高速 WEP 解読法

飯塚 大貴 †　渡辺 優平 †　長尾 篤 †　森井 昌克 †

† 神戸大学大学院工学研究科
657-8501 兵庫県神戸市灘区六甲台町 1-1
iizuka@stu.kobe-u.ac.jp
yuheiwatanabe@stu.kobe-u.ac.jp
a.nagao@stu.kobe-u.ac.jp
mmorii@kobe-u.ac.jp

あらまし 2010 年に寺村らは PTW 攻撃を改良した TeAM-OK 攻撃を提案し，36, 500 個の IP パケットから確率 0.5 で WEP 鍵の回復が可能であることを示した．さらに 2013 年に Sepehrdad らにより 22, 500 個の IP パケットから同様の確率で鍵回復が可能である攻撃が提案された．しかしながら，鍵回復に必要な計算量の評価は行われていない．そのため攻撃成功確率が低くなるパケット数で秘密鍵を更新することにより WEP は安全に利用できると考えられている．本稿では取得できるパケット数が制限された環境下において WEP の鍵回復にかかる計算量の評価を行う．WEP に対する鍵回復攻撃として TeAM-OK 攻撃を利用し，20, 000 個以下の IP パケットで WEP 鍵の回復が可能であることを示す．

Speeding Up Method for WEP Attack

Hiroki Iizuka†　Yuhei Watanabe†　Atsushi Nagao†　Masakatu Morii†

†Graduate School of Engineering, Kobe University
1-1, Rokkodai, Nada-ku, Kobe, Hyogo 657-8501, Japan
iizuka@stu.kobe-u.ac.jp
yuheiwatanabe@stu.kobe-u.ac.jp
a.nagao@stu.kobe-u.ac.jp
mmorii@kobe-u.ac.jp

Abstract In 2010, Teramura et al. proposed a key recovery attack on WEP (called the TeAM-OK attack) by improving the PTW attack, and showed that this attack could recover the WEP key with probability of 0.5 when 36,500 IP packets are given. In 2013, Sepehrdad et al. presented the attack which could recover the WEP key with same probability when 22,500 IP packets are given. However, the complexity required for key recovery attack is not evaluated. Then, since success probability of the attack becomes lower, it is assumed that WEP can use safely by updating a secret key with a small number of packets. In this paper, we evaluate the complexity required for key recovery attack on WEP when the number of obtained packets is restricted. We show that we can recover the WEP key from IP packet of 20,000 or less by using the TeAM-OK attack as a key recovery attack on WEP.

1　はじめに

スマートフォンの急速な普及により個人の携帯端末において膨大なデータを通信する機会が増加している．この通信量の急激な増加により，通信障害が頻発した．そのため，通信規制を設けることで通信量を抑制し，膨大なデータを通信する場合は無線 LAN を利用することが推奨されている．しかし無線 LAN は電波を利用して通信を行うため機密情報を盗聴される危険性がある．無線 LAN を安全に利用するために情報を暗号化して送信する必要がある．無線 LAN 用のセキュリティプロトコルの一つとして IEEE802.11b に規定されている Wired Equivalent Privacy(WEP) [1] がある．WEP は暗号化にストリーム暗号である RC4 [2] を利用している．しかし WEP はセキュリティ面において脆弱性が指摘されており，様々な鍵回復攻撃が提案されている．

2006 年に Klein により提案された関連鍵攻撃 (以降 Klein 攻撃) がある [3]．攻撃関数を利用することでキーストリームから鍵を高い確率で推測し，逐次的に鍵回復する攻撃である．そして 2007 年に Tews らは Klein の関連鍵攻撃を WEP 解読用に拡張した関連鍵攻撃 (以降 PTW 攻撃) を提案した [4]．PTW 攻撃を利用することで約 80,000 個の ARP パケットを取得することで確率 0.9 で鍵回復することができる．しかし ARP パケットを取得するには膨大な時間が必要となる．そこで取得が容易である IP パケットを利用した攻撃が提案された．2010 年に寺村らは PTW 攻撃を拡張した TeAM-OK 攻撃を提案した [5]．TeAM-OK 攻撃は 3 つの攻撃手法 (Klein 攻撃，PTW 攻撃，OKM 攻撃 [9]) を組み合わせた攻撃手法である．キーストリーム先頭 19 番目から 31 番目までの 2 巡目を利用することで少ないパケット数で WEP の解読が可能となる．約 36,500 個の IP パケットを取得することで確率 0.5，約 50,000 個の IP パケットで確率 0.9 で鍵回復することができる．2013 年には Sepehrdad らが暗号化アルゴリズムにおける bias を利用した攻撃を提案した [6]．これにより約 22,500 個のパケットを取得することで確率 0.5 で鍵回復することができる．

WEP に対する鍵回復攻撃により必要なパケットを取得することでほんの数秒で鍵回復が可能となり，他のセキュリティプロトコルへの移行が推奨されている．しかしながら現在でも少ないパケット数で鍵を変更することで WEP が利用されている．鍵回復に必要な計算量の評価は行われていないため，攻撃成功確率が低いパケット数で秘密鍵を更新することにより WEP は安全に利用できると考えられている．

本稿では取得できるパケット数が制限された環境において WEP の安全性評価を行う．これまではパケット数と成功確率の関係から評価が行われていた．しかし，実際の WEP に対する安全性評価を行うためには攻撃成功確率が低くなるパケット数においてどの程度の計算量で鍵回復が可能であるかを評価する必要があると考えられる．そこで少ないパケット数における計算量との関係について評価を行い，20,000 個以下の IP パケットでも探索範囲を拡張することで鍵回復が可能であることを示す．

2　WEP の概要

Wired Equivalent Privacy(WEP) は IEEE802.11b に規定されている無線 LAN のセキュリティプロトコルである．暗号化/復号にはストリーム暗号である RC4 を利用している．本章では RC4，WEP の概要について述べる．

2.1　RC4

RC4 は 1987 年に Rivest が提案したストリーム暗号である．SSL/TLS [7],WEP,WPA [8] など多くの通信プロトコルで利用されている．RC4 は鍵スケジューリングアルゴリズム (KSA) と擬似乱数生成アルゴリズム (PRGA) で構成される．KSA は鍵を用いて内部状態を初期化するアルゴリズムであり，PRGA は初期化された内部状態からキーストリームと呼ばれる擬乱数系列を生成するアルゴリズムである．RC4 の特徴として KSA と PRGA はともに短いコードで記述できるので，ソフトウェア上非常に高速に動作することが挙げられる．KSA と PRGA のアルゴ

Algorithm 1 KSA

KSA($K[0,\ldots,\ell-1]$)**:**

```
for i = 0 to N − 1 do
  S[i] ← i
end for
j ← 0
for i = 0 to N − 1 do
  j ← j + S[i] + K[i mod ℓ]
  Swap S[i] and S[j]
end for
```

Algorithm 2 PRGA

PRGA(K)**:**

```
i ← 0
j ← 0
S* ← KSA(K)
loop
  i ← i + 1
  j ← j + S*[i]
  Swap S*[i] and S*[j]
  Output Z ← S*[S*[i] + S*[j]]
end loop
```

リズムを Algorithm 1，2 に示す．$S[i]$ は KSA における i バイト目の内部状態を示し，$S^*[i]$ は PRGA における内部状態の i バイト目を示す．RC4 では内部状態 S の数は N バイト，鍵長は ℓ と示されそれぞれ可変である．PRGA により得られたキーストリームと平文/暗号文の排他的論理和により RC4 の暗号化/復号を行う．

2.2 WEP

WEP は暗号化/復号にストリーム暗号である RC4 を利用したセキュリティプロトコルである．WEP で用いられる秘密鍵は IV24 ビットと WEP 鍵 104 ビットもしくは 40 ビットを連結することで生成される．本稿ではより安全性の高い 104 ビットの WEP 鍵を想定しているため，104 ビットの WEP 鍵に関して議論を行う．秘密鍵 K を次式で示す．

$$K[i] = \begin{cases} IV[i] \ (i = 0, 1, 2) \\ K'[i] \ (i = 3, 4, \ldots, 15) \end{cases}$$

K' は WEP 鍵を表す．

秘密鍵 K を RC4 に入力し，得られた擬似乱数列と平文の排他的論理和により暗号化を行う．送信者は暗号文と IV を送信する．受信者は送られてきた IV と事前に共有していた WEP 鍵を RC4 に入力し，得られた擬似乱数列と暗号文の排他的論理和により復号を行う．

RC4 に入力する秘密鍵は 1 つも公開してはならない．しかしながら WEP は暗号文を送信する際既知となる IV を送信しており，RC4 の本来の使用方法と異なっている．この点において WEP の脆弱性が指摘されており，様々な鍵回復攻撃が提案されている．

3 鍵回復攻撃

本章では WEP の脆弱性を突いた鍵回復攻撃である Klein 攻撃および TeAM-OK 攻撃について示す．

3.1 Klein 攻撃

2006 年に Klein により IV に依存しない攻撃が提案された．それまで特定の IV を利用する攻撃方法は提案されていたが，Klein 攻撃では全ての IV を利用可能である．Klein 攻撃は IV とキーストリームの先頭 15 バイトを利用して WEP 鍵を先頭から 1 バイトずつ逐次的に回復する．RC4 の PRGA から KSA の内部状態の巻き戻しを行うことで鍵回復を行う．図 1 に Klein 攻撃における PRGA から KSA の巻き戻す内部状態の概要を示す．

まず，PRGA の内部状態の推測について示す．S_i^* は i ラウンド目のにおける PRGA の内部状態を表し，Z_i は i 番目のキーストリームを表す．キーストリームから PRGA の内部状態の値を推測するときの確率は次式で与えられる．

$$P|(Z_i + S_i^*[j] \bmod 256) = c| = \begin{cases} \frac{2}{N} \ (c = i) \\ \frac{N-2}{N\cdot(N-1)} \ (c \neq i) \end{cases} \quad (1)$$

式 (1) より次式が得られる．

$$S_i^*[j] = i - Z_i \quad (2)$$

式 (2) が成立する確率は $2/N$ である．PRGA のアルゴリズムより次式が得られる．

$$S^*_{i-1}[i] = S^*_i[j] \tag{3}$$

式 (3) の成立する確率は 1 である．

次に PRGA の内部状態から KSA の内部状態を推測する．KSA における i ラウンド目のにおける内部状態を S_i と表す．PRGA における内部状態 $S^*_{i-1}[i]$ が KSA における内部状態 $S_{i+1}[i]$ までスワップされないことを利用すると次式が得られる．

$$S_{i+1}[i] = S^*_{i-1}[i] \tag{4}$$

式 (4) の成立する確率は $((N-1)/N)^{N-2}$ である．KSA のアルゴリズムより二つの式が得られる．

$$S_i[j_{i+1}] = S_{i+1}[i] \tag{5}$$

$$j_{i+1} = j_i + S_i[i] + K[i \bmod 16] \tag{6}$$

式 (5)，(6) の成立する確率はそれぞれ 1 である．ここで，j_i は KSA における i ラウンド目のポインタ j の値を表す．式 (1)-(6) から Klein 攻撃の関係式は，

$$\begin{aligned} K[y] &= f_{Klein}(K[0], \ldots, K[y-1], Z_y) \\ &= S_y^{-1}[y - Z_y] - j_y - S_y[y] \end{aligned} \tag{7}$$

で表わすことができる．$S^{-1}[y]$ は内部状態が y となるときのポインタを表す．式 (7) の成立する確立は次式で得られる．

$$\begin{aligned} P_{Klein} &= \left(\frac{N-2}{N}\right)^{N-2} \cdot \frac{2}{N} + \\ &\quad \left(1 - \frac{N-1}{N}\right) \cdot \frac{N-2}{N \cdot (N-1)} \\ &\simeq \frac{1.36}{N} \end{aligned}$$

Klein 攻撃は逐次的に WEP 鍵を回復する．逐次的に求めるため WEP 鍵のあるバイトの推定を誤った場合，それ以降の WEP 鍵の推定も誤ってしまう．その場合鍵回復に必要となる計算量が大幅に増加する可能性がある．よって Klein 攻撃は WEP 鍵間の依存性が非常に大きい攻撃であるといえる．

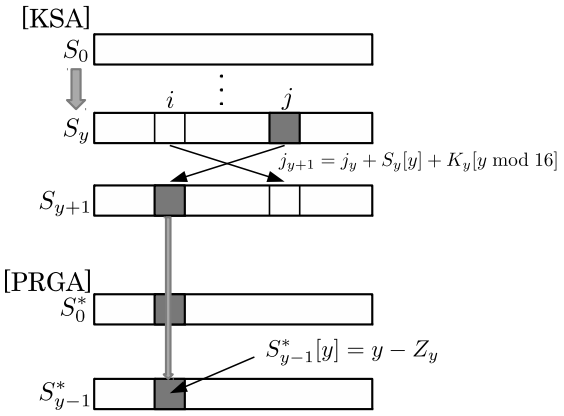

図 1: Klein 攻撃の内部状態巻き戻しの概要

3.2 TeAM-OK 攻撃

2010 年に寺村らは PTW 攻撃を改良した TeAM-OK 攻撃を提案した．TeAM-OK 攻撃は 3 つの攻撃 (Klein 攻撃，PTW 攻撃，OKM 攻撃) を利用する．PTW 攻撃と OKM 攻撃の関係式を示す．

$$\begin{aligned} \sigma[y] &= f_{PTW}(K[0], K[1], K[2], Z_y) \\ &= S_3^{-1}[y - Z_y] - j_3 - \sum_{l=3}^{y} S_3[l] \end{aligned}$$

$$K[y-16] = f_{OKM}(K[0], \ldots, K[y-17], \sigma_{15}, Z_y)$$

PTW 攻撃は IV に依存しない攻撃であり，IV とキーストリームのみを利用して WEP 鍵の和を回復する．WEP 鍵の和を求めるため WEP 鍵のあるバイトの推定を誤ったとしてもそれ以降の WEP 鍵に影響を与えない．

OKM 攻撃は IV と σ_{15} とキーストリーム先頭 19 バイト目から 31 バイト目までを利用して WEP 鍵を逐次的に回復する．OKM 攻撃は WEP 鍵の総和が既知という条件下で適用することが可能であり，下位のキーストリームから高い確率で鍵回復を行うことができる．

また寺村らは Klein 攻撃において誤った鍵を導出した場合，再度同じ処理をするのではなく，鍵の差分を導出することで計算量を減らす方法を提案した．差分の関係式を次式に示す．

$$\begin{aligned} \Delta K[y] &= KT_i[y] - KT_{top}[y] \\ K[y] &= KT_i[y] - \Delta K[y] \end{aligned} \tag{8}$$

ここで $KT_i[y]$ は鍵 y バイト目の投票テーブルで上から i 番目の値を表す．KT_{top} は投票テーブルで上から 1 番目の値を表す．

TeAM-OK 攻撃はキーストリームにより Klein 攻撃，PTW 攻撃および OKM 攻撃使い分けて投票テーブルを作成し，式 (8) を用いて正しい鍵の値を導出する．約 50, 000 個の IP パケットを取得することで確率 0.9 で鍵回復することができる．以下に簡単な攻撃アルゴリズムを示す．詳しいアルゴリズムは文献 [5] に記載されている．

Step.1 σ_{15} の導出
Klein 攻撃により $K[12]$ までの仮鍵を求め，内部状態を更新していくことで近似範囲を可能な限り少なくする．更新した内部状態を利用して PTW 攻撃を適用し，σ_{15} を導出する

Step.2 各鍵バイト毎に投票テーブルを作成
Klein 攻撃と σ_{15} を用いて OKM 攻撃を利用して得られた鍵の候補値に投票を行い，投票テーブルを作成する

Step.3 正しい鍵の導出
Step.2 で得られた投票テーブルから秘密鍵の候補を推定し，正しい鍵か RC4 に入力して暗号化を行うことで確認する．誤った鍵であった場合はパケット数を増やして *Step*.1 から同様に行うことで正しい鍵を導く

4 少数パケットによる鍵回復攻撃

取得できるパケット数が制限された環境において WEP の安全性評価を行う．30, 000 個以下の IP パケットに対して鍵回復に必要な計算量を求める．鍵回復の成功確率をあげるため WEP 鍵の $K[13]$，$K[14]$ を全数探索で求める．またパケット数が少ないため可能な限り攻撃関数のもっとも高い確率で鍵の候補を求める必要がある．そこで攻撃アルゴリズムで導出する σ_{15} も全数探索で求める．正しい σ_{15} を利用することで $K[15]$ を特定することができる．また OKM 攻撃を効率よく適用することができる．図 2 に鍵回復に必要な計算量とパケット数の関係について示す．

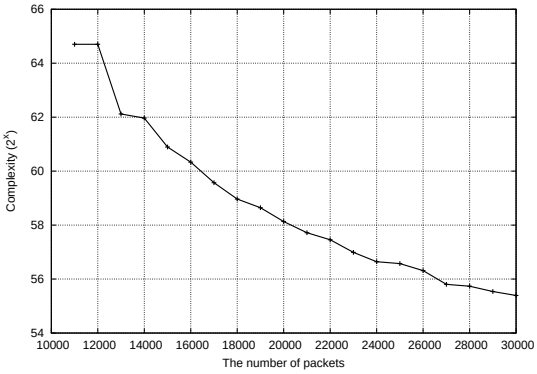

図 2: パケット数と計算量の関係

図 2 から 18, 000 個の IP パケットを用いた場合 2^{58} 程度の計算量で鍵回復することができる．よって取得できるパケット数が制限された環境においても探索範囲を拡張することで鍵回復が可能であることがわかる．

5 まとめ

本稿では取得可能な IP パケット数が制限された環境下における WEP の安全性評価を行った．TeAM-OK 攻撃を用いて 30, 000 パケット以下の場合に WEP 鍵の回復に要する計算量を導出した．結果としてパケット数が 20, 000 個以下であっても，探索範囲を拡張することで WEP 鍵の解読に成功した．したがって WEP を少ないパケット数で秘密鍵を更新して利用する場合でも鍵回復が成功する可能性があると考えられる．今後は鍵探索の手法及び攻撃関数を少ないパケット数に対して最適化することで計算量を 2^{48} 以下に低減することを考える．

参考文献

[1] IEEE Computer Society, “Wireless lan medium access control (MAC) and physical layer (PHY) specifications,” IEEE Std 802.11, 1999.

[2] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4," *SAC*, Lecture Notes in Computer Science, vol2259, pp.1-24, SpringerVerlag, 2001.

[3] A. Klein, "Attacks on the RC4 stream cipher," *Designs, Codes, and Cryptography*, vol.48, no.3, pp.269-286, 2008.

[4] E. Tews, R.P. Weinmann, and A. Pyshkin, "Breaking 104 bit WEP in less than 60 seconds," *WISA*, Lecture Notes in Computer Science, vol.4867, pp.188-202, SpringerVerlag, 2008.

[5] R. Teramura, Y. Asakura, T. Ohigashi, H. Kuwakado, and M. Morii, "Fast WEP-key recovery attack using only encrypted IP packets," *IEICE Trans Fundamentals*, vol.E93A, no.1, pp.164-171, 2010.

[6] P. Sepehrdad, P. Susil, S. Vaudenay, and M. Vuagnoux, "Smashing WEP in A Passive Attack," *FSE*, 2013.

[7] A. Frier, P. Karlton, and P. Kocher,: The SSL 3.0 protocol, Netscape Communications Corp, Vol.18, p.2780, 1996.

[8] W. Alliance: Wi-Fi protected access, available at http://www.weca.net/open section/prote ctedaccess.asp, 2003.

[9] T. Ohigashi, H. Kuwakado, and M. Morii, A Key Recovery Attacks on WEP with Less Packets," *Technical Report of IEICE*, ISEC2007-109, pp.61?68, Nov. 2007.