Michael アルゴリズムによる MIC の生成について

島根大学　総合理工学部　数理・情報システム学科

田中研究室

S113079　福重　絵梨

目次

第 1 章　はじめに

近年、無線 LAN が店舗や公共施設など多くの場所で使用されるようになった。無線 LAN はデータを無線で通信するため、優先での通信よりも盗聴などの脅威が大きくなる。そのため、データを暗号化して通信するセキュリティプロトコルの使用が必須で、そのセキュリティプロトコルとして、WEP や WPA、WPA2 などが利用されている。

このセキュリティプロトコルの中で、WEP に対しては既に様々な脆弱性が指摘されており、また、多数の攻撃方法も提案されている[1][2][3]。これらの脆弱性を取り除く仕組みを、WPA では導入されているため、現在では、WEP よりもセキュリティ性能の高い WPA への移行が推奨されている。

しかし、WPA に対しても、Beck,Tews (2009)に よって提案された beck-tews 攻撃によって、12～15 分と いう時間がかかるものの、WPA のパケットを改ざんするこ とができ、また、条件を加えることによって、実行時間を1 分以下、最も条件が良い時には 10 秒ほどにまで短縮できるという研究結果も発表されている[4]。

そこで本研究では、WPA 内で使われている Michael アルゴリズムについての実装を行った。

第 2 章　Michael アルゴリズム

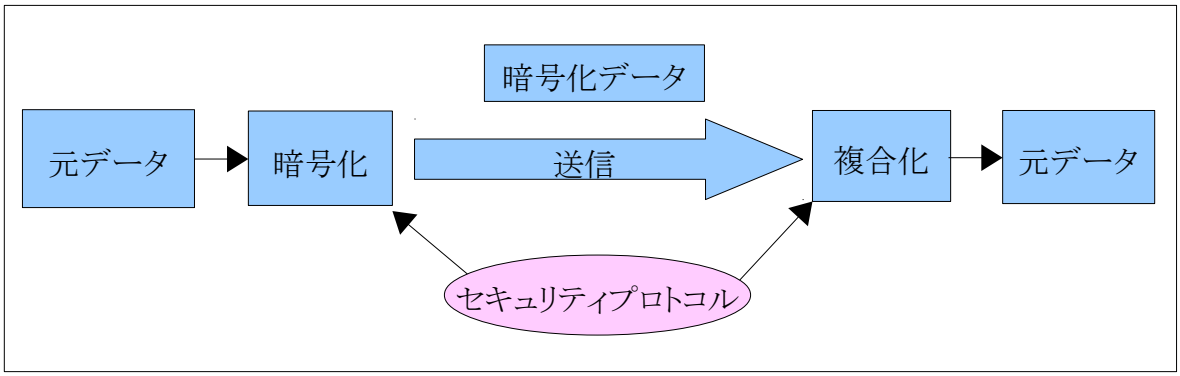
本章では、無線 LAN セキュリティプロトコルである WPA と、Michael アルゴリズムについて述べる。

無線 LAN とは、LAN と呼ばれる、家庭内や施設内といった小さな規模で用いられるコンピュータネットワークのうち、電波の送受信によって通信を行うものである。
単に無線 LAN と言った場合は、IEEE 802.11 規格に準拠した機器で構成されるネットワークを指すことが多く、本論文でもこの意味で用いる。

無線 LAN は通信ケーブルを物理的に接続する必要が無く、また、近年ではスマートフォンや タブレット等の普及もあり、一般家庭や企業のみならず公共施設や店舗など、多くの場所で設置・利用されている。

2.1 WPA 無線 LAN のセキュリティプロトコル

無線 LAN 通信では、有線の通信と比べて極めて容易に傍受を行うことができるため、送信されるパケットを暗号化し、内容を傍受されないようにする必要がある。その暗号化に利用されるのが、WEP や WPA、WPA2 などといった各セキュリティプロトコルである。



＜図 1　セキュリティプロトコル＞

暗号化をしてデータを送り、複合化で元のデータを復元することで傍受の危険を減らすことをセキュリティプロトコルという。

この無線 LAN のセキュリティプロトコルには様々なものがあり、その中の 1 つである WPA は現在広く普及し、利用されている。

2.2 WPA

WPA とは、Wi-Fi Protected Access の略で、無線 LAN セキュリティプロトコルの1つである。

WPA には、WPA-TKIP（Temporal Key Integrity Protocol）と、WPA-AES(Advanced Encryption Standard)の2つがある。

WPA-TKIP の暗号方式には WEP と同じ RC4 が使用されており、WEP を使用している既存の通信機器との互換性もあるため、現在、WEP の後継として広く普及している。
WPA-TKIP には WEP の脆弱性を補うために、メッセージの改竄を防ぐなど、新たな機能を持つことでセキュリティ強度を高めている。
しかし、暗号化の方式としては WEP と同じく RC4 を使用しているため、解析ツールによってセキュリティが破られる恐れもある。

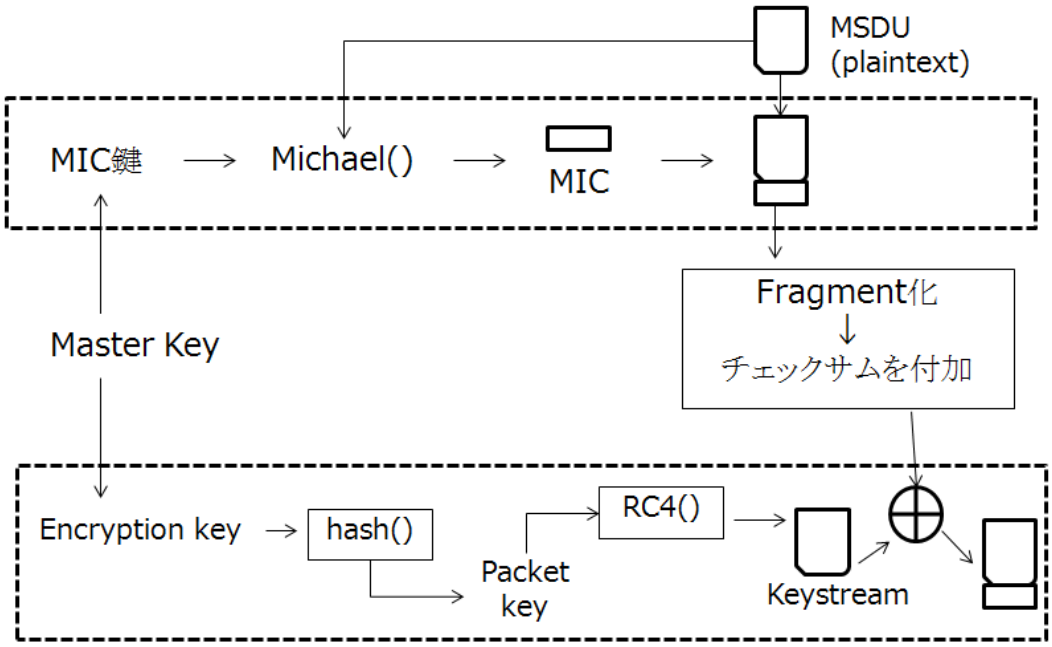
WPA-AES の暗号方式には CCMP(Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)が使用されており、この方式は TKIP のものよりもセキュリティ強度が高い。
しかし、この AES は古い機器では対応できないこともあるため、AES のほうがセキュリティ強度が高いにもかかわらず、TKIP が多く普及しているという現状である。

2.2.1 WPA-TKIP 暗号化

WPA-TKIP では、クライアントとアクセス間で秘密鍵（Master Key）を共有する。その秘密鍵から、64bit の MIC 鍵と 128bit の暗号鍵（Encryption Key）が生成さ れる。

この MIC 鍵を用いて MIC を生成する。秘密鍵から生成された MIC 鍵と平文を用いて、Michael によって生成されたメッセージ完全性符号であ る MIC は、平文の末尾に付され、フラグメント化や、CRC32 によるチェックサムの付加などの処理をされる。

また、秘密鍵から生成された暗号鍵は、hush 関数、RC4 で処理をされ、キーストリームとなる。このキーストリームと、先ほどの MIC が付加された平文の排他的論理和を取ることによって、暗号文が生成される。



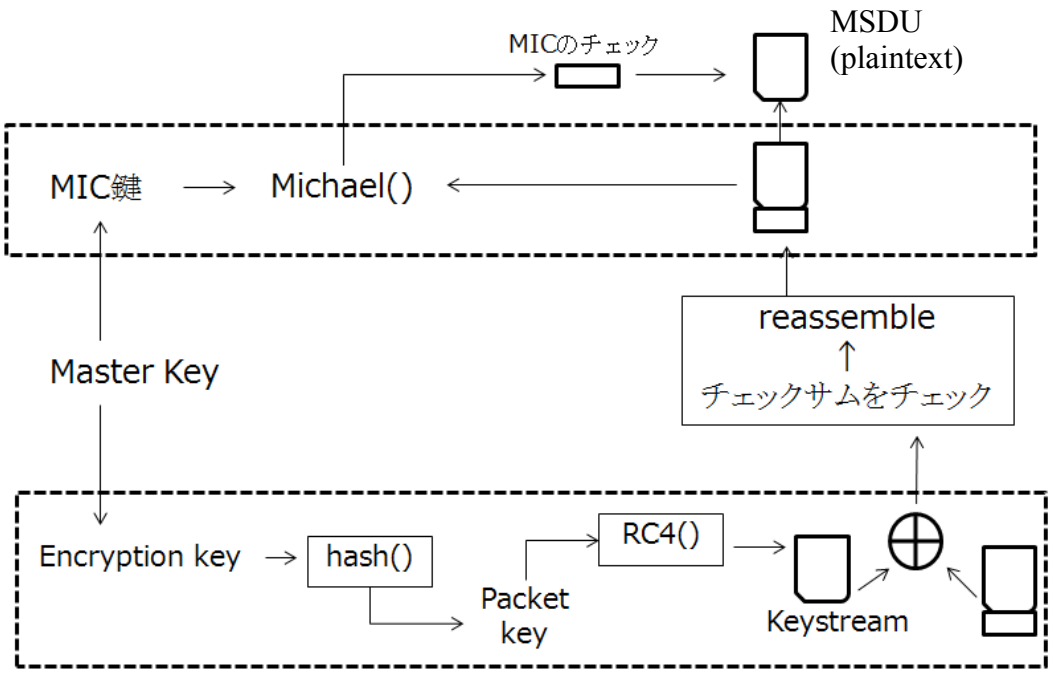
＜図 2　WPA-TKIP 暗号化の流れ＞

2.2.2 WPA-TKIP 複合化

複合化を行う場合は暗号化とは逆の流れになる。

秘密鍵はクライントとアクセス間で共有されているので、暗号化と同じように Michael を用いて MIC と、RC4 を用いてキーストリームを生成する。

暗号文とキーストリームを用いて複合され、チェックサムが計算され、受信したチェックサムと比較されて一致するかどうかを比較する。一致した場合は MIC 鍵を用いて MIC を復元し、受信した MIC 値と比較してメッセージが改竄されていないかをチェックする。[5]



＜図 3　WPA-TKIP 複合化の流れ＞

2.3 Michael アルゴリズム

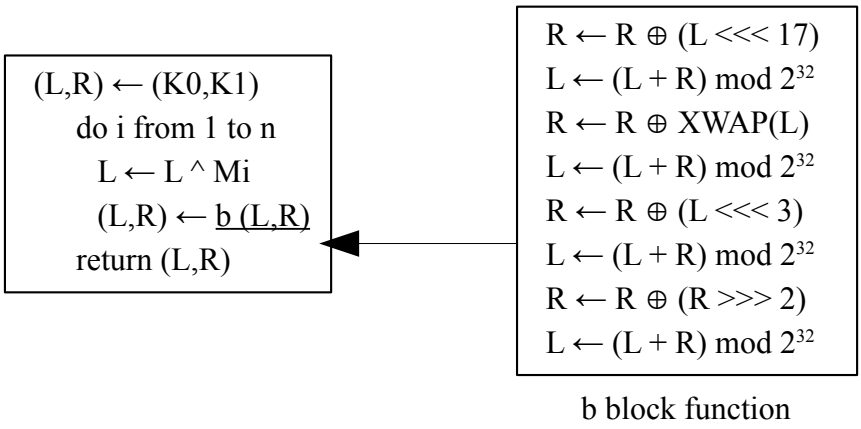
Michael アルゴリズムとは、Niels Ferguson によって考えられたメッセージダイジェスト関数の一種で、WPA-TKIP 内で、改竄を検知するための MIC を生成する際に用いられている。[6]

MIC 鍵（Message Integrity Check Key）とは、64bit の改竄検知用鍵で、この MIC 鍵を用いて 64bit の MIC を生成する。

秘密鍵から生成された MIC 鍵と平文を用いて、64bit の MIC を生成する際に使用されるアルゴリ ズムを Michael アルゴリズムという。Michael によって生成されたメッセージ完全性符号であ る MIC は、メッセージの改竄を検知するために用いられ、受信側で生成された MIC の値と送信側で付加した MIC の値が一致しなければ、メッセージが改竄されたものとみなされる。

第 3 章　実装方法

MIC（64bit）を導出するためには、まず、64bit の MIC 鍵を 32bit にそれぞれ分割し、K0,K1 とする。そして、取得している平文を 1byte 単位で分割して、平文{M1,M2,...,Mn}とし、平文 Mi と K0 の排他的論理和をとり、K0 へ代入する。K0 と K1 をそれぞれ R,L に置き換え、排他的論理和と回転シフトを用いて計算をしていく。



＜図 4　Michael アルゴリズム[7]＞

導出された R,L は、それぞれ 32bit である。R と L を結合して導出される 64bit の文字列が MIC となる。WPA では、この MIC を元の平文の末尾に付加し、そこから、フラグメント化を行うなどの処理をして暗号文を生成する。また、MIC 鍵を導出するには、Michael を逆算していく必要がある。

そして、Michael 関数は一方向関数ではないため、逆算をすることによって MIC 鍵の値を導出することができる。

3.1 MIC 鍵から MIC を生成

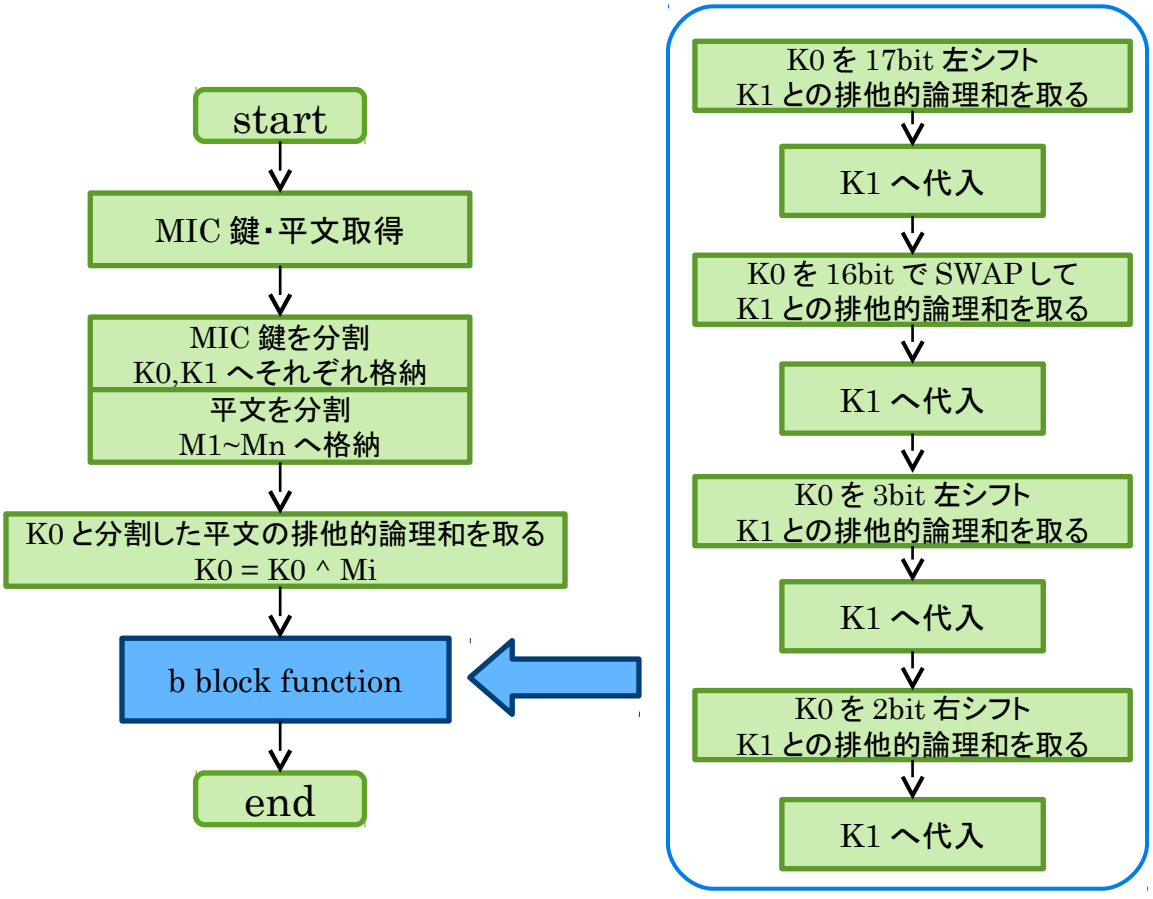
秘密鍵から生成された 64bit の MIC 鍵を 32bit に分割してそれぞれ K0,K1 に格納する。また、平文を 1byte ずつに分割し、M0～Mn へ格納する。

K0 と、分割した平文の排他的論理和を取り、もう一度 K0 へ戻す。

そして、その K0 と K1 を b block function で左回転シフト、右回転シフト、SWAP を用いて計算していく。この時、回転シフトなので右シフトの時は末尾の値が先頭へ格納され、左シフトの時は先頭の値が末尾に格納される。

また、SWAP では、32bit の K0 の上位 16bit と下位 16bit が交換される。

このような計算によってそれぞれ 32bit の K0、K1 が生成され、K0、K1 をつなげた 64bit の値が MIC である。



＜図 5　MIC 鍵から MIC の生成　フローチャート＞

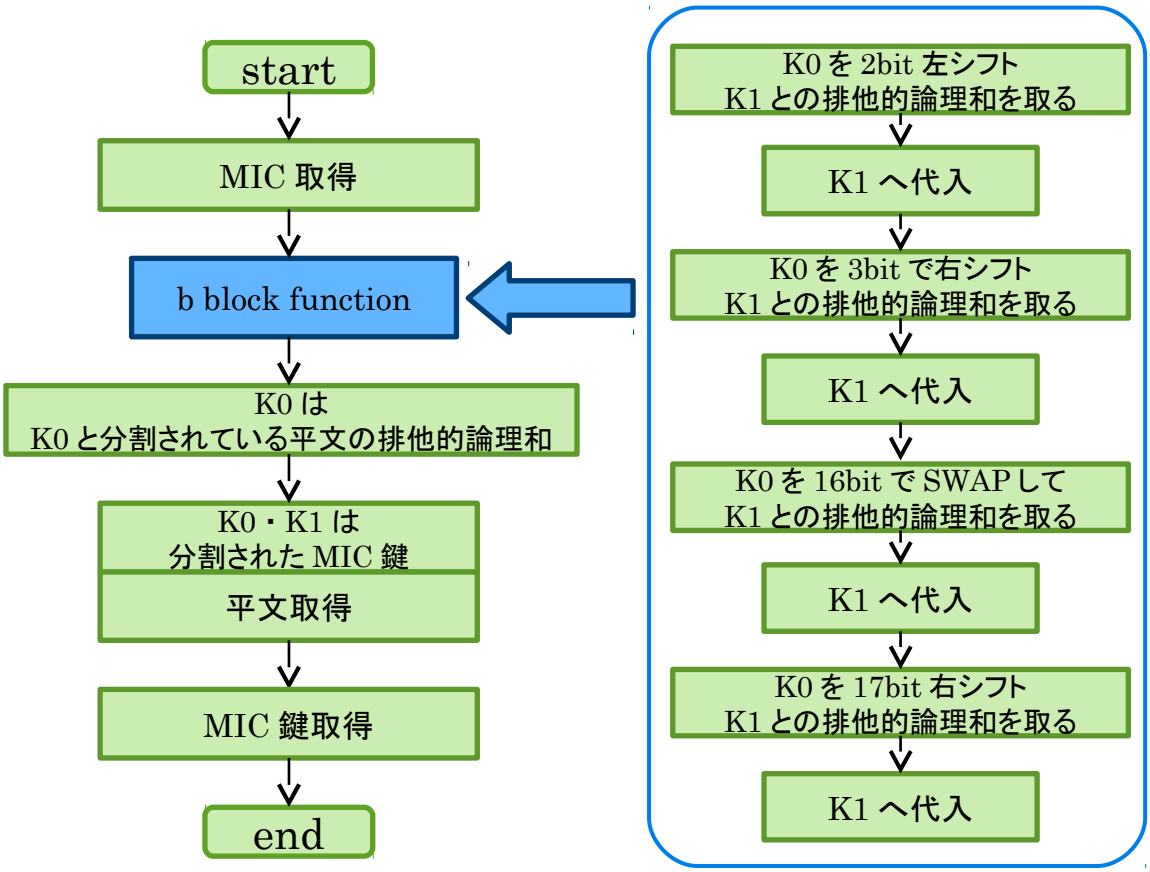
3.2 MIC から MIC 鍵を導出

Michael は一方向関数ではないため、逆算をすることによって MIC から MIC 鍵の値を導くことができる。

まず 64bit の MIC を取得する。64bit の MIC を 32bit に分割して K0,K1 に格納した後に b block function で計算していく。この時、3.1 で右シフトした部分は左シフトを行い、左シフトした部分は右シフトを行う。

また、SWAP は 32bit の上位下位を交換するものなので同じ操作を行う。

b block function で計算が終わった K0 は、32bit 分の MIC 鍵と 1byte 分の平文との排他的論理和を取った値である。これを分解すると、それぞれ 32bit の K0,K1 を取得できる。この K0,K1 をつなげた 64bit の値が元の MIC 鍵である。



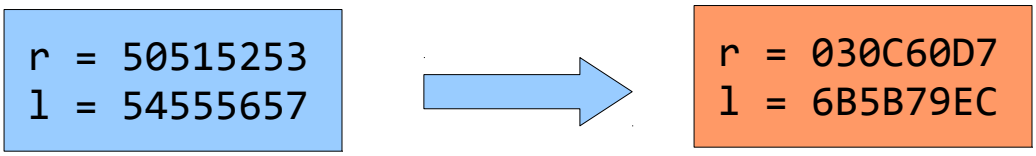
＜図 6　MIC から MIC 鍵の導出　フローチャート＞

第 4 章　結果

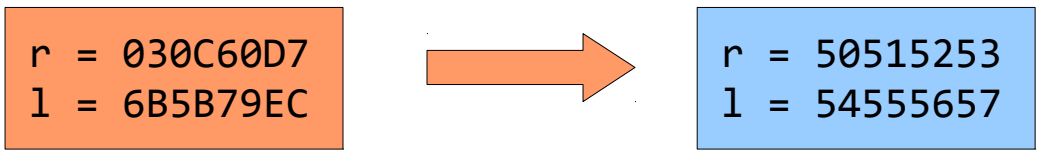
WPA-TKIP に使用されている、Michael　アルゴリズムを実装し、MIC 鍵から MIC を生成することができた。

Michael アルゴリズムを逆算することで、MIC から MIC 鍵の導出するアルゴリズムの実装を行うことができた。

実装した Michael アルゴリズムを用いて MIC 鍵から MIC を生成し、その生成された MIC を、Michael アルゴリズムを逆算するプログラムに入れると、最初に設定したものと同じ値の MIC 鍵を導出することができた。



＜MIC から MIC 鍵を生成＞



＜MIC 鍵から MIC を導出＞

第 5 章　今後の課題

今回は WPA-TKIP 内の 1 部分だけだったが、今後は WPA-TKIP 全体を解析出来るようにしていく。そのために、以下のことを今後の課題としていきたい。

・WPA で使われている暗号方式である RC4 を、既存の研究があるため、それを参考にして実装する。

・TSC カウンタを用いた、リプライ攻撃を防ぐための機能の無効化プログラムの実装。

・チェックサムによる通信エラー判定の無効かプログラムの実装。

これらのプログラムを実装し、無線 LAN に対する攻撃方法の提案を行っていく。

謝辞

本研究を進めるにあたり、最後まで熱心に御指導して頂きました田中章司郎教授には心より御礼申し上げます。

同研究室の皆様にも、数々の御協力と御助言を頂きましたこと、厚く御礼申し上げます。

なお、本論文、本研究で作成したプログラム及び、データ、並びに関連する 発表資料等の全ての知的財産権を、本研究の指導教官の田中章司郎教授に譲渡致 します。

参考・引用文献

[1]S. Fluhrer, I. Mntin, and A. Shamir, “Weaknesses in the Key Scheduling Algorithm of RC4”, SAC2001, Lecture Notes In Computer Science, Vol. 2259, pp.1-24, Springer-Verlag, 2001.
[2]E. Tews, R. Weinmann, and A. Pyshkin, “Breaking 104 bit WEP in less than 60 seconds”, WISA2007, Lecture Notes in Computer Science, Vol.4867, pp.188-202, Springer-Verlag, 2008.
[3]A. Klein, “Attacks on the RC4 stream cipher”, Designs, Codes and Cryptography, Vol.48, no.3, pp.269-286, Sep.2008.
[4]M. Beck, E. Tews, ”Practical attacks against WEP and WPA”, Proceedings of the second ACM conference on Wireless network security, pp.79-86, 2009.
[5]小澤勇騎, 大東俊博, 森井昌克,”無線 LAN 暗号化 WPA への改ざん攻撃の実装と評価”,電子情報通信学会技術研究報告. LOIS, ライフインテリジェンスとオフィス情報システム 109(205), 113-118, 2009-09-17
[6]http://paginas.fe.up.pt/~jaime/0506/SSR/802.11i-2004.pdf
[7]IEEE Standards 802.11i-2004