストリーム暗号を利用しているが，規格化されて間もなく，S. Fluhrerらによって実装上の脆弱性が指摘された．その後，さらにWEPの安全性に関して疑問が投げられ，2008 年研究代表者らが中心となった研究において，数万パケットを観測するだけで暗号化鍵を導出できることが示された．これは現実的な環境において10秒程度で暗号鍵導出を行うことになる．このようにストリーム暗号の安全性評価が求められるだけでなく，その実装における安全性評価も求められている．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WEPについてはFMS攻撃における weak-IV を拡張し，ほとんどのIVがweak-IV であることを示し，その weak-IV を利用すれば高い確率で容易に鍵が導出できることを示した．さらに RC4 自体についても，鍵を用いて内部状態を初期化するアルゴリズムの脆弱性を指摘し，その脆弱性を利用してキーストリームから効率的に鍵を復元する方法を与えた．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．

２．　研究の目的

本研究ではe-STREAMやISOで選定されている各種ストリーム暗号について，その実装部分も含めて安全性評価を行う．また具体的には次のとおりである．

(1)RC4の安全性評価に関する研究

RC4はWEPだけでなく，サーバ・ブラウザ間通信の標準プロトコルである Secure Sockets Layer (SSL) / Transport Layer Security (TLS) に採用され，また様々なアプリケーション（たとえばAdobe Acrobat等）に採用されているストリーム暗号である．研究代表者は90年代からRC4の研究を進めるとともに，最近では暗号アルゴリズム自体の数々の脆弱性について研究成果を与えている．特にRC4とキーストリームの相関について詳細に検討し，有限なキーストリームから鍵を高い確率で推定できる鍵のクラスを定義し，それを弱鍵と呼び，その鍵を特定する研究を進めている．本研究項目では，RC4の安全性評価として、特に平文解読攻撃およびRC4のSSL/TLS実装での安全性について評価する。

(2)WEPの安全性に関する研究

研究代表者らが提案したWEPの解読法を発展させ，より少数の観測パケット，たとえば数千パケットの観測によって，現実的な時間でWEP鍵を導出する方法の開発を行う．

(3)WPA-TKIP の脆弱性とそれを利用した攻撃法に関する研究

研究代表者は先にWPA-TKIPの脆弱性を利用して，不正なパケットを相手に受理させることが可能となる具体的な攻撃法を提案した．本研究項目では MIC 鍵を短い時間，たとえば1分以内に解読する方法の開発を目的とする．さらにこの MIC 鍵によって偽造されたパケットを受理させることにより，深刻な脆弱性を有する示し，実証する．

３．　研究の方法

RC4の弱鍵の定義の拡張を見直し，より広い範囲で弱鍵となる鍵の特定と，キーストリームからその特定の鍵を求める計算アルゴリズムを提案する．次にFMS攻撃の拡張となる weak-IV の導出とそれを用いた鍵回復法を整理するとともに，先の弱鍵の拡張を含めた従来のRC4の脆弱性も含めて，2008年に研究代表者らが提案した IV に依存せず，かつ任意の IP パケットを観測するだけで鍵を導出できる方法との融合を試み，従来法より格段に少ない IP パケットを観測するだけで鍵を導出できる方法を開発する．また研究代表者らが 2009 年に提案した WPA-TKIP に対する攻撃法において，MIC鍵を高速に導出する方法を開発するとともに，攻撃法としてより有効となる偽造パケットの構成方法を提案する．研究代表者は RC4 の弱鍵を再定義し，その弱鍵と定義される一部の鍵については，キーストリームから少ない計算量で鍵を再構成できることを示した．この弱鍵となるクラスにおける鍵の総数を評価すること，そしてキーストリームからその鍵を復元する高速計算アルゴリズムの開発を行う．特に弱鍵のクラスを細分化し，その細分化されたクラス毎に計算アルゴリズムの開発を試みる．逆にこの結果を利用して、安全なWEP運用方法についても開発を試みる。

４．研究成果

(1) RC4の安全性評価に関する研究

オンラインバンクや電子商取引の普及にともない，パスワードやクレジットカード番号などの秘密情報をネットワーク上でやり

とりする機会が増加している.このような秘密情報の通信を保護するために SSL/TLS のようなプロトコルを用いて暗号化して通信を行っている.SSL/TLS では暗号化方式としてブロック暗号の AES やストリーム暗号の RC4 を選択することができる.ブロック暗号を CBC モードで利用する場合には BEAST や Luchy13 という攻撃が提案されているため,暗号化方式としてストリーム暗号である RC4 が広く利用されている.しかしながら,SSL/TLS での RC4 に対しても平文回復攻撃が提案されている. FSE 2013 で研究代表者らは同一の平文を複数の異なる鍵で暗号化する Broadcast Setting においてキーストリームの最も強い bias を用いることで,232 個の暗号文から先頭 257 バイトにおける平文の各バイトを 0.8 以上の確率で復元できることを示した. さらに 2 バイト単位の bias である Digraph repetition bias と復元した平文を利用して,平文の 258 バイト目以降を効率的に復元する手法が提案した. この攻撃により,ほとんど全ての平文を 2^{34} の暗号文のみから特定することが可能である.同種の攻撃として, USENIX Security 2013 で AlFardan らは RC4 のキーストリームの各バイトにおける全ての bias を複合的に利用する方式を提案した.この攻撃では 2^{32} 個の暗号 文から先頭 256 バイトにおける平文の各バイトがほぼ確率 1 で復元可能である.また,彼らは Fluhrer らが提案 した 2 バイト単位の bias を利用した攻撃も提案している.この攻撃では 256 バイトの平文に含まれる 16 バ イトの情報を 2^{33} 個の暗号文から 0.5 以上の確率で復元 可能である.SAC 2013 で大東らは Digraph repetition bias と Fluhrer らの bias を併用した攻撃を提案した. この攻撃では 235 個の暗号文を収集すれば,ほぼ確率 1 で任意の平文を復元することができる.これらの攻撃の うち平文の初期バイトに対する攻撃は RC4 のキーストリームにおける 1 バイト単位の bias のみを利用するも のであり,2 バイト単位の Long-term bias を併用することにより平文回復攻撃の効率化を図ることができると考 えられる.

本研究では 1 バイト単位の bias と 2 バイト単位の Long- term bias を併用することで,先頭 257 バイトのうち任意の位置にある平文を効率よく復元する方式を提案する. この攻撃は,HTTPS による通信においてヘッダ情報や通信されているデータの一部が既知であるという条件の下 で,既知の平文情報と Long-term bias を利用することで 平文回復攻撃の効率化を図る.平文にパスワードなどを 想定した 16 バイトの秘密情報が含まれる場合について, 提案方式を用いた平文回復攻撃を行う.実際の HTTPS による通信に対する攻撃を想定した場合,攻撃者は全て の秘密情報を復元する必要がある.そのため本稿では, 提案方式による平文回復攻撃の結果について攻撃対象とする全ての平文バイトの復元に成功する確率の評価を行 う.提案方式は Single-byte bias が存在すればどの平文 バイトにも適用可能であるが,本研究では Long-term bias の影響がある程度強くなる位置の平文を復元する実験を行った.具体的には平文の 113 バイト目から 128 バイト目 を対象とした攻撃を行い,全ての平文バイトの復元に成功する確率について評価する.結果として 2^{29} 個の暗号文から 16 バイト全ての平文を,従来よりも 6%高い,約 73%の確率で復元できる.さらに,個々の平文バイトの 成功確率については 113 バイト目や 128 バイト目のように既知の平文に隣接する未知の平文の復元に成功する確率が向上していることが確認できる.したがって提案方式は HTTPS による通信において平文の一部が既知である条件のもとで従来より効率のよい平文回復攻撃であるといえる.

(2) WEP の安全性に関する研究

スマートフォンなどの携帯端末の発展に伴い,利便性の高い無線 LAN が急速に普及している.無線 LAN は電波を用いて通信を行うため,常に盗聴の危険性に晒されている.盗聴による情報漏洩を防ぎ,安全に通信を行うために情報を暗号化する必要がある.無線 LAN の暗号化方式の一つに Wired Equivalent Privacy(WEP) がある.WEP はストリーム暗号である RC4 をベー スとした共通鍵暗号方式である.WEP は以前より深刻な脆弱性を指摘されており,その脆弱性を利用した攻撃 が多数提案されている.2001 年に S. Fluhrer, I. Mantin, A. Shamir らによっ て FMS 攻撃が提案された. FMS 攻撃は IV に依存する攻撃であり,weak IV と呼ばれる特定の IV を用いて鍵の導出を行う.2004 年には Korek によって, FMS 攻撃 を拡張した Korek 攻撃 が提案された. Korek 攻撃では FMS 攻撃より多くの IV を weak IV として利用できる.これらの攻撃はフィルタリングによって weak IV を 取り除くことによって対策が可能である.IV に依存しな い攻撃として,2006 年に Klein によって Klein 攻撃 が提案された.これは IV とキーストリームを用いて WEP 鍵を先頭から逐次的に導出する攻撃である.さらに 2008 年に E. Tews, R. Weinmann, A. Pyshkin らによって Klein 攻撃を改良した PTW 攻撃 が提案された. この攻撃は RC4 の内部状態の近似を用いることで,WEP 鍵の和を並列して導出することが可能である.PTW 攻撃では 40,000 パケットの観測によって確率 0.5 で WEP 鍵 を導出することができる. 2010 年には研究代表者らにより TeAM-OK 攻撃 が提案された. TeAM-OK 攻撃は Klein 攻撃, PTW 攻撃, OKM 攻撃 の三つの関係式を用いて鍵の導出を行う.この攻撃は 36,500 パケットを観測することで確率 0.5 で WEP 鍵を 導出することができる.2013 年には P. Sepehrdad, P. Susil, S. Vaudenay, M.

Vuagnoux らによって Tornado Attack が提案された. この攻撃は 22 個のバイアスを 利用して投票を行う. 22,500 パケットの盗聴により確率 0.5 で WEP 鍵の導出が可能である. 以上のように WEP に対する様々な鍵回復攻撃が提案されている. そのため より安全性の高い Wi-Fi Protected Access(WPA), Wi-Fi Protected Access2(WPA2)といった他の暗号化方 式への移行が推奨されている. しかしこれらの方式へ移行するには様々なコストを要することから, 大規模事業所等では未だに WEP が利用されている. WEP に対す る従来の鍵回復攻撃を防ぐ運用方法として, 一つの鍵あたりで使用するパケットを制限する方法がある. 現在のところ 20,000 パケット以下の盗聴によって鍵回復を行う方法は提案されていない. また 10,000 パケットの盗聴において, 既存の鍵回復攻撃の成功確率は 0 である. そのため 10,000 パケットの通信を行うごとに WEP 鍵を更新する方法が一般的である. しかし 10,000 パケッ トは非常に少数であり, 頻繁な鍵の更新は通信のスルー プットに多大な影響を与える. そこで 2011 年に研究代表者らによって Strong IV が提案された. Strong IV は Klein 攻撃が失敗する IV のみを収集した IV の集合を指す. この IV のみを利用することで, 100,000 パケットの盗聴においても 鍵回復攻撃が困難になる. その結果 WEP 鍵の更新間隔を 100,000 パケットまで拡大することが可能となる. 100,000 パケットの通信を行う場合, 100,000 個の Strong IV を生成する必要がある. しかし Strong IV の生成確率は低いため, 100,000 個を生成するために多大な時間 を要してしまう. そのため本来の目的であるスループッ トの向上を達成することが困難であった.

本研究では Strong IV の定義を修正することで, Strong IV の生成を高速化する方法を提案する. 従来の Strong IV では Klein 攻撃が成功する危険性のある IV を取り除いていた. しかし取り除かれた IV の中には, 実際には 攻撃が成功しないものも含まれている. こういった IV も Strong IV として利用することで, Strong IV の領域 を拡大する. これにより Strong IV の生成確率を向上さ せる. 提案する Strong IV の生成確率は 0.96 であり, 従来の Strong IV と比較して高速に生成が可能である. さらにこの Strong IV を効率的に利用した WEP の運用方 法を提案し, その安全性を評価する. 提案方式では定義 を修正した Strong IV とランダムに選択した IV を混合した IV の集合を用いて通信を行う. Klein 攻撃などの鍵回復攻撃では投票により WEP 鍵候補を導出する. この IV の集合に対して鍵回復攻撃を行った場合, すべての鍵 の候補値への投票数がほぼ均等になり, 正しい WEP 鍵 を導出することが困難となる. その結果, 10,000 パケッ ト程度の盗聴では従来の鍵回復攻撃が困難になる. 提案する Strong IV を用いることで, 現実的な WEP 鍵の更 新間隔で, 十分に高速な WEP の運用が可能となる.

(3) WPA-TKIP の脆弱性とそれを利用した攻撃法に関する研究

WPA(Wi-Fi Protected Access) は無線 LAN 通信の機密性や完全性を保護するセキュリティプロトコルであり, 従来から使われてきた WEP (Wired Equivalent Privacy) の脆弱性を取り除く仕組みを導入している. WPA-TKIP の安全性は多くの研究者によって議論されている が, 辞 書攻撃が可能なパスフレーズを使っているなど特定の条件を除いては現実的な攻撃は知られていなかった. 2008 年に Beck と Tews は 12〜15 分で WPA-TKIP の改ざん検出用鍵 (MIC 鍵) を復元でき, ARP パケットなどの短い暗号化パケットを偽造で きる攻撃 (Beck-Tews 攻撃) を提案した. Beck-Tews 攻撃では, chopchop 攻撃と呼ばれる WEP に対するリプレイ攻撃 を IEEE802.11e をサポートしているという条件で WPA-TKIP に適用する. Beck-Tews 攻撃が IEEE802.11e に限定した攻撃 なのは, WPA-TKIP にはリプレイ攻撃対策の仕組みが組み込まれているためである. WPA-TKIP では暗号化パケットを受理する毎に増加する TSC カウンタと呼ばれる値を保持しており, TSC カウンタより小さな値に対応する暗号化パケットを破棄している. IEEE802.11e では通信を複数のアクセスカテゴ リに分類し通信を行い, かつ各アクセスカテゴリ毎に独立して TSC カウンタを管理することから, TSC カウンタが小さなア クセスカテゴリを選択することでリプレイ攻撃を実行できる.

研究代表者らはすでに JWIS2009, CSS2009 で IEEE802.11e をサポートしない無線 LAN 機器にも, 中間者攻撃を行うことで chopchop 攻撃を適用する手法を提案している (大東-森井攻撃). しかし中間者攻撃を実際に実行するには, アクセスポイントと クライアントの通信を遮断する必要があり, 実環境において必ずしも容易に実行可能な攻撃とは言い難い. そこで, 本研究では実環境においても容易に実行でき, なおかつ IEEE802.11e の通信や中間者攻撃の前提を必要としない現 実的な攻撃手法を提案する. 本攻撃はアクセスポイントまたは クライアントの IEEE802.11e 機能の有効/無効に依らず, クラ イアントが QoS パケットを受信すれば処理してしまうという脆弱性を利用している. この実装上の脆弱性は近年発売されてい る無線 LAN 機器の大部分に存在している. 提案手法を用いる ことでユーザの IEEE802.11e の設定に関わらず WPA-TKIP に対して攻撃が可能となる.

５． 主な発表論文等

〔雑誌論文〕(計 ９件)

① Ryoichi Isawa and Masakatu Morii, "Authentication Scheme with User Anonymity Based on Three Party Structure for Wireless Environments," Proceedings of The 6th Joint Workshop on Information Security (JWIS2011), 査読有, vol.1, 2011, 1-8.

② Tatsuya Takehisa, Hiroki Nogawa, and Masakatu Morii, "AES Flow Interception: Key Snooping Method on Virtual Machine - Exception Handling Attack for AES-NI -," The 6th Joint Workshop on Information Security (JWIS2011), 査読有, vol.1, 2011, 9-16.

③ Masakatu Morii and Yosuke Todo, "Cryptanalysis for RC4 and breaking WEP/WPA-TKIP," IEICE Trans. Information and Systems, 査読有, vol.E94-D, 2011, 2087-2094.

④ Yosuke Todo, Yuki Ozawa, Toshihiro Ohigashi, and Masakatu Morii, "Falsification attacks against WPA-TKIP in a realistic environment," IEICE Trans. on Information and Systems, 査読有, vol.E95-D, 2012 588-595.

⑤ Tsubasa Tsukaune, Yosuke Todo, and Masakatu Morii, "Proposal of a Secure WEP Operation against Existing Key Recovery Attacks and its Evaluation" Proc. AsiaJCIS2012, 査読有, vol.1, 2012, 1-6.

⑥ Takanori Isobe, Toshihiro Ohigashi, and Masakatu Morii, "Slide Cryptanalysis of Lightweight Stream Cipher RAKAPOSHI," The 7th Int. Workshop on Security (IWSEC2012), LNCS 7631, Springer-Verlag, 査読有, 2012, 138-155.

⑦ Takanori Isobe, Toshihiro Ohigashi, Yuhei Watanabe, and Masakatu Morii, "Full Plaintext Recovery Attack on Broadcast RC4," 20th Int. Workshop on Fast Software Encryption (FSE2013), LNCS, Springer-Verlag, 査読有, vol.1, 2013, 1-18.

⑧ Takanori Isobe , Toshihiro Ohigashi , Masakatu Morii, "Slide Property of RAKAPOSHI and Its Application to Key Recovery Attack," Journal of information processing, 査読有, vol.21, 2013, 599-606.

⑨ Takanori Isobe, Toshihiro Ohigashi, Yuhei Watanabe, Masakatu Morii, "Comprehensive Analysis of Initial Keystream Biases of RC4," IEICE Trans. Fundamentals, 査読有, vol.EA97-A, 2014, 139-151.

〔学会発表〕(計 9件)

① 塚畝翼, 藤堂洋介, 森井昌克, "既存鍵回復攻撃を無効にする WEP 運用の提案," 信学技報,LOIS, 2011年 9月, 松山

② 塚畝翼, 藤堂洋介, 森井昌克, "既存鍵回復攻撃を困難にする WEP の運用とその評価," 信学技報 ISEC, 2011年11月, 大阪.

③ Masakatu Morii, "How to break WEP/WPA-TKIP; Attack on RC4 and other stream ciphers," AsiaJCIS2013, Aug. 2012, Tokai Univ., Japan

④ Atsushi Nagao, Toshihiro Ohigashi, Takanori Isobe, and Masakatu Morii, "Expanding Weak-Key Space of RC4," SCIS2013, Jan. 2013, Kyoto

⑤ Yuhei Watanabe, Takanori Isobe, Toshihiro Ohigashi, and Masakatu Morii, "New Biases of RC4 and its Application to Disitingushing, Key Recovery, Plaintext Recovery Attacks," SCIS2013, Jan. 2013, Kyoto.

⑥ 飯塚大貴, 渡辺優平, 長尾篤, 森井昌克, "高速 WEP 解読法," コンピュータセキュリティシンポジウム(CSS2013), 2013年10月, 高松

⑦ 入山 敬大, 渡辺 優平, 森井昌克, "WEP における Strong IV の評価とその実装," SCIS2014, 2014年1月, 鹿児島.

⑧ 渡辺 優平, 森井昌克, "SSL/TLS での RC4 に対する平文回復攻撃の改良," SCIS2014, 2014 年 1 月, 鹿児島.
⑨ 大東俊博, 五十部孝典, 渡辺優平, 野島良, 森井昌克, "SSL/TLS の RC4 への Active Attack," 信学技法 ICSS, 2014 年 3 月, 名護.

〔図書〕（計　0 件）

〔産業財産権〕
○出願状況（計　0 件）

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