ストリーム暗号および無線LAN暗号技術の安全性に関する研究

渡邉, 優平

(Degree)
博士（工学）

(Date of Degree)
2017-03-25

(Date of Publication)
2018-03-01

(Resource Type)
doctoral thesis

(Report Number)
甲第6922号

(URL)
https://hdl.handle.net/20.500.14094/D1006922

博 士 論 文

ストリーム暗号および無線LAN暗号技術の安全性に関する研究

平成29年1月

神戸大学大学院工学研究科
渡 辺 優 平

内容梗概

通信技術の発達に伴い，音楽や動画などの大容量データを通信路上でやりとりする機会が増加している．それらのデータをリアルタイムに暗号化して保護するためには，高速に処理可能な暗号技術が必要である．高速な暗号方式の 1 つにストリーム暗号がある．ストリーム暗号は秘密鍵と初期化ベクトル (IV:Initialization Vector) から取得したセッション鍵あるいは秘密鍵自体をシードとして生成した擬似乱数列 (キーストリーム) と平文との排他的論理和を計算することにより暗号化を行う方式である．一般的にストリーム暗号の安全性はキーストリームの乱数性やキーストリームに関する情報から秘密鍵を復元する方法 (鍵回復攻撃) などの解読法に関して解析を行うことによって評価される．キーストリームの乱数性が不十分であれば，平文回復攻撃や鍵回復攻撃に発展する場合がある．もし鍵回復攻撃において鍵の全数探索以下の計算量で実行可能な解読法が発見された場合，その暗号は安全でないと判断される．一方で実際の通信において，通信されている暗号文から平文が復元された場合，その通信方式における暗号は安全でないと考えられる．このように実用および理論の両面から暗号の安全性が評価されている．

本論文ではストリーム暗号の安全性に着目する．一般的に暗号はアルゴリズムをもとに特性が解析される．発見された特性を利用して，実用的な仮定における安全性が評価される．よって暗号アルゴリズムに基づいた理論的な解析と実用的な観点からの解析の両方に着目する．実用的な解析対象として，ストリーム暗号 RC4 に着目する．RC4 は最も有名な暗号の 1 つであり，様々な商用アプリケーションや SSL/TLS，無線 LAN 暗号化方式 WEP. WPA などで利用されている．RC4 はこれまでさまざまな解析が行われており，キーストリームとして出力される値の発生確率に統計的な偏り (bias) が多く存在することが知られている．さらに Broadcast setting において，それらの bias を利用した平文回復攻撃，鍵回復攻撃，識別攻撃などが提案されている．Broadcast setting は同一の平文を複数の異なる秘密鍵で暗号化し，送信する場合を指す．WEP では暗号化に RC4 をベースとしたストリーム暗号が用いられている．秘密鍵の一部を IV として利用し，その情報を公開値として送信することが WEP の脆弱性となっている．この脆弱性を利用して多数の鍵回復攻撃が提案されている．暗号アルゴリズムに基づいた解析対象として，非線形帰還シフトレジスタ (NLFSR:Non-Linear Feedback Shift Register) を用いて構成されたストリーム暗号に着目する．NLFSR 型のストリーム暗号はレジスタに秘密鍵と IV を直接入力するため，秘密鍵や IV に差分を入力してキーストリームに対する差分特性の解析が行われている．差分特性の解析の際に，秘密鍵や IV の値に条件を設定することで，特徴的な差分特性の解析が行われる．発見された差分特性を利用して識別攻撃や鍵回復攻撃が提案されている．実用的なものとアルゴリズムに基づいたもののそれぞれに着目することで，暗号化技術の安全性に寄与することを考える．

初めに SSL/TLS 環境下を想定した RC4 に対する平文回復攻撃を提案する．RC4 のキー

ストリームには 1 バイト単位の bias と 2 バイト単位の bias が存在する．従来の平文回復攻撃ではこれらのどちらかのみが利用されている．2 バイト単位の bias を利用した攻撃については異なる種類の bias を効率的に併用する手法が提案されている．本研究ではこの手法に着目し，1 バイト単位の bias と 2 バイト単位の bias を効率的に併用する方法を提案する．異なる種類の bias を効率的に併用することで，平文回復攻撃の効率化を図る．結果として SSL/TLS 環境を想定した条件下において，8 バイトの平文を従来より効率的に復元できる．

次にファームウェアの更新のみで WEP を安全に利用する方法を提案する．無線 LAN 暗号化方式の一つである WEP は多数の鍵回復攻撃が提案されており，より安全な方式への移行が推奨されている．しかし機器の入れ替えコストの問題や利用者のセキュリティ意識の欠如から未だに利用されている．WEP に対する鍵回復攻撃は特定の脆弱な IV(weak IV) や IV とキーストリームの間の統計的性質に基づいて構築されている．したがって weak IV や統計的性質が成立する IV を取り除くことで，安全に WEP を利用することができると考えられる．本論文では WEP に対する鍵回復攻撃を妨げる IV を改良 Strong IV と呼び，改良 Strong IV の定義と通信のスループットへの影響を低減した利用方法を提案する．結果として，改良 Strong IV を利用することで WEP を安全かつ高速に利用することができる．

NLFSR 型のストリーム暗号について新しい条件付差分特性の探索手法を提案する．ストリーム暗号はキーストリームの乱数性を得るために，秘密鍵と IV に対して鍵初期化という処理を行い，それぞれの情報を撹拌したのち，キーストリームを生成する．NLFSR 型のストリーム暗号は一般的に鍵初期化処理の巻き戻しが可能である．従来より攻撃が困難な仮定において，この性質を利用した条件付差分特性の探索手法を提案する．提案手法を NLFSR 型ストリーム暗号 Grain v1 に適用し，識別攻撃および鍵回復攻撃を実行する．Grain v1 はヨーロッパを中心とした次世代のストリーム暗号選定プロジェクトである eSTREAM において，ハードウェア暗号に選択されており，最も有名な NLFSR 型ストリーム暗号の一つである．結果として，weak key setting において，114 段の Grain v1 について現実時間で実行可能な識別攻撃および鍵回復攻撃が確認できた．

目 次

図 目 次

表 目 次

第1章　序論

近年オンラインバンクや電子商取引などのオンラインサービスの増加に伴い，個人情報やパスワードといった機密情報をインターネット上で通信する機会が増加している．これらの情報を安全に通信するために，ネットワーク上の通信は全て暗号化の処理が行われている．またブロードバンドネットワークの普及やユビキタス環境の整備により，動画像や音楽などのコンテンツのストリーミング配信が可能になるなど，大容量のデータが頻繁にネットワーク上で通信されている．このような大容量のデータの通信には高速な処理が求められている．高速に処理が可能な暗号方式としてストリーム暗号の研究が盛んに行われている．ストリーム暗号方式は秘密鍵，あるいは秘密鍵と初期化ベクトル (IV:Initilization Vector) をシードとして生成したキーストリームと呼ばれる擬似乱数列と平文との排他的論理和を計算することにより暗号化を行う方式である．ここで IV は暗号化処理ごとに変化する公開値である．ストリーム暗号はシードの値を初期化する鍵初期化部と，初期化されたシードからキーストリームを生成する擬似乱数生成部から構成される．ストリーム暗号方式は処理がシンプルであるため，高速化が容易である．そのため，リアルタイムの暗号化および大容量データの暗号化に適した方式である．

一般に暗号はアルゴリズムを公開した上で，各種解読法の議論を受けることにより安全性が評価される．長期間議論されて有効な解読法が発見されない場合，その暗号は安全であると評価される．このように，暗号解読研究は暗号の安全性を評価する上で，非常に重要な研究である．ストリーム暗号では攻撃者がキーストリームの一部を得られるという条件において解読法が議論される．通常，ストリーム暗号の安全性はキーストリームの乱数性に関する評価 (識別攻撃，予測攻撃)，キーストリームから秘密鍵や内部状態の初期値を復元する手法に関する評価 (鍵回復攻撃，内部状態推定攻撃) によって議論される．識別攻撃はキーストリームと真性乱数系列を区別する攻撃である．予測攻撃は一部のキーストリームからそれ以外の部分のキーストリームを高確率で予測する攻撃である．これらは直接的な脅威とはならないが，ストリーム暗号の潜在的な脆弱性を指摘し，鍵回復攻撃や内部状態推定攻撃に発展するものである．鍵回復攻撃はキーストリームの一部から秘密鍵を復元する攻撃である．内部状態復元攻撃はキーストリームの一部から初期状態を復元する攻撃である．これらの攻撃が成立する場合，攻撃者はキーストリームを全て計算でき，復号と同様の処理によって暗号文全体を解読できる．

1.1　ストリーム暗号および無線 LAN 暗号技術の解析

本研究では，共通鍵暗号の一種であるストリーム暗号の安全性評価を行う．一般的にストリーム暗号は，そのアルゴリズムをもとにした解析により攻撃に用いる特性の評価が行われる．さらに発見された特性を用いて実用的な仮定における安全性が評価される．よっ

て理論的な解析と実用的な解析の両方が必要となる．そこで暗号の利用環境に基づいた安全性と暗号アルゴリズムに基づいた安全性それぞれに着目して評価することを研究テーマとする．暗号の利用環境に基づいた安全性評価により，実際に利用されている通信システムの安全性を解析する．暗号アルゴリズムに基づいた安全性評価により，暗号が持つ特性や脆弱性を明らかにすることができる．発見した暗号が持つ特性によって，通信システムなどにおける暗号の安全性や類似した構造を持つ暗号アルゴリズムの解析に寄与すると考えられる．

暗号の利用環境に基づいた安全性評価として，SSL/TLS における RC4 および無線 LAN 暗号化方式である WEP を解析する．暗号アルゴリズムに基づいた解析として，非線形帰還シフトレジスタ (NLFSR:Non-Linear Feedback Shift Register) によって構成されたストリーム暗号に対する新しい条件付差分解読法を提案する．

1.1.1 SSL/TLS における RC4 に対する平文回復攻撃

RC4 は商用アプリケーションや暗号化通信プロトコルである SSL(Secure Sockets Layer) [1] / TLS(Transport Layer Security) [2]，無線 LAN 用のプロトコルである Wired Equivalent Privacy(WEP) [3] および Wi-Fi Protected Access(WPA) などで利用されている．RC4 に関しては，過去 20 年間で多くの解析が行われてきた．そして 2013 年に SSL/TLS における RC4 に対する現実的な平文回復攻撃が AlFardan ら [4] と五十部ら [5] によって提案された．これらの結果により，RC4 の利用は大幅に減少した．しかしながら，Trustworthy Internet Movement の調査 [6] によると，依然として SSL/TLS 上で RC4 が利用されており，その安全性を評価する意義は大きい．

RC4 のキーストリームは乱数性に問題があり，多くの統計的な偏り (bias) が報告されている [7, 8, 5, 9, 10, 11, 12, 13]．統計的な偏りとして 1 バイト単位の bias(single-byte bias) と 2 バイト単位の bias(double-byte bias) が存在する．RC4 に対する平文回復攻撃は，1 つの平文を複数の異なる秘密鍵で暗号化して送信する Broadcast setting において，これらの統計的性質を利用することで構成される．しかしながら，従来の攻撃は 1 バイト単位の bias か 2 バイト単位の bias のどちらか一方のみを利用しており，両方を同時に利用した攻撃は存在しない．

本研究では，1 バイト単位の bias と 2 バイト単位の bias の両方を利用した平文回復攻撃を提案する．それぞれの bias から独立に算出した平文の候補の尤度を効率的に集約し，集約したものから平文の推測を行う．提案手法により，既知平文に含まれる連続した秘密情報を復元する場合において，2^{29} のランダムに選択した鍵で暗号化された暗号文から全ての復元対象の平文を従来より高い確率で復元することができる．

1.1.2 WEP の安全性向上

WEP は RC4 をベースとした共通鍵暗号方式である．RC4 の秘密鍵の一部を IV として利用する仕様が WEP の脆弱性となっており，数多くの鍵回復攻撃が提案されている [14, 15, 16, 17, 18, 19]．そのため，より安全性の高い Wi-Fi Protected Access2(WPA2) [20] などの暗号化方式への移行が推奨されている．しかしながら，機器の入れ替えコストや安

全性に関する意識の問題から，現在でも WEP は利用されている．従来の機器のファームウェアを更新することで導入可能な安全性向上手法が求められている．

WEP に対する鍵回復攻撃は脆弱な IV(weak IV) に依存する攻撃と，IV とキーストリームの間の統計的性質を利用した攻撃が存在する．weak IV に依存する攻撃の対策としては，weak IV を通信から取り除く手法が提案されている [21]．統計的性質を利用した攻撃の対策としては，一定の間隔で秘密鍵を更新することが考えられる．しかしながら，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．鍵の更新間隔を延長する手法として，塚畝らにより Strong IV が提案されている [22]．Strong IV は Klein 攻撃が成立しない IV の集合を指す．しかし，Strong IV の具体的な生成方法や安全性に関する議論が不十分であった．

本研究では，安全な WEP の運用方法を提案する．従来の全ての鍵回復攻撃を防ぐ IV の集合を改良 Strong IV と定義し，その効率的な生成方法を提案する．さらに，改良 Strong IV を用いた安全な WEP の運用方法について議論を行う．提案手法により，100,000 パケットの通信において高速かつ安全に WEP を運用することができる．

1.1.3 NLFSR 型ストリーム暗号に対する条件付差分解読法

NLFSR で構成されたストリーム暗号については，次世代のストリーム暗号選定会議 eSTREAM で選定された Grain v1[23] や Trivium[24] などが存在する．これらのストリーム暗号は今後利用が広がると考えられるため，事前に安全性を評価する意義は大きい．

NLFSR 型ストリーム暗号の解析手法として Cube attack や条件付差分解読法 [25] が提案されている．条件付差分解読法は Knellwolf らによって提案された攻撃で，様々な NLFSR 型の暗号に適用されている．NLFSR 型のストリーム暗号は一般的に鍵初期化処理の巻き戻しが可能である．条件付差分解読法は，複数の関連する秘密鍵を用いて解析を行う関連鍵設定において，この性質を利用している．関連鍵設定は攻撃者に有利な仮定であり，より現実的な仮定で鍵初期化の性質を利用することを考える．

本研究では，NLFSR 型ストリーム暗号に対する新しい条件付差分解読法を提案する．関連鍵の仮定なしに，鍵初期化の逆方向の解析を行う方法について述べる．具体的には，逆方向の解析において差分の拡散を妨げるように条件を決定し，条件付差分特性を探索する．鍵初期化の順方向の解析と組み合わせることで，鍵初期化部全体に対する条件付差分特性を得る．提案手法は，初期状態における条件が増加するため，弱鍵の仮定のもとで有効な解読法となる．

提案手法を Grain v1 に適用し，識別攻撃および鍵回復攻撃を提案する．提案手法により 2^{40} 個の弱鍵および条件付 IV の領域を持つ，条件付差分特性が得られる．条件付差分特性から，114 段の Grain v1 に対して 2^{32} 個の選択 IV を用いた識別攻撃が確認できる．さらに，秘密鍵と IV が関連する条件と識別攻撃の成立の関係から，鍵の情報が 1 ビット得られる．したがって，2^{33} の計算量で 1 ビットの鍵回復攻撃が成立する．さらに残りの 40 ビットの weak key を全数探索することで，41 ビットの鍵が計算量 $2^{40.01}$ で復元できる．

1.2 論文構成

本論文の構成は以下の通りである．第 2 章では，ストリーム暗号の構成およびその安全性評価について述べる．第 3 章では，第一の研究テーマとして SSL/TLS 環境下における RC4 に対する平文回復攻撃について述べる．第 4 章では，第二の研究テーマである無線 LAN 暗号化方式 WEP の安全性向上手法を提案する．第 5 章では，第三の研究テーマとして NLFSR 型ストリーム暗号に対する新しい条件付差分解読法を提案する．最後に，第 6 章では，結論として研究成果をまとめる．

第2章　ストリーム暗号

本章では暗号理論に関する基礎知識について述べる．初めに共通鍵暗号方式について述べ，その一種であるストリーム暗号方式とその安全性の評価方法について説明する．

2.1　ストリーム暗号の構造

ストリーム暗号は平文をシンボルと呼ばれる小ビット単位ごとに逐次的に暗号化する方式であり，1 ビットや 1 バイト単位で暗号化するアルゴリズムが多い．ストリーム暗号は秘密鍵，あるいは秘密鍵と IV をシードとした擬似乱数生成器にによって平文と同じ長さのキーストリームと呼ばれる擬似乱数列を生成する．キーストリームと平文の排他的論理和を計算することで暗号化を行う．復号の際には，暗号化で用いられたものと同様のキーストリームを生成し，暗号文とキーストリームのの排他的論理和を計算する．平文を $P = P_1, P_2, \ldots$，暗号文を $C = C_1, C_2, \ldots$，キーストリームを $Z = Z_1, Z_2, \ldots$ とすると暗号文は

$$C_r = P_r \oplus Z_r \ \ (r = 1, 2, \ldots)$$

で与えられる．復号は同様の操作で，

$$P_r = C_r \oplus Z_r \ \ (r = 1, 2, \ldots)$$

となる．図 2.1 にストリーム暗号のモデルを示す．

一般にストリーム暗号は 1 つの秘密鍵からは一通りのキーストリームしか生成できない．そのため IV と呼ばれる公開値を利用し，暗号化処理ごとに異なるキーストリームを生成する．IV を変化させることにより 1 つの秘密鍵から複数のパターンのキーストリームを生成することが可能となる．

ストリーム暗号のアルゴリズムは鍵初期化部と擬似乱数生成部の 2 つにより構成される．鍵初期化部は秘密鍵と IV を用いて擬似乱数生成器の内部状態を初期化するアルゴリズムである．擬似乱数生成部は初期化された内部状態を利用して，状態を更新しながらキーストリームを生成するアルゴリズムである．

2.2　ストリーム暗号の安全性評価

一般的に暗号の安全性はアルゴリズムを公開した上で，暗号の研究者による解読法の議論を受けることで安全性が評価される．長い間議論され，解読方法が見つからない場合は安全な暗号として評価される．ストリーム暗号の安全性は擬似乱数列であるキーストリー

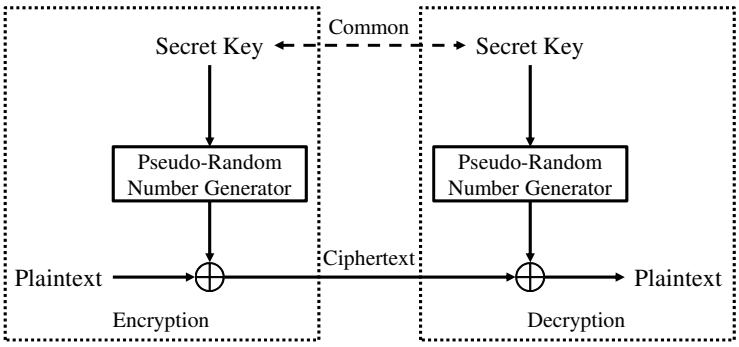

図 2.1: ストリーム暗号

ムの安全性に根拠を置くことになる．暗号解読者が平文の一部を知ることができたとき，それ以外の平文や秘密鍵の情報を知ることができるなら，その暗号は安全なストリーム暗号ではない．暗号解読者は平文と暗号文が既知であるという条件のもとで，次式よりキーストリームの一部を得ることができる．

$$P_r \oplus C_r = P_r \oplus (P_r \oplus Z_r) = Z_r$$

そのためストリーム暗号の安全性評価は攻撃者が既知平文攻撃 (攻撃者が選択不可能な既知の平文に対応する暗号文を入手できる条件で，暗号文から平文を求める攻撃) を実行可能な環境を想定する．攻撃者はストリーム暗号の出力であるキーストリームを十分に入手可能であることを前提に攻撃を行う．したがって，安全性の評価はキーストリームに対して行う．

暗号としての評価基準となる攻撃が総当たり攻撃 (Brute Force Attack) である．総当たり攻撃とは鍵の候補を全て試すことで暗号化に用いられた鍵を特定する攻撃方法である．現在の暗号において，攻撃者は総当たり攻撃を行うことで必ず暗号を解読することができる．ただし一般に暗号は鍵長を長く設定することにより，この攻撃に対して十分な安全性を持つように設計されている．例えば秘密鍵の鍵長が 128 ビットである場合，攻撃者は総当たり攻撃で鍵を導出するためには 2^{128} 個の鍵の候補全てを用いて暗号化を行う必要がある．しかしながら現在の計算機では現実的な時間で 2^{128} 回の暗号化を試行することは不可能であるため，計算量的安全性を有するように設計されており，総当たり攻撃は脅威とならない．

ストリーム暗号に対する攻撃手法は以下の 4 つに分類される．図 2.2 に 4 つの攻撃手法を示す．

1. 識別攻撃 (Distinguishing Attack)：真性乱数と擬似乱数生成器からの出力であるキーストリームを区別する．

2. 予測攻撃 (Prediction Attack)：ランダムに予測するよりも高い精度でキーストリームを予測する．

3. 鍵回復攻撃 (Key Recovery Attack)：キーストリームから秘密鍵を導出する．

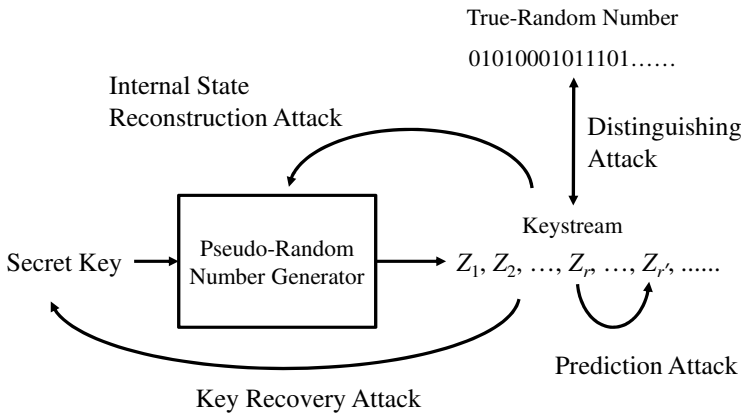

図 2.2: ストリーム暗号に対する攻撃

4. 内部状態推定攻撃 (Internal State Reconstruction Attack)：キーストリームから内部状態の初期値を復元する．

識別攻撃は現実的な脅威となる攻撃方法ではないが，キーストリームの乱数性を計る基準として用いられ，他の攻撃に発展する可能性を示す．予測攻撃が実現すれば，一部のキーストリームから他の部分のキーストリームが分かることになり，暗号文を平文に戻すことが可能となる．鍵回復攻撃が実現すれば，暗号化アルゴリズムを用いてキーストリームを生成することができ，全ての暗号文を平文に戻すことが可能となる．内部状態復元攻撃が実現すれば，秘密鍵と等価な内部状態の初期値が分かることになり，全ての暗号文を平文に戻すことが可能となる．これらの攻撃が秘密鍵の総当たり攻撃に要する計算量より小さい計算量で攻撃が実行できるとき，その攻撃は成功したとみなされる．

識別攻撃の具体例として差分を用いた手法が存在する [25]．あるストリーム暗号の初期状態を X とおく．初期状態 X にある差分を入力したものを X' とおく．状態 X および X' から生成したキーストリームをそれぞれ Z_0，Z_0' とする．キーストリームの差分 ΔZ_0 を Z_0 と Z_0' の排他的論理和から得る．多数の異なる X と X' のペアから ΔZ_0 を取得し，その値の偏りを観測する．ΔZ_0 の値に偏りが確認された場合，真性乱数ではないと判断されるため，識別攻撃が成立する．

2.3 攻撃の仮定

暗号の解析は，攻撃者が得られる情報や秘密鍵などについて様々な仮定に基づいて行われる．ストリーム暗号に対する攻撃における平文および暗号文の仮定として，以下の 4 つが考えられる．

1. 暗号文単独攻撃 (Ciphertext only attack)：攻撃者が暗号文のみを得られる状況で解析を行う．

2. 既知平文攻撃 (Known plaintext attack)：攻撃者が平文とそれに対応する暗号文のペアを知っている状況で解析を行う．

3. 選択平文攻撃 (Chosen plaintext attack) : 攻撃者が任意に選択した平文とそれに対応する暗号文から解析を行う.

4. 選択暗号文攻撃 (Chosen ciphertext attack)：攻撃者が暗号文を選択して復号し，それに対応する平文を知っている状況で解析を行う.

暗号文単独攻撃を除いた上記の仮定において，平文と暗号文の排他的論理和をとることでキーストリームを得ることができる.

IV に関する仮定を用いた攻撃として，選択 IV 攻撃が考えられる．これは攻撃者が IV の値を選択することができるという仮定のもとで，解析を行う.

秘密鍵に関する仮定として，以下の 3 つが考えられる.

1. 単一鍵設定 (Single-key setting)：単一の鍵に対して解析を行う.

2. 弱鍵設定 (Weak-key setting)：秘密鍵に一定の条件を課した状態で解析を行う.

3. 関連鍵設定 (Related-key setting)：複数の関連する秘密鍵を利用して解析を行う.

Related-key setting の例として，一定の差分を持つ秘密鍵のペアを利用した解析が考えられる.

第3章　SSL/TLS環境下におけるRC4に対する平文回復攻撃

3.1　緒言

RC4は1987年にRivestによって設計されたストリーム暗号である，最も広く利用されている暗号の1つである．過去20年間で，RC4に対して多くの解析が行われてきた．最終的に2013年に，SSL/TLSにおけるRC4に対する現実的な平文回復攻撃がAlFardanら[4]と五十部ら[5]によって提案された．これらの結果により，RC4の利用は大幅に減少した．特にTLSにおいてGoogleやMicrosoft，Mozillaはウェブブラウザから RC4を削除したことを，2016年初頭に公式に発表した．しかしながらTrustworthy Internet MovementのSSL Pulseによると，依然としてSSL/TLSの暗号化にRC4が利用されている[6]．また，リモートデスクトッププロトコルなどのシステムにおいてRC4がサポートされている．これは古いシステムにおける暗号技術の入れ替えにはコストがかかるためである．

これまで提案された全ての平文回復攻撃[7, 5, 4, 26, 27, 28, 29, 30, 8]はキーストリームの初期257バイトのsingle-byte bias[7, 10, 9, 5, 29, 11, 8]やFluhrer-McGrew bias (FM00 bias) [12]やMantinのbias (*ABSAB* bias) [13]．Vanhoefらのbias [27]といったdouble-byte biasを利用している．double-byte biasはキーストリームの全体に存在する，一方でsingle-byte biasは初期257バイトといった特定のバイトにのみ存在する．

五十部らは初めてbroadcast settingにおけるRC4の平文全体を復元する攻撃を示した．ここでbroadcast settingとは同一の平文を異なる秘密鍵で暗号化することを指す．この攻撃では最も強いsingle-byte bias[5, 29]と*ABSAB* biasを利用して平文の先頭257バイトと258バイト目以降をそれぞれ復元する．AlFardanらは全てのsingle-byte biasを効率的に利用する方法と，一定の長さの平文が繰り返し暗号化されるという仮定のもとでFM00 biasを用いた攻撃を示した[4]．この攻撃では全てのsingle-byte biasを利用するために多項分布による尤度の算出を行っている．大東らはFM00 biasと*ABSAB* biasの二種類のdouble-byte biasを用いたguess-and-determine攻撃を提案した．これらの攻撃は平文の値がランダムに分布していると仮定している．パスワードなどに平文の分布を制限した場合，より効率の良い攻撃が提案されている．GarmanらはFM00 biasを用いたパスワード復元攻撃を提案している[28]．Vanhoefらは二種類のdouble-byte biasを組み合わせることで平文回復攻撃を改良している[27]．表3.1に従来の結果をまとめる．

キーストリームのbiasは鍵回復攻撃にも利用される．Sepehrdadらは2010年にRC4に対する鍵回復攻撃を提案した[9]．weak keyに基づく鍵回復攻撃も提案されている．weak keyとは全数探索より効率よくキーストリームから復元可能な鍵のクラスを指す．RoosがRC4におけるweak keyの存在を示し[31]，寺村らによってweak keyが拡張された[32]．2014年に長尾らが寺村らのweak keyを拡張し，鍵回復攻撃を提案した[33]．WEPに対す

表 3.1: RC4 に対する平文回復攻撃の結果

平文の状態	Bias	暗号文数	成功確率	Target 対象の平文	参考
ランダムに分布	Single-byte	2^{32}	0.8	先頭 257 バイト	[5]
ランダムに分布	Single-byte	2^{32}	1.0	先頭 256 バイト	[4]
ランダムに分布	Double-byte	2^{34}	1.0	258 バイト以降	[5]
ランダムに分布	Double-byte	$13 \cdot 2^{30}$ (= $2^{33.70}$)	0.5	16 バイトの cookie	[4]
ランダムに分布	Double-byte	2^{35}	1.0	全て	[26]
ランダムに分布	Single-byte	2^{29}	0.882	先頭 257 バイト中の 8 バイト	[4]*1
ランダムに分布	Single-byte and Double-byte	2^{29}	0.961	先頭 257 バイト中の 8 バイト	Our*1
ランダムに分布	Single-byte	2^{29}	0.0136	先頭 257 バイト中の 8 バイト	[4]*2
ランダムに分布	Single-byte and Double-byte	2^{29}	0.0357	先頭 257 バイト中の 8 バイト	Our*2
Cookie	Double-byte	$9 \cdot 2^{27}$ (= $2^{30.17}$)	0.94	16 バイトの cookie	[27]
Password	Single-byte	2^{28}	0.75	先頭 120 バイト中の 6 バイト	[28]
Password	Double-byte	2^{26}	0.78	先頭 48 バイト中の 6 バイト	[28]

*1 平文の 113 から 120 バイト目を復元する場合の結果.
*2 平文の 201 から 208 バイト目を復元する場合の結果.

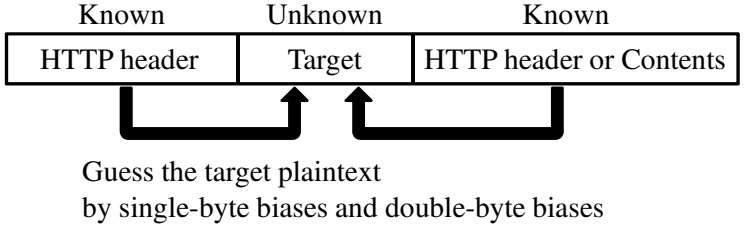

図 3.1: 復元対象の平文に関する仮定

る鍵回復攻撃も研究されている [14, 15, 16, 17, 18]．2007 年に Vaudenay らによって強力な攻撃が提案された [34]．この攻撃は後に Sepehrdad らによって改良された [19]．これらの攻撃は，RC4 のキーストリームにおける鍵が関係する bias に基いている．

従来の攻撃は全て single-byte bias か double-byte bias のどちらか一方を利用している．平文の推測に両方の bias を同時に利用することにより平文回復攻撃の効率化することができると考えられる．したがって，対象の平文を復元するために異なる種類の bias を効率的に利用する方法を考える．

本研究では平文の推測に single-byte bias と double-byte bias の両方を利用する攻撃を提案する．我々の攻撃では，それぞれの bias から独立に平文の候補の尤度を計算し，それを集約したものから平文の推測を行う．提案手法は Vanhoef らの二種類の double-byte bias を集約する手法を拡張したものである．一方で，single-byte bias と double-byte bias を集約する方法を新たに開発する．

提案手法の有効性を確認するために，図 3.1 示すように，既知平文に含まれれる連続した秘密情報を復元する場合を考える．例えば HTTPS のようにヘッダなどの容易に推測できる情報と cookie などの秘密情報が含まれる状態を仮定する．平文の値がランダムに分布していると仮定した場合，2^{29} のランダムに選択した鍵で暗号化された暗号文から全ての

Algorithm 1 RC4 Algorithm

KSA(K)**:**
  for $i = 0$ to $N - 1$ **do**
    $S[i] \leftarrow i$
  end for
  $j \leftarrow 0$
  for $i = 0$ to $N - 1$ **do**
    $j \leftarrow j + S[i] + K[i \bmod \ell]$
    Swap $S[i]$ and $S[j]$
  end for

PRGA(K)**:**
  $i \leftarrow 0$
  $j \leftarrow 0$
  $S \leftarrow KSA(K)$
  loop
    $i \leftarrow i + 1$
    $j \leftarrow j + S[i]$
    Swap $S[i]$ and $S[j]$
    Output $Z \leftarrow S[S[i] + S[j]]$
  end loop

復元対象の平文を従来のベストアタックより高い確率で復元することができる．表 3.1 に本研究の結果を示す．最も効率的な場合では，提案手法の攻撃成功確率は従来と比べて二倍以上となる．

我々の知る限り，single-byte bias と double-byte bias を併用して，RC4 の平文回復攻撃の効率化が可能であることを示した初めての結果である．

3.2 ストリーム暗号 RC4

RC4 は 1987 年に RSA Data Security 社の Ronald Rivest により開発された可変長鍵のストリーム暗号である [35]．RC4 はアルゴリズムを短いコードで記述できるため，ソフトウェアによる高速処理性能に優れている．そのため，Adobe Acrobat などの商用アプリケーションやインターネット用の暗号化通信プロトコルである SSL(Secure Sockets Layer)/TLS(Transport Layer Security) [1, 2]，無線 LAN 用のプロトコルである WEP(Wired Equivalent Privacy) および WPA(Wi-Fi Protected Access) などで広く利用されている．RC4 は開発されて以来，そのアルゴリズムは非公開であった．しかし 1994 年にソースコードがインターネット上に匿名で公開されたため，RC4 のアルゴリズムが一般に知られるようになった．ただし RSA Data Security 社は公開されたソースコードを公式に RC4 と認めておらず，公開されたコードは ARC4(Alleged RC4) や arcfour と呼ばれる RC4 と等価な動作をするアルゴリズムとして公開されている．本論文では ARC4 のアルゴリズムを RC4 とみなした上で安全性評価を行う．

RC4 のアルゴリズムを Algorithm 1 に示す．ここで + は N を法とした算術加算である．RC4 は KSA と PRGA の 2 つのアルゴリズムにより構成される．KSA では $N(= 2^n)$ 個の要素で構成される内部状態が秘密鍵を用いて初期化される．KSA において内部状態の初期化は各時刻で値が 1 づつ加算されるポインタ i と秘密鍵およびその時刻における内部状態により値が決定されるポインタ j が指す位置の値を繰り返しスワップすることで行われる．PRGA では内部状態を更新しながら 1 シンボル単位でキーストリーム $Z_1, Z_2, \ldots, Z_r, \ldots$ が生成される．ここで r は PRGA のラウンド数である．PRGA において内部状態の更新は KSA と同様にポインタ i とある時刻における内部状態により値が決定されるポインタ j が指す位置の値をスワップすることで行われる．ポインタ i，j はそれぞれ n ビットの値を持

表 3.2: ポインタ i (= r mod N) の条件と対応する FM00 bias

イベントの条件	Digraph (Z_r, Z_{r+1})	$\Pr(Z_r \wedge Z_{r+1})$
$i = 1$	$(0, 0)$	$N^{-2} \cdot (1 + 2 \cdot N^{-1})$
$i \neq 1, N-1$	$(0, 0)$	$N^{-2} \cdot (1 + N^{-1})$
$i \neq 0, 1$	$(0, 1)$	$N^{-2} \cdot (1 + N^{-1})$
$i \neq N-2$	$(i+1, N-1)$	$N^{-2} \cdot (1 + N^{-1})$
$i \neq 1, N-2$	$(N-1, i+1)$	$N^{-2} \cdot (1 + N^{-1})$
$i \neq 0, N-3, N-2, N-1$	$(N-1, i+2)$	$N^{-2} \cdot (1 + N^{-1})$
$i = N-2$	$(N-1, 0)$	$N^{-2} \cdot (1 + N^{-1})$
$i = N-1$	$(N-1, 1)$	$N^{-2} \cdot (1 + N^{-1})$
$i = 0, 1$	$(N-1, 2)$	$N^{-2} \cdot (1 + N^{-1})$
$i = 2$	$(N/2+1, N/2+1)$	$N^{-2} \cdot (1 + N^{-1})$
$i \neq N-2$	$(N-1, N-1)$	$N^{-2} \cdot (1 - N^{-1})$
$i \neq 0, N-1$	$(0, i+1)$	$N^{-2} \cdot (1 - N^{-1})$

つ．RC4 では一般的に鍵長は 128 ビット，$n = 8$，$N = 256$ が利用されているため，本論文ではこのパラメータのみを扱う．

3.2.1 1 バイト単位の bias(Single-byte bias)

RC4 のキーストリームの先頭 257 バイトにおいて多くの 1 バイト単位の bias が存在する．このバイアスを Single-byte bias と呼ぶ．特徴的な bias として，Mantin と Shamir の bias($Z_2 = 0$) [7]，Maitra らの bias($Z_r = 0$ for $3 \leq r \leq 255$) [8]，五十部らの bias($Z_3 = 131$, $Z_r = r$ for $3 \leq r \leq 255$, $Z_r = (256 - r)$ ($r = 32, 48, 64, 80, 96, 112$), $Z_{256} \neq 0$, $Z_{257} = 0$) [5] が存在する．さらに Sepehrdad らにより $Z_\ell = -\ell$ となる bias が実験的に確認された [9]．また Z_1 の分布に多くの bias が存在することが Mironov により実験的に確認されている [10]．このうち最も強いものは Bernstein らにより $Z_1 = 129$ であると実験的に示された [11]．

3.2.2 2 バイト単位の bias(Double-byte bias)

RC4 のキーストリームにおける 2 バイト単位の bias を Double-byte bias と呼ぶ．RC4 のキーストリームにおける Double-byte bias として Fluhrer と McGrew の bias(FM00 bias) [12] と Digraph repetition bias [13] の 2 つが提案されている．

Fluhrer と McGrew の bias (FM00 bias)

FM00 bias は FSE 2000 で Fluhrer と McGrew によって示されたキーストリームの 2 バイト単位の bias である [12]．この bias は条件を満たすポインタ i(= r mod N) ごとに 12 個のイベントにより構成されている．各イベントの詳細を表 3.2 に示す．

Digraph repetition bias (*ABSAB* bias)

ABSAB bias は EUROCRYPT 2005 で Mantin により提案された Long-term bias である [13]．この bias は A と B を 2 つのキーストリームの値とした場合，*ABAB* や *ABCAB*，*ABCDAB*

のように AB が短い間隔 S ごとに出力される．間隔 S の長さを G とおく．$ABSAB$ bias の詳細は以下の式で表される．

$$Z_r \| Z_{r+1} = Z_{r+2+G} \| Z_{r+3+G} \text{ for } G \geq 0 \tag{3.1}$$

ここで $\|$ はバイトの連結を表す．式 (3.1) の確率は定理 1 で与えられる．

定理 1. [13] *RC4* のキーストリームにおける，G に対する *ABSAB bias* の確率は $(1 + e^{(-4-8G)/N}/N) \cdot 1/N^2$ となる．

3.2.3 SSL/TLS における RC4 に対する平文回復攻撃

RC4 のキーストリームには多数の統計的な bias が存在する．それらの bias を利用して SSL/TLS 環境下における RC4 に対して多数の平文回復攻撃が提案されている．昨今は，SSL/TLS におけるパスワードや cookie を復元する攻撃が示されている．

USENIX 2013 において，AlFardan らが最尤推定を用いて全ての bias を利用する平文回復攻撃を提案した．本論文では，この攻撃を *ABPPS attack* と呼ぶ．この攻撃では初めの 256 バイトのキーストリームの確率分布を 2^{44} 通りの鍵から取得し，その分布をキーストリームの理想的な分布として利用する．平文の候補を μ，キーストリームを k とおく．M 個の暗号文から頻度表を得る．頻度表 $N_k^{(\mu)}$ は以下から得られる．

$$N_k^{(\mu)} = |\{j \mid C_{j,r} = k \oplus \mu\}_{1 \leq j \leq M}| \quad (0 \leq k \leq 255)$$

キーストリームの値の確率を $\text{Prob}[r, k]$，μ の尤度を $\lambda[\mu]$ とおく．尤度 $\lambda[\mu]$ は

$$\lambda[\mu] = \frac{S!}{N_0^{(\mu)}! \cdots N_{255}^{(\mu)}!} \cdot \prod_{k \in \{0,1,\ldots 255\}} (\text{Prob}[r, k])^{N_k^{(\mu)}}$$

から得られる．二つの候補 μ と μ' について $(N_0^{(\mu)}, \ldots, N_{255}^{(\mu)})$ と $(N_0^{(\mu')}, \ldots, N_{255}^{(\mu')})$ はそれぞれを並べ替えたものになる．したがって，最大の $\lambda[\mu]$ を算出する際には無視することができる．尤度を計算する際には $\lambda[\mu]$ の代わりに $\log(\lambda[\mu])$ を計算する．尤度 $\log(\lambda[\mu])$ を $\Lambda[\mu]$ とおく．$\Lambda[\mu]$ は

$$\Lambda[\mu] = \log(\lambda[\mu]) = \sum_{k=0}^{255} \left(N_k^{(\mu)} \cdot \log(\text{Prob}[r, k]) \right) \tag{3.2}$$

から得られる．最大の $\Lambda[\mu]$ から平分を推測する．この攻撃は 2^{32} の暗号文から，平文の最初の 256 バイトをほぼ確率 1 で復元できる．我々の攻撃でも同様の考えを利用する．

3.3 複数種類の Bias を利用した平文回復攻撃

本節では single-byte bias と double-byte bias を同時に用いた，新たな平文回復攻撃について述べる．上述の通り，従来の攻撃は single-byte bias と double-byte bias のどちらか一方を利用して平文を復元している．提案手法の有効性を示すために，連続した 8 バイトの秘密情報を復元する場合を考える．その他の平文は攻撃者が既知であると仮定する．HTTPS におけるヘッダやコンテンツは容易に推測可能であるため，上記は現実的な仮定と言える．

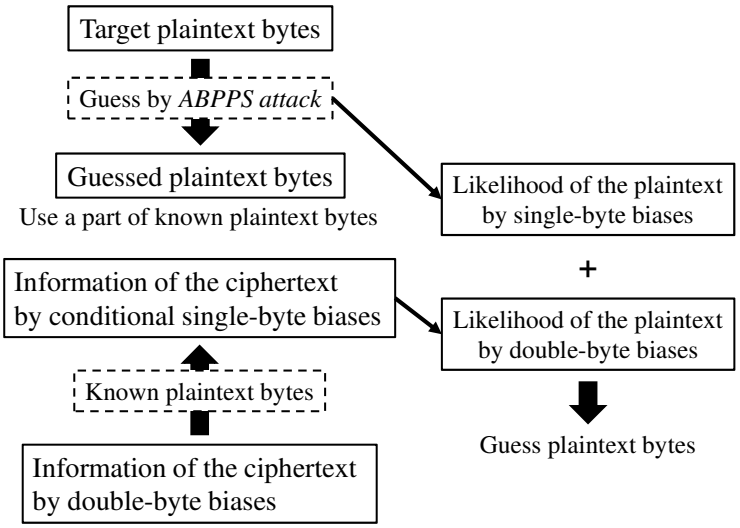

図 3.2: 提案手法の概要

3.3.1 攻撃の概要

復元対象の平文を $P_r, P_{r+1}, \ldots, P_{r+x}$ とおく．異なる n 個の鍵から生成された暗号文を $C^{(1)}, C^{(2)}, \ldots, C^{(n)}$ とおく．暗号文 $C^{(1)}, C^{(2)}, \ldots, C^{(n)}$ が得られた時，single-byte bias と double-byte bias(FM00 bias と ABSAB bias) それぞれについて暗号文の頻度表を作成する．復元対象の平文バイトについて適切に頻度表を組み合わせることで，復元精度の効率化を図る．図 3.2 に攻撃の概要を示す．

3.3.2 頻度表の構成

本項では，single-byte bias と double-byte bias の頻度表の作成方法について述べる．

Single-Byte Bias について

single-byte bias の頻度表を T_{Single} とおく．暗号文 $C^{(1)}, C^{(2)}, \ldots, C^{(n)}$ から暗号文の各バイトの値の数を取得し，T_{Single} を得る．復元対象を T_{Single} から $ABPPS attack$ を用いて推測する．復元対象の仮バイト $P^*_{r_t}(r \leq r_t \leq r+x)$ を得る．これらのバイトを double-byte bias の変換において既知の平文バイトとして利用する．

Double-Byte Bias について

復元対象以外の平分が既知であると仮定した場合，文献 [5, 26] の攻撃と同様に既知の平文バイトを利用して double-byte bias を条件付の single-byte bias に変換する．$ABSAB$ bias

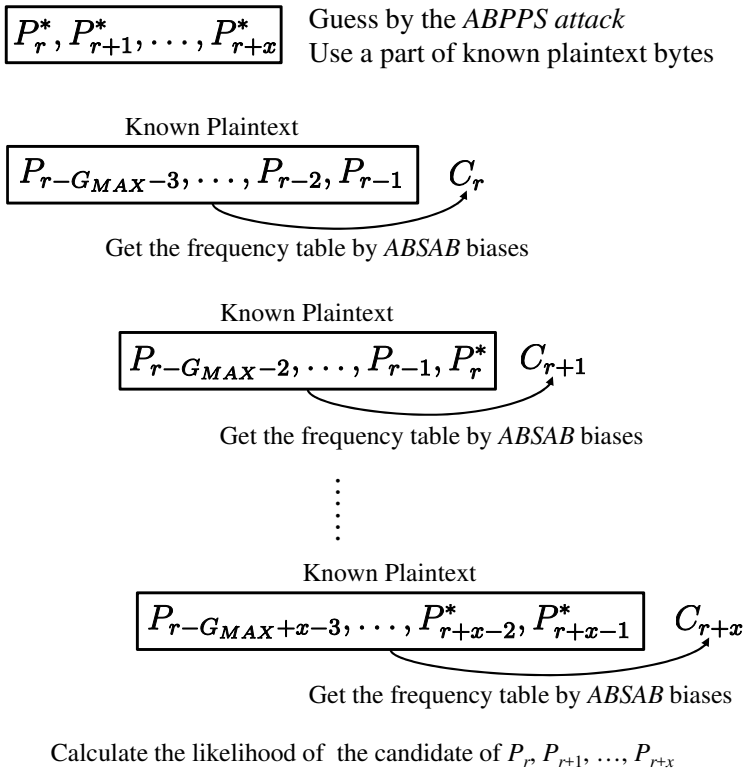

図 3.3: 前方からの $ABSAB$ bias による頻度表の構成方法

を条件付 bias として利用する方法について述べる．$ABSAB$ bias に関して $(C_{r-3-G}\|C_{r-2-G}) \oplus (C_{r-1}\|C_r)$ は

$$\begin{aligned}
&(C_{r-3-G}\|C_{r-2-G}) \oplus (C_{r-1}\|C_r) \\
&= (P_{r-3-G} \oplus Z_{r-3-G}\|P_{r-2-G} \oplus Z_{r-2-G}) \oplus (P_{r-1} \oplus Z_{r-1}\|P_r \oplus Z_r) \\
&= (P_{r-3-G} \oplus Z_{r-3-G} \oplus P_{r-1} + Z_{r-1}\|P_{r-2-G} \oplus Z_{r-2-G} \oplus P_r \oplus Z_r)
\end{aligned}$$

で表される．$ABSAB$ bias が成立している場合，上記の関係式は

$$(C_{r-3-G}\|C_{r-2-G}) \oplus (C_{r-1}\|C_r) = (P_{r-3-G} \oplus P_{r-1}\|P_{r-2-G} \oplus P_r)$$

のように変換される．この関係式と既知平文の情報を用いることで 1 バイト単位の頻度表が得られる．$ABSAB$ bias における G の最大値を G_{MAX} とおく．関係式と既知平文を用いた処理を $0 \le G \le G_{MAX}$ について実行する．図 3.3 に復元対象の前方からの $ABSAB$ bias の変換方法を示す．後方からの $ABSAB$ bias の変換についても同様にする．両方向からの 1 バイト単位の頻度表をそれぞれ T_{ABSAB_F}，T_{ABSAB_B} とおく．復元対象の平文について $T_{ABSAB_F}[r_t]$ と $T_{ABSAB_B}[r_t]$ を取得し，尤度を計算する．

次に FM00 bias を条件付 single-byte bias として扱う方法について述べる．FM00 bias を $(Z_{r+1}|Z_r)$ と $(Z_r|Z_{r+1})$ のように条件付 bias として考える．表 3.3 に $(Z_{r+1}|Z_r)$ and $(Z_r|Z_{r+1})$ のイ

ベントおよびその条件付確率を示す．暗号文 C_r の頻度表は $C_{r-1} = P_{r-1} \oplus Z_{r-1}$ より，FM00 bias と既知平文 P_{r-1} から得られる．図 3.4 に復元対象の前方からの FM00 bias の変換方法を示す．後方からの FM00 bias の変換についても同様にする．両方向からの 1 バイト単位の頻度表をそれぞれ T_{FM00_F}，T_{FM00_B} とおく．復元対象の平文について $T_{FM00_F}[r_t]$ と $T_{FM00_B}[r_t]$ を取得し，尤度を計算する．

表 3.3: ポインタ $i(= r \bmod N)$ ごとの FM00 bias に関する条件付き確率

i	Z_r	Z_{r+1}	条件付き確率
0	0	0	$N^{-1} \cdot (1 + N^{-1})$
	1	$N-1$	$N^{-1} \cdot (1 + N^{-1})$
	$N-1$	1	$N^{-1} \cdot (1 + N^{-1})$
	$N-1$	2	$N^{-1} \cdot (1 + N^{-1})$
	$N-1$	$N-1$	$N^{-1} \cdot (1 - N^{-1})$
1	0	0	$N^{-1} \cdot (1 + 2 \cdot N^{-1})$
	2	$N-1$	$N^{-1} \cdot (1 + N^{-1})$
	$N-1$	3	$N^{-1} \cdot (1 + N^{-1})$
	$N-1$	2	$N^{-1} \cdot (1 + N^{-1})$
	$N-1$	$N-1$	$N^{-1} \cdot (1 - N^{-1})$
	0	2	$N^{-1} \cdot (1 - N^{-1})$
2	0	0	$N^{-1} \cdot (1 + N^{-1})$
	0	1	$N^{-1} \cdot (1 + N^{-1})$
	3	$N-1$	$N^{-1} \cdot (1 + N^{-1})$
	$N-1$	3	$N^{-1} \cdot (1 + N^{-1})$
	$N-1$	4	$N^{-1} \cdot (1 + N^{-1})$
	$N/2+1$	$N/2+1$	$N^{-1} \cdot (1 + N^{-1})$
	$N-1$	$N-1$	$N^{-1} \cdot (1 - N^{-1})$
	0	3	$N^{-1} \cdot (1 - N^{-1})$
$3, 4, \ldots, N-4$	0	0	$N^{-1} \cdot (1 + N^{-1})$
	0	1	$N^{-1} \cdot (1 + N^{-1})$
	$i+1$	$N-1$	$N^{-1} \cdot (1 + N^{-1})$
	$N-1$	$i+1$	$N^{-1} \cdot (1 + N^{-1})$
	$N-1$	$i+2$	$N^{-1} \cdot (1 + N^{-1})$
	$N-1$	$N-1$	$N^{-1} \cdot (1 - N^{-1})$
	0	$i+1$	$N^{-1} \cdot (1 - N^{-1})$
$N-3$	0	0	$N^{-1} \cdot (1 + N^{-1})$
	0	1	$N^{-1} \cdot (1 + N^{-1})$
	$N-2$	$N-1$	$N^{-1} \cdot (1 + N^{-1})$
	$N-1$	$N-2$	$N^{-1} \cdot (1 + N^{-1})$
	$N-1$	$N-1$	$N^{-1} \cdot (1 - N^{-1})$
	0	$N-2$	$N^{-1} \cdot (1 - N^{-1})$
$N-2$	0	0	$N^{-1} \cdot (1 + N^{-1})$
	0	1	$N^{-1} \cdot (1 + N^{-1})$
	$N-1$	0	$N^{-1} \cdot (1 + N^{-1})$
	0	$N-1$	$N^{-1} \cdot (1 - N^{-1})$
$N-1$	0	1	$N^{-1} \cdot (1 + N^{-1})$
	0	$N-1$	$N^{-1} \cdot (1 + N^{-1})$
	$N-1$	0	$N^{-1} \cdot (1 + N^{-1})$
	$N-1$	1	$N^{-1} \cdot (1 + N^{-1})$
	$N-1$	$N-1$	$N^{-1} \cdot (1 - N^{-1})$

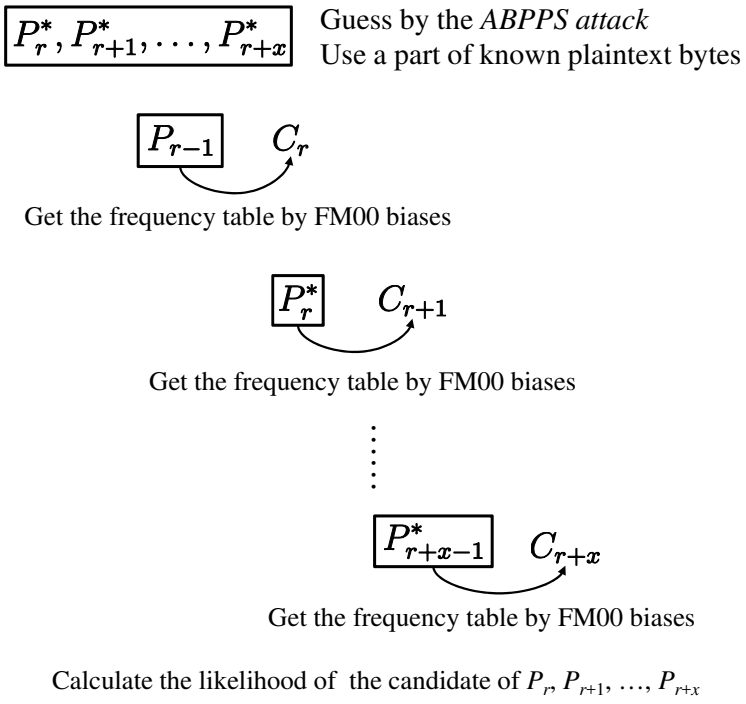

図 3.4: 前方からの FM00 bias による頻度表の構成方法

3.3.3 Sigle-Byte および Double-Byte Bias の頻度表の集約

3.3.2 項の議論より，single-byte bias と double-byte bias の両方から 1 バイト単位の頻度表を取得する．1 バイト単位の頻度表と式 (3.2) による bias の確率を利用して平文の候補の尤度を算出する．式 (3.2) は

$$\Lambda[\mu] = \sum_{k=0}^{255} \left(N_k^{(\mu)} \cdot \log(\mathrm{Prob}[r,k]) \right)$$

である．それぞれの bias に対する頻度表 $N_k^{(\mu)}$ は T_{Single}, T_{ABSAB_F}, T_{ABSAB_B}, T_{FM00_F}, T_{FM00_B} から得られる．single-byte bias に対する確率 Prob$[r,k]$ は 2^{40} 個のランダムに選択した鍵から生成されたキーストリームの分布から取得する．*ABSAB* bias に対する確率 Prob$[r,k]$ は定理 1 から，FM00 bias に対する Prob$[r,k]$ は表 3.3 からそれぞれ取得する．それぞれの bias から得られる尤度を Λ_{Single}, Λ_{ABSAB_F}, Λ_{ABSAB_B}, Λ_{FM00_F}, and Λ_{FM00_B} とおく．アルゴリズム 2, 3, 4, 5 に double-byte bias による尤度の算出方法を示す．加算により全ての尤度を集約する．

3.3.4 平文回復攻撃の流れ

提案手法の手順は以下である．

Algorithm 2 Calculate the likelihood of the forward $ABSAB$ bias

Require: r_t, /* position of a target byte */
G_{MAX}, /* parameter of the $ABSAB$ bias*/
$P_{r-3-G_{MAX}}, \ldots, P_{r-1}$, /* known plaintext bytes */
$P^*_r, \ldots P^*_{r+x-1}$, /* guessed plaintext bytes by single-byte biases */
$(C_{r-3-G_{MAX}}, \ldots C_{r+x})$s of $C^{(1)}, C^{(2)}, \ldots, C^{(n)}$ /* bytes of n ciphertexts encrypted by different keys */
Prob_{ABSAB_F} /* probabilities of the $ABSAB$ bias */
Ensure: The likelihood Λ_{ABSAB_F} of $P_r, \ldots P_{r+x}$
1: Regard $P^*_r, \ldots P^*_{r+x-1}$ as known plaintext bytes $P_r, \ldots P_{r+x-1}$
2: **for** $r_t = r$ **to** $r + x$ **do**
3: **for** $G = 0$ **to** G_{MAX} **do**
4: Make frequency tables $T_{count}[r_t][G]$ of $(C_{r_t-3-G} \| C_{r_t-2-G}) \oplus (C_{r_t-1} \| C_{r_t})$ from all ciphertexts $C^{(1)}, C^{(2)}, \ldots, C^{(n)}$, where $(C_{r_t-3-G} \| C_{r_t-2-G}) \oplus (C_{r_t-1} \| C_{r_t}) = (P_{r_t-3-G} \| P_{r_t-2-G}) \oplus (P_{r_t-1} \| P_{r_t})$ only if Eq. (3.1) holds.
5: Convert $T_{count}[r_t][G]$ into a frequency table $T_{convert}[r_t]$ of $(P_{r_t-1} \| P_{r_t})$ by $P_{r_t-G-3}, \ldots, P_{r_t-2}$.
6: Convert $T[r_t]$ into a frequency table $T_{ABSAB_F}[r_t]$ of P_{r_t} by P_{r_t-1}.
7: Calculate the likelihood $\Lambda_{ABSAB_F}[P_{r_t}]$ for all candidates of P_{r_t} from $T_{ABSAB_F}[r_t]$ and $\mathrm{Prob}_{ABSAB_F}[G][r_t, k]$, and merge the likelihood of all tables $T_{ABSAB_F}[r_t]$ by the addition.
8: **end for**
9: **end for**
10: Output the likelihood Λ_{ABSAB_F} of $P_r, \ldots P_{r+x}$

Step 1 平文 P_{r_t} の全ての候補について頻度表 $T_{Single}[r_t]$ および $\mathrm{Prob}_{Single}[r_t, k]$ から尤度 $\Lambda_{Single}[P_{r_t}]$ を計算する．尤度 $\Lambda_{Single}[P_{r_t}]$ が最大となる候補を仮平文 $P^*_{r_t}(r \le r_t \le r+x)$ として推測する．以後の Step において $P^*_{r_t}$ を既知平文として扱う．

Step 2 暗号文，既知平文，それぞれの bias の確率を利用して尤度 $\Lambda_{ABSAB_F}[P_{r_t}]$, $\Lambda_{ABSAB_B}[P_{r_t}]$, $\Lambda_{FM00_F}[P_{r_t}]$, $\Lambda_{FM00_B}[P_{r_t}](r \le r_t \le r + x)$ をアルゴリズム 2, 3, 4, 5 にしたがって計算する．

Step 3 尤度 $\Lambda_{Single}[P_{r_t}]$, $\Lambda_{ABSAB_F}[P_{r_t}]$, $\Lambda_{ABSAB_B}[P_{r_t}]$, $\Lambda_{FM00_F}[P_{r_t}]$, $\Lambda_{FM00_B}[P_{r_t}](r \le r_t \le r+x)$ を加算により集約する．それぞれの復元対象の平文について集約した尤度 $\Lambda_{merge}[P_{r_t}]$ が最大となる候補を平文として得る．

結果として，復元対象の平文 $P_r, P_{r+1}, \ldots, P_{r+x}$ について最も確からしい候補が得られる．

3.3.5 評価実験

本項では，提案する平文回復攻撃の実験を行う．復元対象の平文は POST 命令等の HTTP メソッドやハッシュ値の範囲外から選択している．8 バイトの秘密情報を含む既知平文

Algorithm 3 Calculate the likelihood of the backward $ABSAB$ bias

Require: r_t, /* position of a target byte */
G_{MAX}, /* parameter of the $ABSAB$ bias*/
$P_{r+x+1}, \ldots, P_{r+x+3+G_{MAX}}$, /* known plaintext bytes */
$P^*_{r-1}, \ldots P^*_{r+x}$, /* guessed plaintext bytes by single-byte biases */
$(C_r, \ldots C_{r+x+3+G_{MAX}})$s of $C^{(1)}, C^{(2)}, \ldots, C^{(n)}$ /* bytes of n ciphertexts encrypted by different keys */
Prob_{ABSAB_B} /* probabilities of the $ABSAB$ bias */

Ensure: The likelihood Λ_{ABSAB_B} of $P_r, \ldots P_{r+x}$

1: Regard $P^*_{r-1}, \ldots P^*_{r+x}$ as known plaintext bytes $P_{r-1}, \ldots P_{r+x}$
2: **for** $r_t = r + x$ **to** r **do**
3: **for** $G = 0$ **to** G_{MAX} **do**
4: Make frequency tables $T_{count}[r_t][G]$ of $(C_{r_t+3+G} \| C_{r_t+2+G}) \oplus (C_{r_t+1} \| C_{r_t})$ from all ciphertexts $C^{(1)}, C^{(2)}, \ldots, C^{(n)}$, where $(C_{r_t+3+G} \| C_{r_t+2+G}) \oplus (C_{r_t+1} \| C_{r_t}) = (P_{r_t+3+G} \| P_{r_t+2+G}) \oplus (P_{r_t+1} \| P_{r_t})$ only if Eq. (3.1) holds.
5: Convert $T_{count}[r_t][G]$ into a frequency table $T_{convert}[r_t]$ of $(P_{r_t+1} \| P_{r_t})$ by $P_{r_t+G+3}, \ldots, P_{r_t+2}$.
6: Convert $T[r_t]$ into a frequency table $T_{ABSAB_B}[r_t]$ of P_{r_t} by P_{r_t+1}.
7: Calculate the likelihood $\Lambda_{ABSAB_B}[P_{r_t}]$ for all candidates of P_{r_t} from $T_{ABSAB_B}[r_t]$ and $\mathrm{Prob}_{ABSAB_B}[G][r_t, k]$, and merge the likelihood of all tables $T_{ABSAB_B}[r_t]$ by the addition.
8: **end for**
9: **end for**
10: Output the likelihood Λ_{ABSAB_B} of $P_r, \ldots P_{r+x}$

を仮定する．秘密情報を提案手法により復元し，全てのバイトの復元に成功する確率の評価を行う．復元対象の平文 $\{P_{89}, P_{90}, \ldots, P_{96}\}$, $\{P_{113}, P_{114}, \ldots, P_{120}\}$, $\{P_{161}, P_{162}, \ldots, P_{168}\}$, $\{P_{201}, P_{202}, \ldots, P_{208}\}$ の 4 通りに対して実験を行う．G_{MAX} の値を 80 とする．256 通りの異なる平文について，ランダムに選択した鍵から生成した $2^6, 2^7, \ldots, 2^{29}$ 個の暗号文を用いて実験を行う．

表 3.4 に 2^{29} 個の暗号文を用いた場合の攻撃成功確率を示す．同時に *ABPPS attack* による同じ平文バイトに対する攻撃成功確率を示す．表 3.4 より，2^{29} 個の暗号文が与えられたとき，$P_{113}, P_{114}, \ldots, P_{120}$ が約 0.961 の確率で復元できる．これは *ABPPS attack* の結果より高い確率である．さらに $\{P_{161}, P_{162}, \ldots, P_{168}\}$ や $\{P_{201}, P_{202}, \ldots, P_{208}\}$ を復元する場合には，攻撃成功確率の差が大きくなっている．これは single-byte bias の影響が弱まり，double-byte bias が復元に有効に働くためであると考えられる．特に P_{201} や P_{208} は既知平文と隣り合っているため，$\{P_{201}, P_{202}, \ldots, P_{208}\}$ における他の対象より高い確率で復元に成功している．結果として，平文の値がランダムに分布しているという仮定のもと，従来より効率の良い攻撃であることがわかる．

Algorithm 4 Calculate the likelihood of the forward FM00 bias

Require: r_t, /* position of a target byte */
P_{r-1}, /* known plaintext bytes */
$P^*_r, \ldots P^*_{r+x-1}$, /* guessed plaintext bytes by single-byte biases */
$(C_{r-1}, \ldots C_{r+x})$s of $C^{(1)}, C^{(2)}, \ldots, C^{(n)}$ /* bytes of n ciphertexts encrypted by different keys */
Prob_{FM00_F} /* probabilities of the FM00 bias */

Ensure: The likelihood Λ_{FM00_F} of $P_r, \ldots P_{r+x}$

1: Regard $P^*_r, \ldots P^*_{r+x-1}$ as known plaintext bytes $P_r, \ldots P_{r+x-1}$
2: **for** $r_t = r$ **to** $r + x$ **do**
3: Make frequency tables $T_{count}[r_t]$ of $(C_{r_t-1}|C_{r_t})$ from all ciphertexts $C^{(1)}, C^{(2)}, \ldots, C^{(n)}$.
4: Convert $T_{count}[r_t]$ into a frequency table $T_{FM00_F}[r_t]$ of P_{r_t} by P_{r_t-1}.
5: Calculate the likelihood $\Lambda_{FM00_F}[P_{r_t}]$ for all candidates of P_{r_t} from $T_{FM00_F}[r_t]$ and $\mathrm{Prob}_{FM00_F}[r_t, k]$, and merge the likelihood of all tables $T_{FM00_F}[r_t]$ by the addition.
6: **end for**
7: Output the likelihood Λ_{FM00_F} of $P_r, \ldots P_{r+x}$

3.4 結言

本章では，SSL/TLS における RC4 に対する効率的な平文回復攻撃を提案した．Vanhoef らの攻撃に着目し，single-byte bias と double-byte bias を同時に利用する手法を構築した．提案手法の有効性を確認する実験を行った．復元対象の平文を $\{P_{89}, P_{90}, \ldots, P_{96}\}$, $\{P_{113}, P_{114}, \ldots, P_{120}\}$, $\{P_{161}, P_{162}, \ldots, P_{168}\}$, $\{P_{201}, P_{202}, \ldots, P_{208}\}$ とした．提案手法を対象の平文全ての復元に成功する確率で評価した．結果として，2^{29} の暗号文から $\{P_{113}, P_{114}, \ldots, P_{120}\}$ 全体を約 0.961 の確率で復元することができた．これは *ABPPS attack* より高い確率である．したがって，提案手法は，平文バイトがランダムに分布しているという仮定のもと，従来より効率的な攻撃である．他のストリーム暗号の解析に提案手法が適用されることを期待する．

Algorithm 5 Calculate the likelihood of the backward FM00 bias

Require: r_t, /* position of a target byte */
P_{r+x+1}, /* known plaintext bytes */
$P^*_{r+1}, \ldots P^*_{r+x}$, /* guessed plaintext bytes by single-byte biases */
$(C_r, \ldots C_{r+x+1})$s of $C^{(1)}, C^{(2)}, \ldots, C^{(n)}$ /* bytes of n ciphertexts encrypted by different keys */
Prob_{FM00_B} /* probabilities of the FM00 bias */

Ensure: The likelihood Λ_{FM00_B} of $P_r, \ldots P_{r+x}$

1: Regard $P^*_{r-1}, \ldots P^*_{r+x}$ as known plaintext bytes $P_{r-1}, \ldots P_{r+x}$
2: **for** $r_t = r + x$ **to** r **do**
3: Make frequency tables $T_{count}[r_t]$ of $(C_{r_t+1}|C_{r_t})$ from all ciphertexts $C^{(1)}, C^{(2)}, \ldots, C^{(n)}$.
4: Convert $T_{count}[r_t]$ into a frequency table $T_{FM00_B}[r_t]$ of P_{r_t} by P_{r_t+1}.
5: Calculate the likelihood $\Lambda_{FM00_B}[P_{r_t}]$ for all candidates of P_{r_t} from $T_{FM00_B}[r_t]$ and $\mathrm{Prob}_{FM00_B}[r_t, k]$, and merge the likelihood of all tables $T_{FM00_B}[r_t]$ by the addition.
6: **end for**
7: Output the likelihood Λ_{FM00_B} of $P_r, \ldots P_{r+x}$

表 3.4: 提案手法および *ABPPS attack* の攻撃成功確率

r	提案手法	*ABPPS attack*
89	0.996	0.996
90	1	1
91	1	1
92	1	0.996
93	0.996	1
94	1	0.996
95	1	1
96	1	1
ALL(89-96)	0.992	0.988
113	0.992	0.980
114	1	0.980
115	1	0.980
116	0.996	0.992
117	1	0.984
118	1	0.984
119	0.988	0.992
120	0.984	0.980
ALL(113-120)	0.961	0.882
161	0.875	0.820
162	0.902	0.789
163	0.871	0.750
164	0.883	0.840
165	0.879	0.797
166	0.832	0.766
167	0.863	0.828
168	0.871	0.797
ALL(161-168)	0.334	0.164
201	0.750	0.613
202	0.672	0.621
203	0.644	0.590
204	0.605	0.586
205	0.602	0.574
206	0.621	0.559
207	0.641	0.531
208	0.758	0.605
ALL(201-208)	0.0357	0.0136

第4章　Strong IVを用いたWEPの安全な運用方法

4.1　緒言

スマートフォンなどの携帯端末の発展や普及にともない，無線 LAN の利用が急速に拡大している．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さらされている．安全に通信を行うために情報の暗号化を行い，情報の漏洩を防ぐ必要がある．無線 LAN の暗号化方式の一つに Wired Equivalent Privacy(WEP)[3] がある．WEP はストリーム暗号である RC4 をもとに開発された共通鍵暗号方式である．WEP は 3 バイトの IV を含む秘密鍵を利用して暗号化を行っている．WEP は深刻な脆弱性が指摘されており，それ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 [14]．FMS 攻撃は weak IV と呼ばれる特定の IV を用いて WEP 鍵の導出を行う．FMS 攻撃を拡張した攻撃が 2004 年に Korek によって提案された [36, 15]．Korek 攻撃では FMS 攻撃より多くの IV を weak IV として利用することができる．これらの特定の IV に依存する攻撃はフィルタリングによって weak IV を取り除くことで対策が可能である．一方で特定の IV に依存しない攻撃が提案されている．2006 年に A. Klein によって Klein 攻撃が提案された [16]．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．2008 年に E. Tews，R. Weinmann，A. Pyshkin らによって PTW 攻撃が提案された [17]．この攻撃は Klein 攻撃を改良した攻撃であり，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．複数の攻撃関数を用いる攻撃として 2010 年に寺村，朝倉，大東，桑門，森井らにより TeAM-OK 攻撃が提案された [18]．この攻撃は Klein 攻撃，PTW 攻撃，OKM 攻撃 [37] の三つの攻撃関数を用いて WEP 鍵の導出を行う．2013 年に P. Sepehrdad，P. Suisil，S. Vaudenay，M. Vuagnoux らによって Tornado 攻撃が提案された [19]．この攻撃は改良した Klein 攻撃や Korek 攻撃などから導出した 22 個の攻撃関数を利用して投票を行い，WEP 鍵を推定する．この攻撃は 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 Access2(WPA2)[20] など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の移行は様々なコストを要することから，大規模な施設などでは現在でも 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 WEP 鍵を使用するパケット数を制限し，一定間隔ごとに WEP 鍵を更新する方法がある．従来の鍵回復攻撃は 10,000 パケットの盗聴において成功確率は 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．別の対策として，weak IV や統計的性質の成立を回避することが考えられる．weak IV を回避する方法は WEPplus[21] として実現されている．WEPplus はファームウェアの更新により，無線 LAN 機器に導入されている．また，統計的性質の成立を妨げる IV も存在する．したがって特定の IV を用いることで WEP を安全に利用することができる．2011 年に塚畝らにより，Klein 攻撃，PTW 攻撃，TeAM-OK 攻撃を妨げる IV の存在が明らかにされた [22]．彼らはそのような IV を Strong IV と呼んでいる．しかしながら，Strong IV の取得方法や安全性については，十分な議論が行われていない．

本章では WEP のより安全な運用方法を提案する．さらに WEP と同等の速度で実行可能であることを確認する．提案方式では Strong IV に加えて Tornado 攻撃における Korek 攻撃，キーストリームのバイアス (SVV_10[9]) による攻撃関数に対応した Strong IV を用いる．Tornado 攻撃では投票条件が全て成立している場合に攻撃関数による WEP 鍵の候補値に対する投票が行われる．そこで任意の IV と WEP 鍵を用いた場合に投票条件が成立しているかどうかを効率的に判定する方法を提案する．100,000 パケットごとに鍵を更新することを想定した WEP の運用方法として Klein 攻撃，Korek 攻撃，SVV_10 のバイアスによる攻撃関数を全て無効にする Strong IV を 50,000 個，Klein 攻撃を除いた攻撃関数のみを無効にする IV を 50,000 個混合して利用する．このとき Strong IV の判定と並行して暗号化を行うことで通信への負荷を軽減する．Strong IV の判定と暗号化を並行して行った場合に 50,000 パケットの暗号化に要する時間の評価を行う．Strong IV の判定と同時に 1472 バイトの平文を 50,000 個暗号化するのに要した時間は 338 ミリ秒である．一般的な WEP を用いた場合には 50,000 パケットの暗号化に 306 ミリ秒を要する．したがって，提案手法では暗号化に 1.1-1.2 倍程度の時間が必要となる．結果として，提案手法により WEP と同等の通信速度で安全な通信が実現可能である．また，提案手法は WEP の処理に IV の判定を導入することで実現できるため，従来の機器のファームウェアを更新することで導入可能であると考えられる．

4.2 Wired Equivalent Privacy

WEP は無線 LAN の暗号化方式の一つであり，RC4 をベースにした共通鍵暗号方式である．RC4 の要素数 N は 256 とする．WEP において秘密鍵 K は 24 ビットの初期化ベクトル (IV) と 40 ビットあるいは 104 ビットの WEP 鍵の連結により構成される．本稿では 104 ビットの WEP 鍵を想定して議論する．WEP の秘密鍵は

$$K = K[0]||K[1]||K[2]||K[3]||\cdots||K[15] = IV_0||IV_1||IV_2||K[3]||\cdots||K[15]$$

のように表される．ただし IV_i は $i+1$ バイト目の IV を表し，$K[3]||\cdots||K[15]$ は WEP 鍵を表す．図 4.1 に WEP の処理を示す．WEP による暗号化通信において，IV の値はパケットごとに変更される．パケットごとに異なる秘密鍵を用いることで常に同じキーストリームが生成されるのを防ぐためである．IV は通信を行う二者間で共有する必要があるため，暗号文とともに送信される．このとき IV は暗号化されておらず，WEP 鍵を共有していない第三者にも既知となる．IV の長さは 24 ビットであり十分に大きい領域を確保しているとはいえない．以上のような IV の性質が WEP の脆弱性の要因となっている．

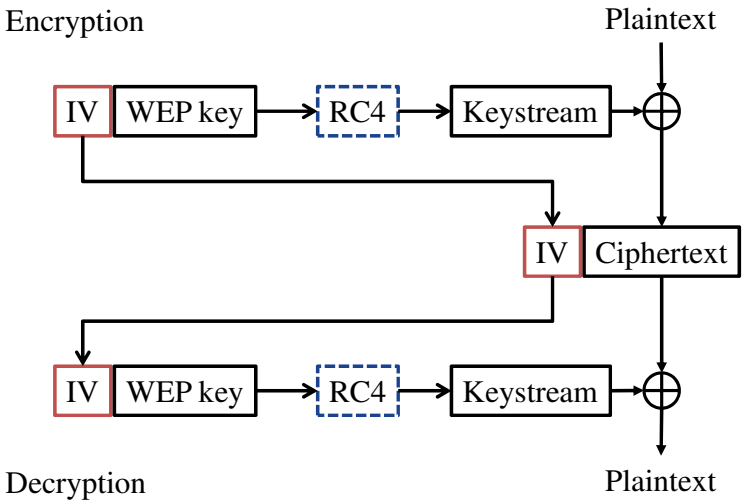

図 4.1: WEP の暗号化および復号

4.3 WEP に対する鍵回復攻撃とその対策

WEP に対する鍵回復攻撃は IV の値に依存する攻撃と，統計的性質に基づく攻撃が提案されている．一方で，鍵回復攻撃の対策が提案されている．本節ではこれらについて述べる．

4.3.1 WEP に対する鍵回復攻撃

IV の値に依存する攻撃

2001 年に，Fluher らが初めて IV の値に依存する鍵回復攻撃を示した [14]．この攻撃は FMS 攻撃と呼ばれる．FMS 攻撃では weak IV を利用して RC4 の内部状態を推測し，WEP 鍵を復元する攻撃である．この攻撃は weak IV を用いて暗号化されたパケットに対してのみ有効であるため，非常に多くのパケットが必要になる．FMS 攻撃は WEP 鍵の復元に 6,000,000 パケット必要となる．2004 年に，Korek が FMS 攻撃を拡張した攻撃を提案した [15]．この攻撃は FMS 攻撃より多くの IV を weak IV として利用することができる．よってこの攻撃に必要なパケット数が減少する．Korek 攻撃では WEP 鍵の復元に 500,000 から 1,000,000 パケット必要となる．

統計的性質に基づく攻撃

2006 年に，Klein は統計的性質に基づく鍵回復攻撃を提案した [16]．Klein 攻撃は RC4 の内部状態において特定の遷移が起こりやすいことを利用して内部状態の遷移を予測し，その内部状態とキーストリームの関係から WEP 鍵を復元する．内部状態の予測に復元対象の WEP 鍵の一つ前のバイトの情報を用いるため，WEP 鍵を先頭から逐次的に復元する攻撃である．

Klein 攻撃が成立する内部状態の遷移は二つの条件から構成される．WEP 鍵のインデックスを x とおく．WEP 鍵 $K[x]$ を解析する場合を考える．一つ目の条件は KSA の x ラウンドにおいてスワップされた要素 $S[j]$ が PRGA の $x-1$ ラウンド目までスワップされないことである．条件式は以下のように表される．

$$S_{x+1}[x] = S'_{x-1}[x]$$

この条件を Condition 1 とおく．二つ目の条件は $S'_{x-1}[x]$ の値がキーストリームにより一意に決定することである．条件式は以下のように表される．

$$S'_{x-1}[x] = x - Z_x$$

この条件を Condition 2 とおく．図 4.2 に Condition 1 および 2 を示す．Condition 1，2 が同時に成立した場合，以下の等式が成立する．

$$\begin{aligned} K[x] &= f_{Klein}(K[0], \ldots, K[x-1], Z_x) \\ &= S_x^{-1}[x - Z_x] - j_x - S_x[x] \end{aligned} \tag{4.1}$$

攻撃者は IV，キーストリーム Z_x，WEP 鍵 $K[3], K[4], \ldots, K[x-1]$ から，上式を用いて $K[x]$ の候補を得る．したがって，一つのパケットから一つの候補が決定される．Klein 攻撃の成功確率は

$$\begin{aligned} Prob_{Klein} &= \left(\frac{255}{256}\right)^{254} \cdot \frac{2}{256} + \left(1 - \left(\frac{255}{256}\right)^{254}\right) \cdot \frac{254}{256 \cdot 255} \\ &\approx \frac{1.36}{256} \end{aligned}$$

となる．多数のパケットに対して式 (4.1) から鍵の候補値の推測と投票を行い，最も投票数の多かった候補値を WEP 鍵の 1 バイトとする．Klein 攻撃は，60,000 パケットの盗聴から確率 0.5 で WEP 鍵を復元可能である．

2008 年に Tews らによって PTW 攻撃が提案された [17]．Klein 攻撃と同様に IV とキーストリームの関係を利用して WEP 鍵を復元する．KSA において WEP 鍵により遷移する内部状態について近似を行う．近似以外については Klein 攻撃と同様の攻撃手法である．PTW 攻撃の攻撃関数は

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

となる．ただし σ_x は $K[3]$ から $K[x]$ までの和を表す．PTW 攻撃の成功確率は

$$Prob_{(PTW,x)} = q_x \cdot \left(\frac{255}{256}\right)^{254} \cdot \frac{2}{256} + \left(1 - q_x \cdot \left(\frac{255}{256}\right)^{254}\right) \cdot \frac{254}{256 \cdot 255}$$

となる．ただし，

$$q_x = \left(\frac{255}{256}\right)^{x-3} \cdot \left(\frac{256 - x + 3}{256}\right) \cdot \prod_{k=1}^{x-3} \left(\frac{256 - k}{256}\right)$$

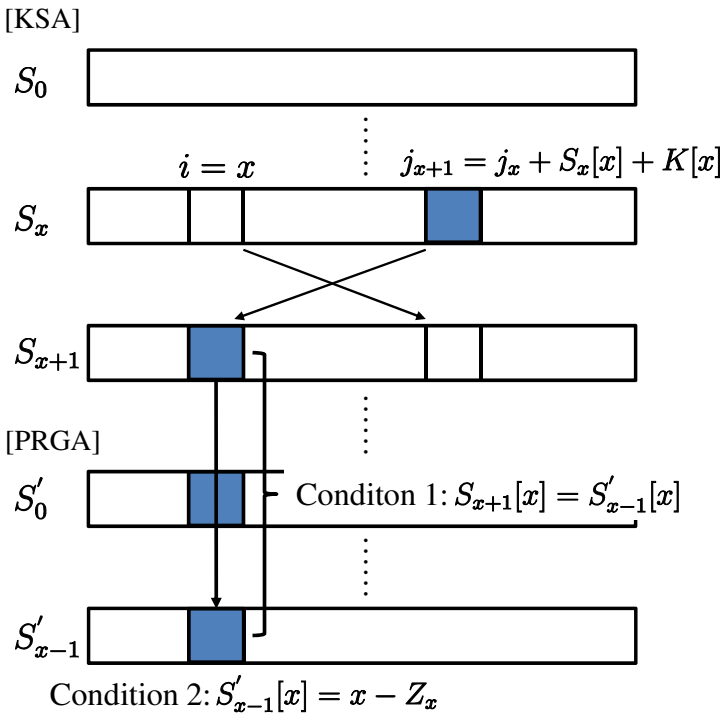

図 4.2: Klein 攻撃の条件

である．この攻撃は WEP 鍵の和を並列に求めることができる．PTW 攻撃は，40,000 パケットの盗聴から確率 0.5 で WEP 鍵を復元可能である．

2010 年に寺村らにより TeAM-OK 攻撃が提案された [18]．この攻撃は Klein 攻撃，PTW 攻撃，OKM 攻撃 [37] の攻撃関数を利用している．キーストリームのインデックスを w とおく．OKM 攻撃の攻撃関数は

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

となる．ただし，$w = 19, 20, \ldots, 31$ である．OKM 攻撃の攻撃成功確率は

$$Prob_{(OKM,w)} = q'_w \cdot \left(\frac{255}{256}\right)^{254} \cdot \frac{2}{256} + \left(1 - q'_w \cdot \left(\frac{255}{256}\right)^{254}\right) \cdot \frac{254}{256 \cdot 255}$$

である．ただし，

$$q'_w = \left(\frac{255}{256}\right)^{32-w} \cdot \left(\frac{256-32+w}{256}\right) \cdot \prod_{k=w-15}^{16} \left(\frac{256-w-1+k}{256}\right)$$

となる．OKM 攻撃は WEP 鍵の和が既知であるという仮定の下で，キーストリーム Z_{19}, Z_{20}, $\ldots$, Z_{31} から高い確率で WEP 鍵を導出することが可能である．TeAM-OK 攻撃は，36,500 パケットの盗聴から確率 0.5 で WEP 鍵を復元可能である．

PTW 攻撃，TeAM-OK 攻撃ともに Klein 攻撃の条件が必要な攻撃である．したがって Klein 攻撃の条件が不成立である場合，これらの攻撃は成功しない．

Tornado 攻撃

表 4.1: Tornado 攻撃で利用される攻撃関数

位置	名称	攻撃関数	投票条件
x	Klein-Improved	$S_t^{-1}[x - Z_x] - \sigma_x(t)$	$(x - Z_x) \notin \{S_t[t+1], \ldots, S_t[x-1]\}$
$x \neq 1$	MP-Improved	$Z_{x+1} - \sigma_x(t)$	$x \neq 1,\ z_{x+1} \geq x,\ \forall 0 \leq i' \leq t : j_{i'} \neq z_{x+1}$
16	SVV_10 [9]	$S_t^{-1}[0] - \sigma_{16}(t)$	$S_t^{-1}[0] < t+1$ or $S_t^{-1}[0] > 15,\ Z_{16} = -16,$ $j_2 \notin \{t+1, \ldots, 15\}$
x	A_u15	$2 - \sigma_x(t)$	$S_t[x] = 0,\ Z_2 = 0$
x	A_s13	$S_t^{-1}[0] - \sigma_x(t)$	$S_t[1] = x,\ (S_t^{-1}[0] < t+1$ or $S_t^{-1}[0] > x-1),$ $Z_1 = x$
x	A_u13_1	$S_t^{-1}[Z_1] - \sigma_x(t)$	$S_t[1] = x,\ (S_t^{-1}[Z_1] < t+1$ or $S_t^{-1}[Z_1] > x-1),$ $Z_1 = 1 - x$
x	A_u13_2	$1 - \sigma_x(t)$	$S_t[x] = x,\ S_t[1] = 0,\ Z_1 = x$
x	A_u13_3	$1 - \sigma_x(t)$	$S_t[x] = x,\ S_t[1] = 1 - x,\ Z_1 = 1 - x$
x	A_s5_1	$S_t^{-1}[Z_1] - \sigma_x(t)$	$S_t[1] < t+1,\ S_t[1] + S_t[S_t[1]] = x,$ $Z_1 \neq \{S_t[1], S_t[S_t[1]]\},$ $(S_t^{-1}[Z_1] < t+1$ or $S_t^{-1}[Z_1] > x-1)$
x	A_s5_2	$S_t^{-1}[S_t[1] - S_t[2]] - \sigma_x(t)$	$S_t[2] + S_t[1] = x,\ S_t^{-1}[S_t[1] - S_t[2]] \neq \{1, 2\},$ $(S_t^{-1}[S_t[1] - S_t[2]] < t+1$ or $S_t^{-1}[S_t[1] - S_t[2]] > x-1),\ Z_2 = S_t[1]$
x	A_s5_3	$S_t^{-1}[Z_2] - \sigma_x(t)$	$S_t[2] + S_t[1] = x,\ S_t^{-1}[Z_2] \neq \{1, 2\},$ $(S_t^{-1}[Z_2] < t+1$ or $S_t^{-1}[Z_2] > x-1),$ $Z_2 = 2 - S_t[2]$
x	A_u5_1	$S_t^{-1}[S_t^{-1}[Z_1] - x] - \sigma_x(t)$	$S_t[1] = x,\ S_t^{-1}[Z_1] < t+1,\ S_t^{-1}[S_t^{-1}[Z_1] - x] \neq 1,$ $(S_t^{-1}[S_t^{-1}[Z_1] - x] < t+1$ or $S_t^{-1}[S_t^{-1}[Z_1] - x] > x-1),$ $Z_1 \neq \{x, 1-x, S_t^{-1}[Z_1] - x\},\ S_t^{-1}[Z_1] \neq 2x$
x	A_u5_2	$1 - \sigma_x(t)$	$S_t[x] = 1,\ Z_1 = S_t[2]$
x	A_u5_3	$1 - \sigma_x(t)$	$S_t[x] = x,\ S_t^{-1}[Z_1] \neq 1,\ S_t^{-1}[Z_1] < t+1,$ $Z_1 = S_t[S_t[1] + x]$
x	A_s3	$S_t^{-1}[Z_2] - \sigma_x(t)$	$S_t[1] \neq 2,\ S_t[2] \neq 0,\ S_t[2] + S_t[1] < t+1,$ $S_t[2] + S_t[S_t[2] + S_t[1]] = x,$ $S_t^{-1}[Z_2] \neq \{1, 2, S_t[1] + S_t[2]\},$ $S_t[1] + S_t[2] \neq \{1, 2\},$ $(S_t^{-1}[Z_2] < t+1$ or $S_t^{-1}[Z_2] > x-1)$
4	A_4_s13	$S_t^{-1}[0] - \sigma_4(t)$	$S_t[1] = 2,\ S_t[4] \neq 0,$ $(S_t^{-1}[0] < t+1$ or $S_t^{-1}[0] > x-1),\ Z_2 = 0$
4	A_4_u5_1	$S_t^{-1}[254] - \sigma_4(t)$	$S_t[1] = 2,\ Z_2 \neq 0,\ Z_2 \neq 254,$ $(S_t^{-1}[254] < t+1$ or $S_t^{-1}[254] > 3)$
4	A_4_u5_2	$S_t^{-1}[255] - \sigma_4(t)$	$S_t[1] = 2,\ Z_2 \neq 0,$ $(S_t^{-1}[255] < t+1$ or $S_t^{-1}[255] > 3),\ Z_2 = S_t[2]$
x	A_neg_1	$1 - \sigma_x(t)$ or $2 - \sigma_x(t)$	$S_t[2] = 0,\ S_t[1] = 2,\ Z_1 = 2$
x	A_neg_2	$2 - \sigma_x(t)$	$S_t[2] = 0,\ S_t[1] \neq 2,\ Z_2 = 0$
x	A_neg_3	$1 - \sigma_x(t)$ or $2 - \sigma_x(t)$	$S_t[1] = 1,\ Z_1 = S_t[2]$
x	A_neg_4	$-\sigma_x(t)$ or $1 - \sigma_x(t)$	$S_t[1] = 0,\ S_t[0] = 1,\ Z_1 = 1$

2013 年に Sepehrdad らによって Tornado 攻撃が提案された [19]．この攻撃は 22 個の攻撃関数を用いて WEP 鍵の推測を行う．利用する攻撃関数は，Klein 攻撃を改良したもの (Klein-Improved)，Maitra-Paul 攻撃 [38] を改良したもの (MP-Improved)，Korek 攻撃のバイ

アスを改良したもの，キーストリームの 16 バイト目のバイアス (SVV_10[9]) を利用したものである．表 4.1 に攻撃関数およびそれぞれの投票条件を示す．WEP において最後に既知である内部状態の段数を t とおく．例えば，WEP において $K[0]$，$K[1]$，$K[2]$ が既知であるため，$t = 2$ となる．表 4.1 において，$\sigma_x(t)$ は

$$\sigma_x(t) = \sum_{j=0}^{t} S_{j-1}[x] + \sum_{j=t+1}^{x} S_t[j]$$

である．それぞれの攻撃関数について，全ての投票条件が成立した場合に WEP 鍵の候補の推測が行われる．Tornado 攻撃は 22,500 パケットの盗聴から，確率 0.5 で WEP 鍵を復元可能である．

4.3.2 WEP に対する鍵回復攻撃への対策

WEPplus

WEPplus は weak IV を回避することで WEP の安全性を向上する手法である [21]．よって WEPplus は weak IV に基づく攻撃を防ぐことができる．しかしながら WEPplus は統計的性質に基づく攻撃を防ぐことはできない．

2006 年に，吉田らによって FMS 攻撃の weak IV を効率的に取り除く手法が提案された [39]．この手法により，FMS 攻撃に対する weak IV をほぼ全て取り除くことができる．

Strong IV

4.3.1 項より，従来の鍵回復攻撃は 20,000 パケットの盗聴では成立が困難である．さらに 10,000 パケットの盗聴で WEP 鍵が復元できる攻撃は存在しない．統計的性質に基づく鍵回復攻撃を防ぐために，10,000 パケットごとに WEP 鍵を更新する方法が考えられる．しかし，10,000 パケットは非常に少数であり，通信のスループットの多大な影響を与える．

この問題の解決策として，塚畝らにより Strong IV が提案された [22]．Strong IV は Klein 攻撃が成立しない IV の集合である．Strong IV を用いた場合，Klein 攻撃の条件が成立しないため，Klein 攻撃による WEP 鍵の復元が困難になる．PTW 攻撃および TeAM-OK 攻撃も Klein 攻撃と同様の条件が必要であるため，Strong IV はこれらの攻撃も防ぐことができる．しかしながら，このような IV を取得する現実的な手法や安全性に関する議論が不十分であった．

4.4 新たな Strong IV を用いた安全な WEP の運用

本節では安全な WEP の運用方法について述べる．初めに新たな Strong IV を用いて鍵回復攻撃を困難にする方法を説明する．さらに提案手法を用いた場合に，暗号化の処理時間を評価する．

4.4.1 鍵回復攻撃を困難にする WEP の運用方法

Strong IV の定義

高い確率で取得可能な Strong IV の定義について述べる．Klein 攻撃の Condition 1 あるいは Condition 2 のどちらか一方が成立しない IV を Strong IV として定義する．このとき $K[x]$ に対する Strong IV の条件は

$$S_{x+1}[x] \neq S'_{x-1}[x] \; or \; S'_{x-1}[x] \neq x - Z_x$$

となる．Strong IV の値は WEP 鍵に依存するため，WEP 鍵の各バイトごとに Strong IV を決定する必要がある．提案する運用方法では WEP 鍵の 13 バイトを保護する Strong IV を利用する．利用する Strong IV の生成確率を $Prob_{StrongIV_{13}}$ とする．Strong IV の生成確率は，

$$Prob_{StrongIV_{13}} = \left(1 - \left(\frac{255}{256}\right)^{254} \cdot \frac{2}{256}\right)^{13} \approx 0.96$$

となる．高い確率で Strong IV が得られるため，短時間で生成可能である．

WEP において Strong IV のみを利用する場合，Klein 攻撃の条件が発生しない．先述の通り，PTW 攻撃および OKM 攻撃も同様の条件を持つ．したがってそれぞれの攻撃の成功確率が以下のようになる．

$$Prob'_{Klein} = \left(1 - \left(\frac{255}{256}\right)^{254}\right) \cdot \frac{254}{256 \cdot 255} \approx \frac{0.63}{256}$$

$$Prob'_{(PTW,x)} = \left(1 - q_x \cdot \left(\frac{255}{256}\right)^{254}\right) \cdot \frac{254}{256 \cdot 255}$$

$$Prob'_{(OKM,w)} = \left(1 - q'_w \cdot \left(\frac{255}{256}\right)^{254}\right) \cdot \frac{254}{256 \cdot 255}$$

これらの確率はランダムより低いため，低確率の候補を観測することによって WEP 鍵の情報が漏洩する．

Korek 攻撃のフィルタリング

表 4.1 の通り，Tornado 攻撃は 22 個の攻撃関数から構成されている．ある攻撃関数の投票条件が全て成立した場合，攻撃者は WEP 鍵の候補を推測する．投票条件が少なくとも一つ成立しなければ，攻撃関数は無効になる．したがって，幾つかの投票条件を回避することによって Tornado 攻撃を防ぐことができる．4.2 節に示した通り，$K[0]$，$K[1]$，$K[2]$ が既知であるため，表 4.1 において $t = 2$ と仮定する．Korek 攻撃に基づく攻撃関数はいくつかの IV を取り除くことによって防ぐことができると考えられる．表 4.1 より，最後の既

知内部状態が以下の条件を満たす場合，A_u5_3 以外の Korek 攻撃に基づく攻撃関数は無効になる．

$$
\begin{aligned}
&S_2[x] \neq 0, \\
&S_2[x] \neq 1, \\
&S_2[2] \neq 0, \\
&15 < S_2[1] < 241, \\
&15 < S_2[1] + S_2[2]
\end{aligned}
$$

ただし，$3 \leq x \leq 15$ である．IV による KSA の処理後に最後の既知内部状態が得られるため，IV によって条件の成立が決定できる．約 78%の IV が上記の条件を満たす．残りの IV を後述するフィルタリングパターンにより取り除く．ここで $j_{r'}$ を KSA の r' 段目のポインタ j とおく．条件 $S_2[x] \neq 0$，$S_2[x] \neq 1, S_2[2] \neq 0$，$15 < S_2[1] < 241$ を満たすために，$3 \leq IV_0 \leq 15$ を取り除く．KSA のアルゴリズムより，$IV_0 = 0$ のとき $j_0 = 0$ となる．この場合，$j_1 = 0 + 1 + IV_1 = IV_1 + 1$ となる．$S_1[1]$ と $S_1[IV_1 + 1]$ を入れ替える．条件 $S_2[x] \neq 1$ および $15 < S_2[1] < 241$ を満たすために $j_2 \neq 1$ である．また IV_1 は $14 < IV_1 < 240$ である．よって以下の IV_1 を取り除く．

$$
0 \leq IV_1 \leq 14,\ 240 \leq IV_1 \leq 255
$$

この場合，$j_2 = IV_1 + IV_2 + 3$ である．条件 $S_2[2] \neq 0$ を満たすために，$j_2 = IV_1 + IV_2 + 3 \neq 0$ となる．このとき，$IV_1 + IV_2 \neq 253$ となる．$j_2 \neq 1$ であるため，$IV_1 + IV_2 + 3 \neq 1$ となる．このとき，$IV_1 + IV_2 \neq 254$ となる．$S_2[2]$ と $S_2[j_2]$ を入れ替える．入れ替えたのち，$S_2[1] = IV_1 + 1$ および $S_2[2] = IV_1 + IV_2 + 3$ が成立する．条件 $15 < S_2[1] + S_2[2](< 256)$ を満たす場合，以下が成立する．

$$
\begin{aligned}
&15 < IV_1 + 1 + IV_1 + IV_2 + 3 < 256 \\
&\rightarrow 11 < 2IV_1 + IV_2 < 252
\end{aligned}
$$

したがって，$0 \leq 2IV_1 + IV_2 \leq 11$ および $252 \leq 2IV_1 + IV_2 \leq 255$ を取り除く．$IV_2 = 254$ の場合，$j_2 = IV_1 + 1$ となる．このとき，入れ替えたのち $S_2[2]$ は 1 となる．$S_2[1]$ が $15 < S_2[1] < 241$ を満たしているため，条件 $15 < S_2[1] + S_2[2]$ が成立する．取り除く IV の条件をまとめると以下のようになる．

Case 1 $IV_0 = 0$

IV_1 および IV_2 が以下の条件を満たしている場合，IV_1 および IV_2 を取り除く．

$$
\begin{aligned}
&0 \leq IV_1 \leq 14,\ 240 \leq IV_1 \leq 255, \\
&0 \leq 2IV_1 + IV_2 \leq 11,\ 252 \leq 2IV_1 + IV_2 \leq 255, \\
&IV_1 + IV_2 = 253,\ 254,
\end{aligned}
$$

ただし，$IV_2 = 254$ は取り除かない．

IV_0 が他の値をとる場合，IV_1 および IV_2 のフィルタリングパターンは以下のようになる．これらは Case 1 と同様にして得られる．

Case 2 $IV_0 = 1$

IV_1 および IV_2 が以下の条件を満たしている場合，IV_1 および IV_2 を取り除く．

$$
\begin{aligned}
&0 \le IV_1 \le 14,\ 240 \le IV_1 \le 255,\\
&0 \le 2IV_1 + IV_2 \le 11,\ 252 \le 2IV_1 + IV_2 \le 255,\\
&IV_1 + IV_2 = 254,\\
&IV_2 = 254.
\end{aligned}
$$

Case 3 $IV_0 = 2$

IV_1 および IV_2 が以下の条件を満たしている場合，IV_1 および IV_2 を取り除く．

$$
\begin{aligned}
&0 \le IV_1 \le 12,\ 238 \le IV_1 \le 255,\\
&0 \le 2IV_1 + IV_2 \le 9,\ 250 \le 2IV_1 + IV_2 \le 255,\\
&0 \le IV_1 + IV_2 \le 12,\ 254 \le IV_1 + IV_2 \le 255,
\end{aligned}
$$

ただし，$IV_2 = 0$ は取り除かない．

Case 4 $IV_0 = 16$

IV_1 が以下の条件を満たしている場合，IV_1 を取り除く．

$$
\begin{aligned}
&224 \le IV_1 \le 238,\\
&240 \le IV_1 \le 255.
\end{aligned}
$$

このとき，IV_1 の値に依存して IV_2 に 3 つのフィルタリングパターンが考えられる．

Case 4-1 $IV_1 = 223$

IV_2 が以下の条件を満たしている場合，IV_2 を取り除く．

$$
\begin{aligned}
&30 \le IV_2 \le 45,\\
&IV_2 = 14, 15.
\end{aligned}
$$

Case 4-2 $IV_1 = 239$

IV_2 が以下の条件を満たしている場合，IV_2 を取り除く．

$$
\begin{aligned}
&238 \le IV_2 \le 253,\\
&IV_2 = 14, 255.
\end{aligned}
$$

Case 4-3 その他の IV_1

IV_2 が以下の条件を満たしている場合，IV_2 を取り除く．

$$
\begin{aligned}
&220 \le 2IV_1 + IV_2 \le 235,\\
&IV_1 + IV_2 = 238, 253,
\end{aligned}
$$

ただし，$IV_2 = 254$ は取り除かない．

Case 5 $IV_0 = 17, 18, \ldots, 240$

IV_1 が以下の条件を満たしている場合，IV_1 を取り除く．

$$
\begin{aligned}
&0 \le IV_0 + IV_1 \le 14, \\
&240 \le IV_0 + IV_1 \le 254, \\
&IV_1 = 255.
\end{aligned}
$$

このとき，IV_1 の値に依存して IV_2 に 3 つのフィルタリングパターンが考えられる．

Case 5-1 $0 \le 2IV_0 + IV_1 \le 14$ or $2IV_0 + IV_1 = 255$

IV_2 が以下の条件を満たしている場合，IV_2 を取り除く．

$$
\begin{aligned}
&0 \le 2(IV_0 + IV_1) + IV_2 \le 11, \\
&252 \le 2(IV_0 + IV_1) + IV_2 \le 255, \\
&IV_0 + IV_1 + IV_2 = 253, 254.
\end{aligned}
$$

Case 5-2 $IV_0 + IV_1 = 255$

IV_2 が以下の条件を満たしている場合，IV_2 を取り除く．

$$
\begin{aligned}
&IV_1 - 1 \le IV_2 \le IV_1 + 14, \\
&IV_1 + IV_2 = 253, \\
&IV_0 + IV_1 + IV_2 = 254.
\end{aligned}
$$

Case 5-3 その他の IV_1

IV_2 が以下の条件を満たしている場合，IV_2 を取り除く．

$$
\begin{aligned}
&0 \le 2(IV_0 + IV_1) + IV_2 \le 11, \\
&252 \le 2(IV_0 + IV_1) + IV_2 \le 255, \\
&IV_1 + IV_2 = 253, \\
&IV_0 + IV_1 + IV_2 = 254,
\end{aligned}
$$

ただし，$IV_2 = 254$ は取り除かない．

Case 6 $IV_0 = 241, 242, \ldots, 255$

IV_1 が以下の条件を満たしている場合，IV_1 を取り除く．

$$
\begin{aligned}
&0 \le IV_0 + IV_1 \le 14, \\
&240 \le IV_0 + IV_1 \le 255.
\end{aligned}
$$

このとき，IV_1 の値に依存して IV_2 に 2 つのフィルタリングパターンが考えられる．

Case 6-1 $0 \le 2IV_0 + IV_1 \le 14$ or $2IV_0 + IV_1 = 255$

IV_2 が以下の条件を満たしている場合，IV_2 を取り除く．

$$
\begin{aligned}
&0 \le 2(IV_0 + IV_1) + IV_2 \le 11, \\
&252 \le 2(IV_0 + IV_1) + IV_2 \le 255, \\
&IV_0 + IV_1 + IV_2 = 253, 254.
\end{aligned}
$$

Case 6-2 その他の IV_1

IV_2 が以下の条件を満たしている場合，IV_2 を取り除く．

$$
\begin{aligned}
&0 \leq 2(IV_0 + IV_1) + IV_2 \leq 11,\\
&252 \leq 2(IV_0 + IV_1) + IV_2 \leq 255,\\
&IV_1 + IV_2 = 253,\\
&IV_0 + IV_1 + IV_2 = 254,
\end{aligned}
$$

ただし，$IV_2 = 254$ は取り除かない．

Storong IV の取得方法

内部状態およびキーストリームを観測し，Klein-Improved，A_u5_3 bias，SVV_10 bias といった主要な攻撃関数の条件の成立を確認する．Tornado 攻撃の攻撃関数に対応する IV を改良 Strong IV と呼ぶ．改良 Strong IV は以下の手順で生成する．

Step1 weak IV の除去
ランダムに生成した IV に対して上記の IV に対する条件の成立を確認する．条件が成立していた場合は，異なる IV を生成し，再度の条件の確認を行う．

Step2 A_u5_3 bias および SVV_10 bias の除去
RC4 の内部状態およびキーストリームを取得し，投票条件の成立を確認する．

Step3 Klein-Improved の除去
RC4 の内部状態およびキーストリームを取得し，Condition 1 および 2 の成立を確認する．

Step4 改良 Strong IV の決定
全ての攻撃関数の投票条件が不成立の場合，その IV を改良 Strong IV とする．攻撃関数が成立する場合，異なる IV を生成し，Step 1 に戻る．

結果として，改良 Strong IV が得られる．改良 Strong IV は主要な攻撃関数の成立を防ぐため，WEP に対する従来の鍵回復攻撃全てを回避することができる．

4.4.2 改良 Strong IV を用いた安全な WEP の運用

改良 Strong IV を用いた WEP の運用方法について述べる．100,000 パケットごとに WEP 鍵を更新する場合を考える．WEP において改良 Strong IV のみを用いた場合，WEP 鍵の候補の確率が 1/256 より低くなり，WEP 鍵に関する情報が漏洩する．この問題の対策として改良 Strong IV と通常の IV を混合して用いることを考える．改良 Strong IV の個数を

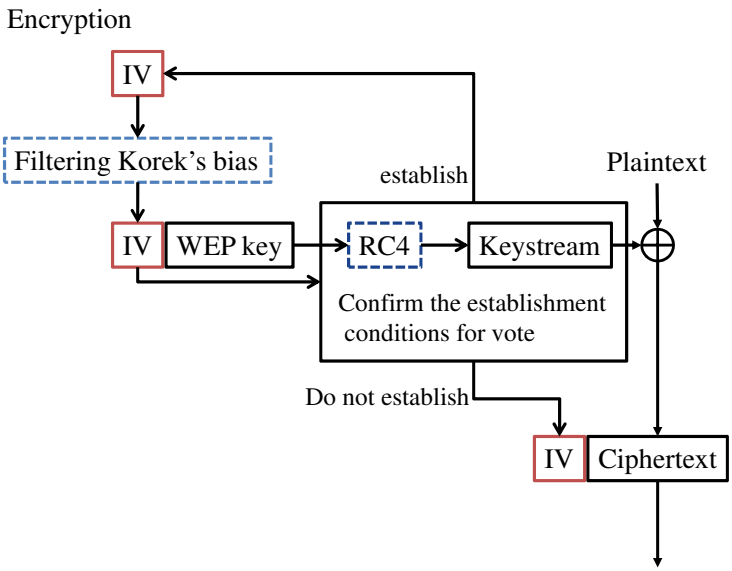

図 4.3: 提案手法の概要

y とおく．混合した IV の通信において，Klein 攻撃の成功確率は

$$\frac{y \cdot \frac{0.63}{256} + (100000 - y) \cdot \frac{1.36}{256}}{100000} = \frac{1}{256}$$
$$y = \frac{100000}{1.36 - 0.63} \cdot 0.36$$
$$y = 49315$$

となる．Klein 攻撃の成功確率は一定であるため，y は一意に決まる．同様に PTW 攻撃および OKM 攻撃に対する改良 Strong IV の個数を導出する．混合した IV の通信において，それぞれの攻撃成功確率は

$$\frac{y \cdot Prob'_{(PTW,x)} + (100000 - y) \cdot Prob_{(PTW,x)}}{100000} = \frac{1}{256}$$

$$\frac{y \cdot Prob'_{(OKM,w)} + (100000 - y) \cdot Prob_{(OKM,w)}}{100000} = \frac{1}{256}$$

で与えられる．これらはそれぞれ x と w に依存するため，改良 Strong IV の個数の最大値と最小値を示す．表 4.2 に PTW 攻撃および OKM 攻撃の成立を妨げる改良 Strong IV の個数を示す．結果として，改良 Strong IV と通常の IV とを 50,000 個づつ混合することで，Klein 攻撃，PTW 攻撃，OKM 攻撃の成功確率が 1/256 になる．混合した IV を利用する場合，通常の IV のみを攻撃者が収集すれば，攻撃が成立する可能性がある．しかし攻撃者は WEP 鍵の値を知らないため，改良 Strong IV と通常の IV の区別ができない．したがって，100,000 パケットの通信において，攻撃成功確率は 1/256 となる．以上より，Klein 攻撃，PTW 攻撃，TeAM-OK 攻撃を 100,000 パケットの通信において防ぐことができる．さ

表 4.2: PTW 攻撃および OKM 攻撃に対する改良 Strong IV の個数

PTW Attack	Maximum	Minimum
#improved Strong IVs	49660	46745
OKM Attack	Maximum	Minimum
#improved Strong IVs	49586	49208

表 4.3: 50,000 パケットの暗号化に要する時間

Data length (byte)	256	1024	1472
RC4 (ms)	104	232	306
Improved Strong IV (ms)	125	260	338
Semi-Improved Strong IV (ms)	111	243	320

らに Tornado 攻撃を防ぐために，改良 Strong IV において Klein 攻撃の条件を回避しない IV を考える．この集合を準改良 Strong IV とする．改良 Strong IV と準改良 Strong IV とを 50,000 個づつ混合することで，Tornado 攻撃を防ぐ通信が可能になる．図 4.3 に提案手法の概要を示す．通信において IV を 4.4.1 項に示した手順で判定する．もし通常の IV であれば，WEP に搭載された手法で異なる IV を生成する．改良 Strong IV あるいは準改良 Strong IV と判定された場合は，パケットの暗号化を行い，送信する．改良 Strong IV は $0.96 \cdot 0.78 = 0.749$ の確率で，準改良 Strong IV は 0.78 の確率で生成される．結果として，混合 IV の生成とパケットの暗号化を同時に行うことができる．

暗号化に要する時間の評価を行う．改良 Strong IV，準改良 Strong IV，通常の IV のそれぞれを用いて 50,000 パケットの暗号化を行う．平文の長さは 256，1024，1472 バイトとする．異なる 1024 個の WEP 鍵に対して実験を行い，その平均値を評価する．実験には Core i3 530 を搭載した PC を用いた．これは家庭用 PC において，提案手法が実行可能であることを示すためである．表 4.3 に実験の結果を示す．表 4.3 より，提案手法は暗号化に WEP と比べて 1.1 倍から 1.2 倍程度の時間を要することがわかる．したがって，提案手法は，100,000 パケットの通信において，安全かつ WEP と同等に高速な通信が可能である．

4.5 結言

本章では，安全な WEP の運用方法を提案した．Klein 攻撃，Korek 攻撃，SVV_10 bias の条件が成立しない IV の集合を示した．この IV を改良 Strong IV と定義し，効率的な生成方法を提案した．提案手法により 100,000 パケットの通信を安全に行うことができる．計算機実験により，提案手法を用いた場合における WEP の暗号化に必要な時間の評価を行った．結果として，WEP と比べて 1.1 から 1.2 倍の時間が必要であることが確認できた．したがって，提案手法は全ての鍵回復攻撃を防ぎ，高速な通信を実現可能である．提案手法は IV の判定プロセスおよび鍵の更新プロセスを導入することで実現できる．よって，提案手法は従来の機器のファームウェアを更新することで導入可能である．

統計的性質に基づく鍵回復攻撃より，今後提案される攻撃も Klein 攻撃の条件を利用すると考えられる．提案手法は，そのような攻撃も防ぐことが可能であると考えられる．

第5章　非線形帰還シフトレジスタ型ストリーム暗号に対する条件付差分解読法

5.1　緒言

近年，非線形帰還シフトレジスタ (NLFSR) によって構成されたストリーム暗号が提案されている [24, 23]．NLFSR 型ストリーム暗号では初めに秘密鍵と初期化ベクトル (IV) をレジスタに入力する．この状態を初期状態と呼ぶ．NLFSR 型ストリーム暗号では鍵と IV を撹拌し，キーストリームを生成する．Hell らによって設計された Grain v1[23] は最も有名な NLFSR 型ストリーム暗号の一つであり，eSTREAM においてハードウェア暗号の一つに選択されている [40]．

Grain v1 に対する様々な解析が行われてきた．Lee らは関連鍵の脆弱性を用いて鍵回復攻撃を示した [41]．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．Cannière らは Grain v1 における関連鍵攻撃を提案した [42]．Knellwolf らは関連鍵設定において条件付差分解読法を提案した [43]．この解読法では鍵初期化の両方向について解析を行い，条件の設定を行う．

Cannière らは 112 段の Grain v1 について単一鍵攻撃を提案した．しかしこの攻撃は 2^{72} 個の選択 IV が必要であり，IV の総数より多くの選択 IV が必要になるため，実現不可能な攻撃である．Grain v1 に対する実現可能な単一鍵攻撃として，Knellwolf らによって提案された条件付差分解読法がある [25]．この手法は NLFSR 型の暗号である KATAN や Grain v1，Grain-128 に適用されている．条件付差分解読法において，攻撃者は初期状態に条件を入力し，多くの段数の差分特性を得る．得られた特性により識別攻撃を構築する．彼らは単一鍵設定において 2^{35} 個の選択 IV を利用して 104 段の Grain v1 に対して識別攻撃および鍵回復攻撃を行った．2014 年には Banik によって 105 段の識別攻撃および鍵回復攻撃が示された [44]．さらに Sarkar によって 106 段の識別攻撃が提案された [45]．表 5.1 に従来の結果を示す．

一般的に NLFSR 型のストリーム暗号は鍵初期化処理の巻き戻しが可能である．前述のとおり，従来の条件付差分解読法では関連鍵設定において，順方向と逆方向の鍵初期化を解析して条件付差分特性を取得している [43]．この攻撃では 1 つの差分が存在する状態を中間状態と仮定して，鍵初期化を二つに分割する．逆方向では，条件の数が少なくなるように条件を設定するとともに，中間状態と初期状態の間の条件付差分特性を探索する．順方向では，初期状態とキーストリームとの間の条件付差分特性を探索する．この手法により初期状態に複数ビットの差分が入力されている場合において，条件付差分特性を探索することが可能である．一方で差分が鍵に拡散しやすいため，関連鍵設定のみでこの手法が利用されている．

従来の条件付差分解読法では，関連鍵設定においてのみ鍵初期化処理の両方向の解析を

表 5.1: Grain v1 の解析結果

段数	IV 数	鍵の仮定	攻撃の種類	Related key の数	参考
97	2^{27}	Single key	鍵回復攻撃	なし	[25]
104	2^{35}	Single key	鍵回復攻撃	なし	[25]
105	2^{32}	Single key	鍵回復攻撃	なし	[44]
106	2^{23}	Single key	識別攻撃	なし	[45]
114	2^{32}	Weak key	鍵回復攻撃	なし	5.4 節
133	2^{35}	Related key	鍵回復攻撃	2	[43]
160	$2^{22.59}$	Related key	鍵回復攻撃	3	[41]
160	2^{55}	Related key	鍵回復攻撃	2	[42]

利用している．関連鍵の仮定なしに，この技術を利用する方法を検討する．具体的には差分の鍵への拡散を妨げるように逆方向の解析方法を考える．

本研究では，NLFSR 型ストリーム暗号に対する新たな条件付差分解読法を提案する．我々は関連鍵の仮定なしに逆方向の解析を効率的に行う方法について述べる．逆方向の解析において，初期状態の差分の数を減少するように条件付差分特性を探索する．具体的には，差分の拡散を妨げるように条件を決定する．結果として，関連鍵の仮定なしに条件付差分特性を得ることができる．一方で，初期状態における条件が増加し，鍵に条件を設定するため，weak key の下で有効な解読法となる．

提案手法を Grain v1 に適用し，識別攻撃および鍵回復攻撃を提案する．Grain v1 は 80 ビットの秘密鍵と 64 ビットの IV を持つ．提案手法では条件として，39 ビットの鍵と 24 ビットの IV を固定する．さらに鍵と IV が関連する条件が一つ存在する．提案手法による条件付差分特性は 2^{40} 個の weak key を持つ．結果として Grain v1 に対して 2^{32} 個の選択 IV から 114 段の識別攻撃が得られる．114 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う．さらに識別攻撃を利用した鍵回復攻撃を提案する．鍵と IV が関連する条件と識別攻撃の成立の関係から，鍵の情報が 1 ビット得られる．2^{33} の計算量で 1 ビットの鍵回復攻撃が成立する．さらに残りの 40 ビットの weak key を全数探索することで，41 ビットの鍵が計算量 $2^{40.01}$ で復元できる．表 5.1 に本研究の結果を示す．

5.2 Grain v1 とその解析

5.2.1 ストリーム暗号 Grain v1

Grain v1 は 2005 年に Hell，Johansson，Meier によって提案されたハードウェア指向のストリーム暗号である [23]．Grain v1 は二つのシフトレジスタから構成されており，80 ビットの秘密鍵 K と 64 ビットの初期化ベクトル IV を持つ．図 5.1 に Grain v1 の構成を示す．80 ビットの線形帰還シフトレジスタ (LFSR:Linear Feedback Shift Register) により更新される状態を $(s_0, s_1, \ldots, s_{79})$，80 ビットの非線形帰還シフトレジスタ (NLFSR) により更新される状態を $(b_0, b_1, \ldots, b_{79})$ とおく．状態 s および b のインデックスを $i(0 \leq i \leq 79)$ とおく．段数を t とおく．よって s_i^t および b_i^t は t 段目の内部状態のビットを表す．Grain v1 の更新

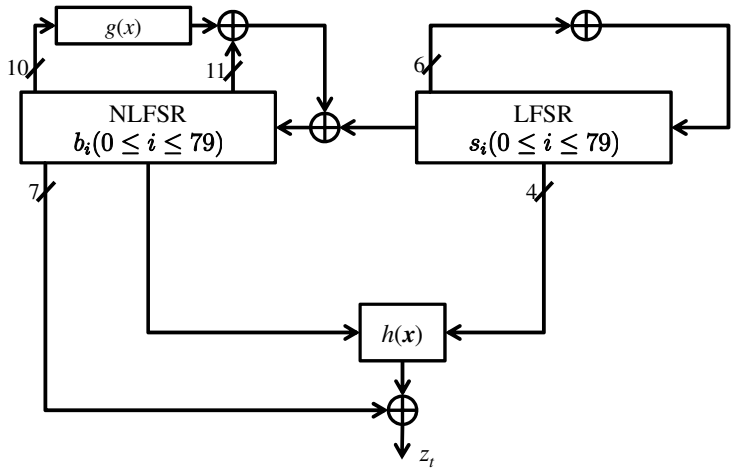

図 5.1: Grain v1 の構成

関数は以下で与えられる．

$$
\begin{aligned}
s_{79}^{t+1} &= f(s^t) \\
&= s_0^t \oplus s_{13}^t \oplus s_{23}^t \oplus s_{38}^t \oplus s_{51}^t \oplus s_{62}^t \\
b_{79}^{t+1} &= s_0^t \oplus g(b^t) \\
&= s_0^t \oplus b_0^t \oplus b_9^t \oplus b_{14}^t \oplus b_{21}^t \oplus b_{28}^t \oplus b_{33}^t \oplus b_{37}^t \oplus b_{45}^t \oplus b_{52}^t \oplus b_{60}^t \oplus b_{62}^t \\
&\quad \oplus b_9^t b_{15}^t \oplus b_{33}^t b_{37}^t \oplus b_{60}^t b_{63}^t \\
&\quad \oplus b_{21}^t b_{28}^t b_{33}^t \oplus b_{45}^t b_{52}^t b_{60}^t \\
&\quad \oplus b_9^t b_{28}^t b_{45}^t b_{63}^t \oplus b_{15}^t b_{21}^t b_{60}^t b_{63}^t \oplus b_{33}^t b_{37}^t b_{52}^t b_{60}^t \\
&\quad \oplus b_9^t b_{15}^t b_{21}^t b_{28}^t b_{33}^t \oplus b_{37}^t b_{45}^t b_{52}^t b_{60}^t b_{63}^t \\
&\quad \oplus b_{21}^t b_{28}^t b_{33}^t b_{37}^t b_{45}^t b_{52}^t
\end{aligned}
$$

キーストリームの出力関数は以下のとおりである．

$$
\begin{aligned}
z_t &= \sum_{j \in \mathcal{A}} b_j^t \oplus h(b_{63}^t, s_3^t, s_{25}^t, s_{46}^t, s_{64}^t) \\
&= b_1^t \oplus b_2^t \oplus b_4^t \oplus b_{10}^t \oplus b_{31}^t \oplus b_{43}^t \oplus b_{56}^t \oplus b_{63}^t \oplus s_{25}^t \\
&\quad \oplus s_3^t s_{64}^t \oplus s_{46}^t s_{64}^t \oplus b_{63}^t s_{64}^t \oplus s_3^t s_{25}^t s_{46}^t \oplus s_3^t s_{46}^t s_{64}^t \\
&\quad \oplus b_{63}^t s_3^t s_{46}^t \oplus b_{63}^t s_{25}^t s_{46}^t \oplus b_{63}^t s_{46}^t s_{64}^t
\end{aligned}
$$

ここで $\mathcal{A} = \{1, 2, 4, 10, 31, 43, 56\}$ である．

Grain v1 は鍵初期化部とキーストリーム生成部から構成される．初めに NLFSR に K を，LFSR に IV を入力する．LFSR の残りのビットには 1 を入力する．図 5.2 に鍵初期化部の構成を示す．鍵初期化部では K および IV を撹拌し，内部状態の初期化を行う．鍵初期化

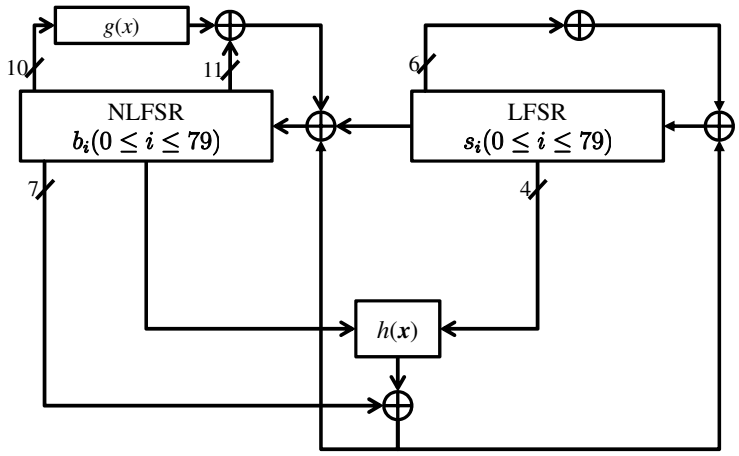

図 5.2: 鍵初期化部の構成

部での更新関数は以下のとおりである．

$$z_t = \sum_{j \in \mathcal{A}} b_j^t \oplus h(b_{63}^t, s_3^t, s_{25}^t, s_{46}^t, s_{64}^t)$$
$$s_{79}^{t+1} = f(s^t) \oplus z_t$$
$$b_{79}^{t+1} = s_0^t \oplus g(b^t) \oplus z_t$$

更新は 160 回行われる．

5.2.2 条件付差分解読法

2010 年に Knellwolf らが条件付差分解読法を提案した [25]．条件付差分解読法は差分解読法の一種である，NLFSR 型ストリーム暗号の解析に適している．この攻撃では差分の拡散を妨げるように秘密鍵や IV に条件を設定し，最初に出力されるキーストリームにおける差分の bias を観測する．観測された bias を用いて識別攻撃などを行う． この攻撃について簡単に述べる．図 5.3 に概要を示す．IV に 1 ビットの差分を入力したとき，鍵初期化における更新関数によって差分が拡散する．攻撃者は鍵初期化処理における差分の拡散を観測する．このとき，差分の拡散を抑制するように初期状態の条件の解析を行う．このようにして条件付差分特性を取得し，キーストリームにおける識別攻撃を構成する．Grain v1 への適用例として，Knellwolf らは 97 段までの識別攻撃および鍵回復攻撃を実験的に示した．さらに 104 段に拡張した攻撃を示した．Banik は 97 段の結果に対して理論的な定義を与え [46]，識別攻撃および鍵回復攻撃を 105 段に改良した [44]．Sarkar は同様の手法を用いて 106 段の識別攻撃を示した [45].

Knellwolf は関連鍵設定における条件付差分解読法を提案している [43]．手法の概要を図 5.4 に示す．この手法では条件付差分特性を取得するために，順方向の鍵初期化処理と逆方向の鍵初期化処理を用いて解析を行っている．

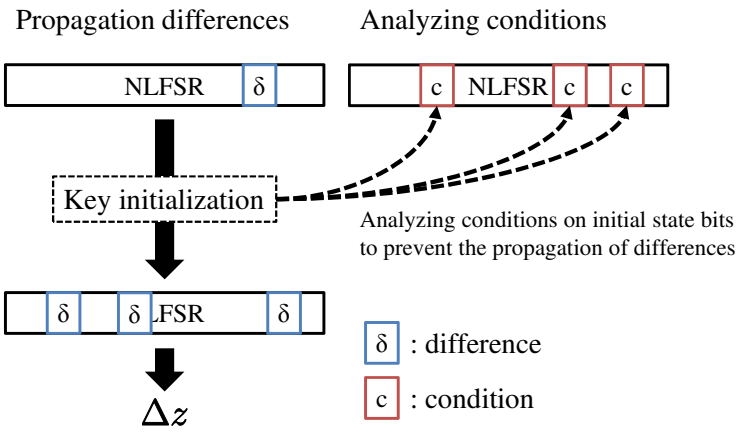

図 5.3: 従来手法の概要 (single-key setting)

5.3 新しい条件付差分解読法

従来の攻撃は条件付差分特性を得るために鍵初期化について順方向と逆方向の両方を解析する．逆方向の解析において，条件の数が少なくなるように条件を決定している．しかしながら，初期状態に多くの差分が拡散してしまう．したがって，この技術は関連鍵設定においてのみ利用されている．本節では，関連鍵設定に基づいていない場合において鍵初期化処理の両方向の解析が有効であることを示す．図 5.5 に提案手法の概要を示す．

5.3.1 鍵初期化処理における差分の拡散

一般的に更新関数は線形関数と非線形関数に分解できる．NLFSR 型ストリーム暗号の内部状態を S，S のインデックスを $j(0 \leq j \leq j_{MAX})$ とおく．T 段目の内部状態ビットは S_j^T で表す．内部状態 S において，線形演算で利用されるビットのインデックスの集合を A とし，A にインデックスが含まれる内部状態ビットの集合を S_A とおく．具体的には $S_A = [S_{j_0}, S_{j_1}, \ldots, S_{j_l}]$，ただし $A = \{j_0, j_1, \ldots, j_l\}$ と表される．同様に内部状態 S において，非線形演算で利用されるビットのインデックスの集合を B とし，B にインデックスが含まれる内部状態ビットの集合を S_B とおく．線形関数および非線形関数を f_A と f_B で表記する．NLFSR 型ストリーム暗号の更新関数は

$$S_{j_{MAX}}^{T+1} = S_0^T \oplus f_A(S_A^T) \oplus f_B(S_B^T)$$

となる．上式より，逆方向の更新関数は

$$S_0^T = S_{j_{MAX}}^{T+1} \oplus f_A(S_A^T) \oplus f_B(S_B^T)$$

で表される．図 5.6 に逆方向の更新関数の例を示す．$S_{j_{MAX}}^{T+1}$ の差分を $\Delta S_{j_{MAX}}^{T+1}$ とする．このとき，$\Delta S_{j_{MAX}}^{T+1}$ は

$$\Delta S_{j_{MAX}}^{T+1} = \Delta S_0^T \oplus \Delta f_A(S_A^T) \oplus \Delta f_B(S_B^T)$$

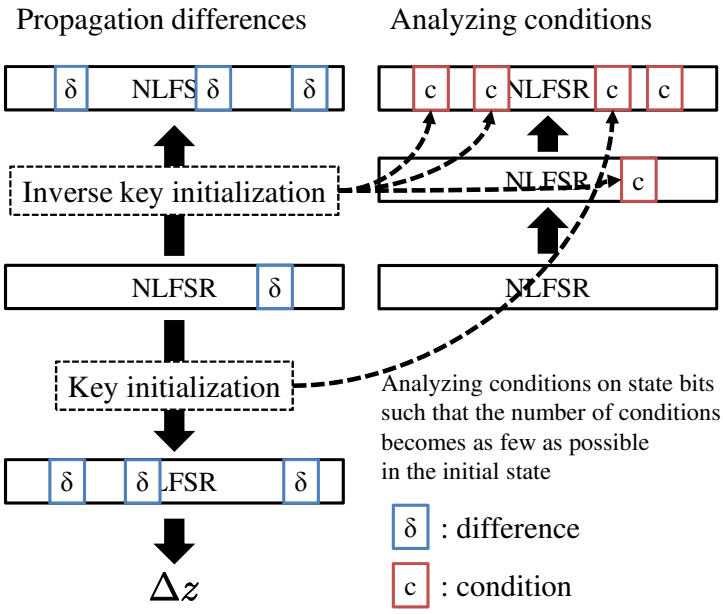

図 5.4: 従来手法の概要 (related-key setting)

から計算される．ただし，ΔS_0^T，$\Delta f_A(S_A^T)$，$\Delta f_B(S_B^T)$ はそれぞれ S_0^T，$f_A(S_A^T)$，$f_B(S_B^T)$ の差分を表している．よって ΔS_0^T は

$$\Delta S_0^T = \Delta S_{j_{MAX}}^{T+1} \oplus \Delta f_A(S_A^T) \oplus \Delta f_B(S_B^T)$$

から計算される．逆方向において，$\Delta S_{j_{MAX}}^{T+1}$ および S_A^T，S_B^T 中の内部状態ビットが同時に差分を持つ場合，既に差分が内部状態全体に拡散していると考えられる．したがって，このような場合は解析を行わない．S_B に差分ビットが存在した場合，非線形演算を経るため $\Delta f_B(S_B)$ の出力が不明になる．このとき，更新ビットの差分について以下の 4 つのケースが考えられる．

Case 0 $\Delta f_A(S_A) = 0$ and $\Delta f_B(S_B) = 0$

Case 1 $\Delta f_A(S_A) = 1$ and $\Delta f_B(S_B) = 0$

Case 2 $\Delta f_A(S_A) = 0$ and $\Delta f_B(S_B) =$ unknown

Case 3 $\Delta f_A(S_A) = 1$ and $\Delta f_B(S_B) =$ unknown

順方向の解析においては，差分の拡散を観測する．逆方向の解析においては条件を設定し，条件付差分特性の探索を行う．Case 0 においては差分の拡散は発生しない．図 5.7 に逆方向における Case 1，2，3 を示す．$\Delta S_{j_{MAX}}^{T+1} = 0$ の場合を考える．Case 1 において，$\Delta S_0^T = 1$ のように差分が拡散する．Case 2 において，$\Delta f_B(S_B) = 0$ を満たすように条件を設定し，差分の拡散を防止する．これらは従来手法と同様である．一方で，Case 3 において従来とは異なるアプローチを取る．

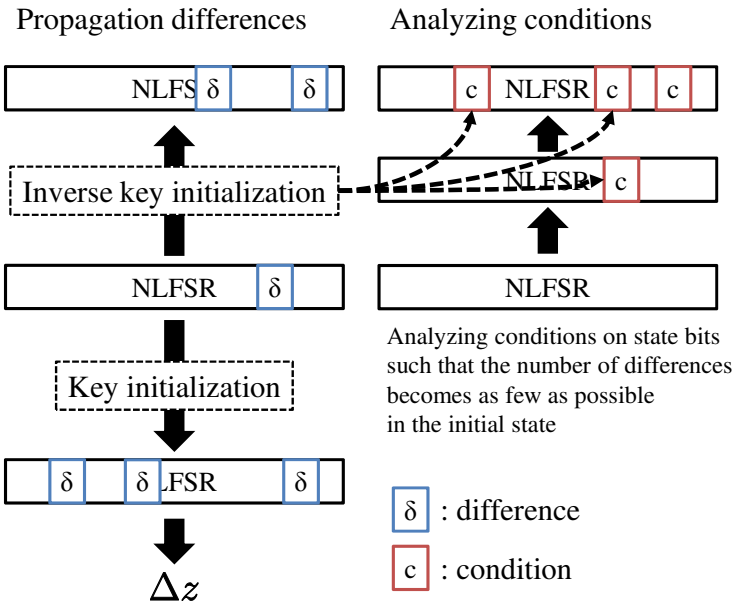

図 5.5: 提案手法の概要

5.3.2 Case 3 の解析

簡単のために，8 ビットの NLFSR 型ストリーム暗号を考える．内部状態ビットを $S_j(0 \leq j \leq 7)$ とおく．T 段目の内部状態ビットは S_j^T で表す．逆方向の更新関数を以下のように定義する．

$$S_0^{T-1} = S_7^T \oplus S_2^T \oplus S_2^T S_4^T S_5^T \tag{5.1}$$

この場合，$f_A(S_A) = S_2^T$，$f_B(S_B) = S_2^T S_4^T S_5^T$ となる．内部状態ビットの差分を ΔS_j^T とする．

従来手法における Case 3 の解析

Case 3 において，従来手法は $\Delta f_B(S_B) = 0$ を満たすように条件を設定し，$\Delta S_0^{T-1} = 1$ のように差分を拡散する．式 (5.1) を用いて Case 3 の処理を説明する．$\Delta S_2^T = 1$ と仮定した場合，$\Delta f_B(S_B) = \Delta(S_2^T S_4^T S_5^T)$ は未知となる．このとき従来手法では

$$S_4^T S_5^T = 0$$

を満たすように条件を設定する．この場合，差分 $\Delta S_0^{T-1} = 1$ が拡散する．したがって，差分の拡散が抑制されないため，初期状態全体に差分が拡散する．

提案手法における Case 3 の解析

Case 3 において，我々は差分の拡散を抑制するように条件を設定し，初期状態における差分の数を可能な限り少なくする．二つのルールを考える．一つ目は，$\Delta f_B(S_B) = 0$ を満

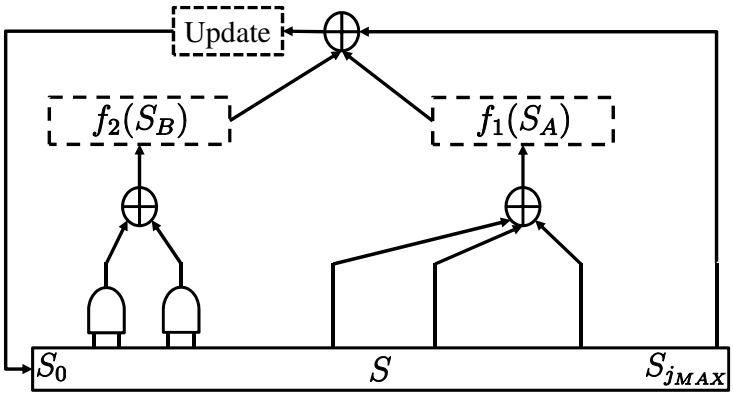

図 5.6: 逆方向の更新関数

たすように条件を設定することにより差分を拡散する．この拡散させた差分を後のラウンドで Case 1 の発生を回避するために利用する．二つ目は，$\Delta f_B(S_B) = 1$ とを満たすように条件を設定することにより S_0^{T-1} への差分の拡散を妨げる．条件の設定には 5.3.3 項で後述する定理 2 を利用する．内部状態ビットに既に条件が設定されている場合は，その値を差分の計算に利用する．式 (5.1) を用いて $\Delta f_B(S_B) = 1$ の場合の処理を説明する．$\Delta S_2^T = 1$ と仮定した場合，$\Delta f_B(S_B) = \Delta(S_2^T S_4^T S_5^T)$ は未知となる．このとき

$$S_4^T S_5^T = 1$$

を満たすように条件を設定する．具体的には $S_4^T = 1$，$S_5^T = 1$ という二つの条件を設定する．この場合，S_0^{T-1} への差分の拡散を防ぐことができる．上述の通り，従来手法では一つの条件を設定し，S_0^{T-1} へ差分を拡散している．提案手法では，従来より多くの条件が必要になるが，内部状態への差分の拡散を抑制することができる．

我々は上記の二つのルールを利用して，最終的に初期状態への差分の拡散を抑制する．結果として，初期状態における差分の数を減らすことができるため，関連鍵設定なしに条件付差分特性を取得することが可能である．しかしながら多くの条件が必要となるため，発見された特性は weak-key setting において有効に働く．

5.3.3 $\Delta f_B(S_B) = 1$ に対する条件

内部状態において $j \in B$ である S_j に差分が入力されている場合，$\Delta f_B(S_B)$ の出力は不明になる．もし S_B における他のビットの値が既知であれば，未知の出力差分の値を決定することができる．非線形演算における差分と内部状態ビットの間の関係について述べる．$j \in B$ であるポインタを $j_0, j_1, \ldots, j_n$ とおく．$S_{j_0}, S_{j_1}, \ldots, S_{j_n}$ における差分をそれぞれ $\Delta S_{j_0}, \Delta S_{j_1}, \ldots, \Delta S_{j_n}$ と表記する．また非線形演算 $S_{j_0} \wedge S_{j_1} \wedge \ldots \wedge S_{j_n}$ の出力差分を $\Delta(S_{j_0} \wedge S_{j_1} \wedge \ldots \wedge S_{j_n})$ とおく．よって $\Delta(S_{j_0} \wedge S_{j_1} \wedge \ldots \wedge S_{j_n})$ は $\Delta f_B(S_B)$ に相当する．S_B における差分の数を $m(1 \leq m \leq n-1)$ とする．非線形演算と内部状態の間に以下のような関係が存在する．

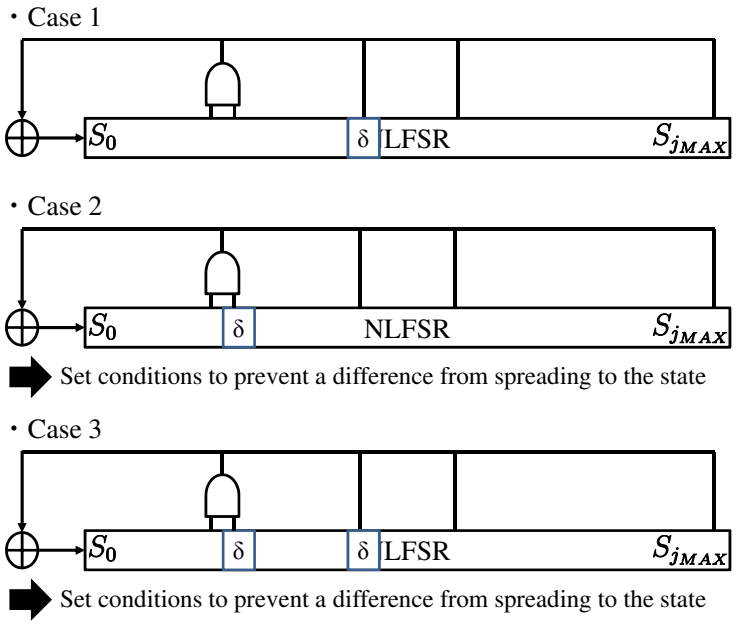

図 5.7: 逆方向の鍵初期化処理における差分の拡散

定理 2. 差分および内部状態の値について $\Delta S_{j_0} = \Delta S_{j_1} = \cdots = \Delta S_{j_{m-1}} = 1$ と $\Delta S_{j_m} = \Delta S_{j_{m+1}} = \cdots = \Delta S_{j_n} = 0$ を仮定した場合，条件とし $S_{j_0} = S_{j_1} = \cdots = S_{j_{m-1}}$ および $S_{j_m} = S_{j_{m+1}} = \cdots = S_{j_n} = 1$ を設定する．このとき，$\Delta(S_{j_0} \wedge S_{j_1} \wedge \cdots \wedge S_{j_n}) = 1$ となる．

証明. 差分を含む非線形演算を考える．この演算は

$$
\begin{aligned}
& f_B(S_B) \oplus \Delta f_B(S_B) \\
&= (S_{j_0} \oplus \Delta S_{j_0}) \wedge (S_{j_1} \oplus \Delta S_{j_1}) \wedge \cdots \wedge (S_{j_n} \oplus \Delta S_{j_n}) \\
&= (S_{j_0} \wedge S_{j_1} \wedge \cdots \wedge S_{j_n}) \oplus \Delta(S_{j_0} \wedge S_{j_1} \wedge \ldots \wedge S_{j_n})
\end{aligned}
$$

と表せる．このとき，$\Delta S_{j_0} = \Delta S_{j_1} = \cdots = \Delta S_{j_{m-1}} = 1$，$\Delta S_{j_m} = \Delta S_{j_{m+1}} = \cdots = \Delta S_{j_n} = 0$, $S_{j_0} = S_{j_1} = \cdots = S_{j_{m-1}}$, and $S_{j_m} = S_{j_{m+1}} = \cdots = S_{j_n} = 1$ と仮定しても一般性を失わない．式 $\Delta f_B(S_B) = \Delta(S_{j_0} \wedge S_{j_1} \wedge \ldots \wedge S_{j_n})$ は

$$
\begin{aligned}
\Delta f_B(S_B) &= \Delta(S_{j_0} \wedge S_{j_1} \wedge \cdots \wedge S_{j_n}) \\
&= \Delta S_{j_0} \wedge \Delta S_{j_1} \wedge \cdots \wedge \Delta S_{j_{m-1}} \\
&\quad \wedge S_{j_m} \wedge S_{j_{m+1}} \wedge \cdots \wedge S_{j_n} = 1
\end{aligned}
$$

となる．したがって，$\Delta S_{j_0} = \Delta S_{j_1} = \cdots = \Delta S_{j_{m-1}} = 1$ と仮定した場合，$S_{j_0} = S_{j_1} = \cdots = S_{j_{m-1}}$ and $S_{j_m} = S_{j_{m+1}} = \cdots = S_{j_n} = 1$ のように条件を設定する．結果として，$\Delta(S_{j_0} \wedge S_{j_1} \wedge \cdots \wedge S_{j_n}) = 1$ が得られる． □

差分の個数が $1 < m$ の場合，$S_{j_0}, S_{j_1}, \ldots, S_{j_{m-1}}$ は差分と条件の両方を持つ．この場合，条件付差分特性を得るためにより強力な仮定が必要となるため，解析には利用できない．したがって $m = 1$ の場合のみを考える．

5.4 Grain v1 に対する識別攻撃および鍵回復攻撃

本節では Grain v1 に対する識別攻撃および鍵回復攻撃について述べる．5.3 節で述べた手法を利用して条件付差分特性を構成する．その条件付差分特性を利用して識別攻撃を得る．提案手法により weak-key setting において 114 段の識別攻撃が理論的に取得する．また 2^{32} 個の選択 IV から実験的に提案する識別攻撃を確認する．さらに鍵回復攻撃について述べる．先述の識別攻撃によりランダムに選択した鍵と weak key とを識別する．weak key を識別したのち，鍵と IV の間の条件より 1 ビットの鍵の情報を復元する．

Grain v1 のアルゴリズムより，逆方向の鍵初期化のアルゴリズムは

$$
\begin{aligned}
s_0^{t'} &= s_{12}^{t'+1} \oplus s_{22}^{t'+1} \oplus s_{37}^{t'+1} \oplus s_{50}^{t'+1} \oplus s_{61}^{t'+1} \oplus s_{79}^{t'+1} \oplus z_{t'}, \\
b_0^{t'} &= s_0^{t'} \oplus b_8^{t'+1} \oplus b_{13}^{t'+1} \oplus b_{20}^{t'+1} \oplus b_{27}^{t'+1} \oplus b_{32}^{t'+1} \oplus b_{36}^{t'+1} \oplus b_{44}^{t'+1} \oplus b_{51}^{t'+1} \oplus b_{59}^{t'+1} \oplus b_{61}^{t'+1} \oplus b_{79}^{t'+1} \\
&\quad \oplus b_8^{t'+1} b_{14}^{t'+1} \oplus b_{32}^{t'+1} b_{36}^{t'+1} \oplus b_{59}^{t'+1} b_{62}^{t'+1} \\
&\quad \oplus b_{20}^{t'+1} b_{27}^{t'+1} b_{32}^{t'+1} \oplus b_{44}^{t'+1} b_{51}^{t'+1} b_{59}^{t'+1} \\
&\quad \oplus b_8^{t'+1} b_{27}^{t'+1} b_{44}^{t'+1} b_{62}^{t'+1} \oplus b_{14}^{t'+1} b_{20}^{t'+1} b_{59}^{t'+1} b_{62}^{t'+1} \oplus b_{32}^{t'+1} b_{36}^{t'+1} b_{51}^{t'+1} b_{59}^{t'+1} \\
&\quad \oplus b_8^{t'+1} b_{14}^{t'+1} b_{20}^{t'+1} b_{27}^{t'+1} b_{32}^{t'+1} \oplus b_{36}^{t'+1} b_{44}^{t'+1} b_{51}^{t'+1} b_{59}^{t'+1} b_{62}^{t'+1} \\
&\quad \oplus b_{20}^{t'+1} b_{27}^{t'+1} b_{32}^{t'+1} b_{36}^{t'+1} b_{44}^{t'+1} b_{51}^{t'+1} \oplus z_{t'}, \\
z_{t'} &= b_0^{t'+1} \oplus b_1^{t'+1} \oplus b_3^{t'+1} \oplus b_9^{t'+1} \oplus b_{30}^{t'+1} \oplus b_{42}^{t'+1} \oplus b_{55}^{t'+1} \oplus b_{62}^{t'+1} \oplus s_{24}^{t'+1} \\
&\quad \oplus s_2^{t'+1} s_{63}^{t'+1} \oplus s_{45}^{t'+1} s_{63}^{t'+1} \oplus b_{62}^{t'+1} s_{63}^{t'+1} \\
&\quad \oplus s_2^{t'+1} s_{24}^{t'+1} s_{45}^{t'+1} \oplus s_2^{t'+1} s_{45}^{t'+1} s_{63}^{t'+1} \oplus b_{62}^{t'+1} s_2^{t'+1} s_{45}^{t'+1} \\
&\quad \oplus b_{62}^{t'+1} s_{24}^{t'+1} s_{45}^{t'+1} \oplus b_{62}^{t'+1} s_{45}^{t'+1} s_{63}^{t'+1}
\end{aligned}
$$

となる．$s_i^{t'}$，$b_i^{t'}$，$z_{t'}$ の差分をそれぞれ $\Delta s_i^{t'}$，$\Delta b_i^{t'}$，$\Delta z_{t'}$ とおく．

5.4.1 条件付差分特性の構成

逆方向の鍵初期化を解析し，条件付差分特性を取得する．非線形演算に利用されるビットに差分が入力された場合，初期状態における差分の数が少なくなるように条件を探索する．本論文では，逆方向の鍵初期化について 24 段の解析を行い，条件付差分特性を得る．表 5.2 に全てのラウンドにおける差分の位置を示す．表 5.2 より，非線形演算に利用される差分の位置は (s_2)，(s_{24})，(s_{45}) である．後述する 5.5.1 項において，それぞれの位置の差分について条件の決定方法を説明する．

内部状態の条件は $s_4^0 = 0$，$s_{25}^0 = 0$，$s_{44}^0 = 0$，$s_{65}^0 = 1$，$s_{68}^0 = 1$，$b_{79}^3 = 0$，$b_{79}^6 = 0$，$s_{79}^4 = 1$ となる．このうち $b_{79}^3 = 0$，$b_{79}^6 = 0$，$s_{79}^4 = 1$ を満たすために初期状態に条件を設定する．5.5.2 項に上記を満たす条件を決定する方法を後述する．結果として内部状態の条件は以下のように与えられる．

- Condition of both key and IV: $k_{13} = x_{54}$
- Condition $k = 0$: $k_3, k_4, k_6, k_7, k_9, k_{11}, k_{12}, k_{14}, k_{15}, k_{16}, k_{19}, k_{23}, k_{26}, k_{30}, k_{33}, k_{34}, k_{35}, k_{36}, k_{38}, k_{39}, k_{42}, k_{45}, k_{46}, k_{47}, k_{48}, k_{50}, k_{54}, k_{57}, k_{58}, k_{59}, k_{61}, k_{62}, k_{64}, k_{65}, k_{66}, k_{67}, k_{68}$

表 5.2: Positions of differences for the weak-key setting

Round	Positions on the LFSR	Round	Positions on the LFSR
0	s_1, s_{22}, s_{47}	12	s_{10}, s_{35}
1	s_0, s_{21}, s_{46}	13	s_9, s_{34}
2	s_{20}, s_{45}	14	s_8, s_{33}
3	s_{19}, s_{44}	15	s_7, s_{32}
4	s_{18}, s_{43}	16	s_6, s_{31}
5	s_{17}, s_{42}	17	s_5, s_{30}
6	s_{16}, s_{41}	18	s_4, s_{29}
7	s_{15}, s_{40}	19	s_3, s_{28}
8	s_{14}, s_{39}	20	s_2, s_{27}
9	s_{13}, s_{38}	21	s_1, s_{26}
10	s_{12}, s_{37}	22	s_0, s_{25}
11	s_{11}, s_{36}	23	s_{24}

- Condition $k = 1$: k_2, k_5
- Condition $x = 0$: $x_2, x_4, x_6, x_8, x_{15}, x_{16}, x_{18}, x_{25}, x_{26}, x_{27}, x_{28}, x_{30}, x_{40}, x_{41}, x_{43}, x_{44}, x_{48}, x_{49}, x_{51}, x_{53}, x_{56}$
- Condition $x = 1$: x_3, x_5

これらの条件は発見的に得られたものである．条件より weak key および IV は 40 ビットの自由に選択可能な領域を持つ．この領域におけるビットを free bit と呼ぶ．結果として，逆方向の解析により 24 段の条件付差分特性を構成する．

順方向の鍵初期化処理において差分の拡散を観測し，キーストリームにおいて特徴的な差分 $\Delta z_{t'}$ を探索する．s_{23} に差分を入力した場合，47 段の差分特性が得られる．この場合，特徴的な差分として $\Delta z_{47} = 1$ を取得する．

両方向の解析から得られた差分特性を結合する．したがって，71(24+47) 段の条件付差分特性が得られる．この特性は確率 1 で発生する．

条件付差分特性の拡張を考える．このとき条件付差分特性において，キーストリームを出力する内部状態における既知差分の数から特性を評価する．一定の段数だけ延長した後に，出力関数に多くの既知差分が入力されていれば，その特性を識別攻撃を得るために利用する．本研究では，114 段の条件付差分特性を利用する．図 5.8 に 114 段の条件付差分特性を示す．図中の黒点が既知の差分を，灰色の点が未知の差分を表す．

5.4.2 114 段の識別攻撃

114 段の条件付差分特性を利用した識別攻撃について述べる．このとき，最初に出力されるキーストリームを z_{114} とおく．5.4.1 項で取得した条件付差分特性を利用し，キーストリームの差分が $\Delta z_{114} = 0$ に偏っていることを発見する．差分を用いた識別攻撃について説明する．内部状態を X_0 とおく．X_0 に条件を設定した鍵および IV を入力する．X_0 に差分を入力した状態を X'_0 とおく．X_0 および X'_0 から初めに出力される差分をそれぞれ Z_0, Z'_0 とおく．Z_0 と Z'_0 の排他的論理和をとることでキーストリームの差分を得る．IV の値を

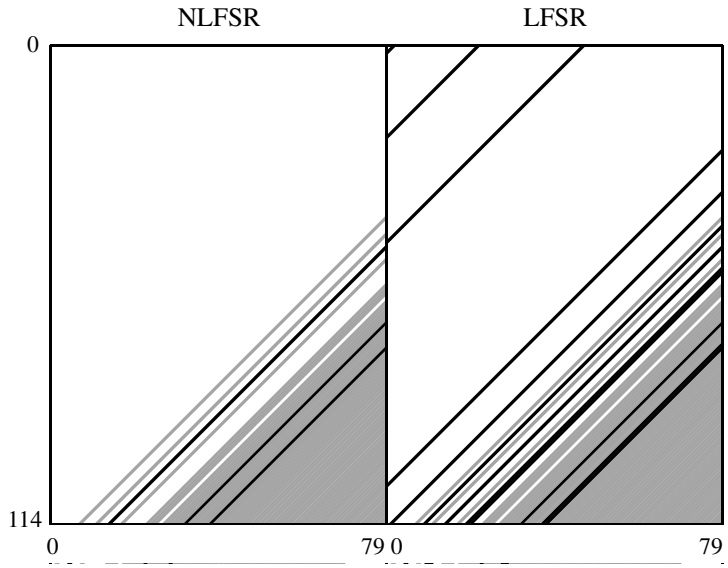

図 5.8: 114 段の条件付差分特性

ランダムに変更し，キーストリームの差分を観測する．結果として，114 段の初期化の後に初めて出力されるキーストリームの差分の値について偏りを発見する．理論的な確率は 0.500119 となる．詳細は後述する．

正規分布により識別攻撃に利用するバイアスの妥当性を評価する．正規分布における上側累積確率は以下のように導出される．

$$Q(y,\mu,\sigma) = \frac{1}{\sqrt{2\pi}\sigma}\int_{y}^{\infty} e^{-\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2} dt$$

ここで y，μ，σ はそれぞれパーセント点，平均，標準偏差を表している．N 個の選択 IV を利用する場合，$\mu = \frac{N}{2}$，$\sigma^2 = \frac{N}{4}$ となる．パーセント点 y ごとに上側累積確率を計算する．上側累積確率が 2^{-80} より小さくなる場合，分布の偏りが妥当であると判断する．正規分布によるキーストリームの差分の確率を $\Pr(\Delta z_{114} = 0)_{nd}$ とおく．提案手法により得られた $\Pr(\Delta z_{114} = 0)$ が $\Pr(\Delta z_{114} = 0)_{nd}$ より大きければ，妥当な bias であると考える．

キーストリームの差分がランダムに分布する場合に 2^{32} のサンプル数で分布を導出する．このとき平均，分散，標準偏差はそれぞれ 2^{31}，2^{30}，2^{15} となる．これらの値による正規分布において $\Pr(\Delta z_{114} = 0)_{nd} \geq 0.500078$ となる確率は 2^{-80} より小さくなる．従ってバイアスの確率が 0.500078 より大きければバイアスとして妥当であると考えられる．提案手法により観測された偏りは $\Pr(\Delta z_{114} = 0) \approx 0.500119$ である．以上より実験値，理論値ともに妥当であるといえる．このようにして Grain v1 において，$\Pr(\Delta z_{114} = 0)$ の偏りを用いることでランダムな出力との識別が可能である．

5.4.3 識別攻撃の評価実験

識別攻撃の評価実験を行う．5.4.1 項に示した条件を満たす 2^{32} 個の IV を利用してキーストリームの差分のバイアスの観測を行う．114 段の鍵初期化処理の後に初めて出力され

るキーストリームの差分の偏りを観測する．128 通りの条件を満たす鍵に対して同様の実験を行った結果，$\Pr(\Delta z_{114} = 0)$ の最小値が 0.500127 となる．よって識別攻撃は実験的にも確認できる．

5.4.4 $\Delta z_{114} = 0$ の確率の理論的な評価

$\Delta z_{114} = 0$ の確率 $\Pr(\Delta z_{114} = 0)$ を計算する．z_{114} は以下のように生成される．

$$\begin{aligned} z_{114} = {} & b_1^{114} \oplus b_2^{114} \oplus b_4^{114} \oplus b_{10}^{114} \oplus b_{31}^{114} \oplus b_{43}^{114} \oplus b_{56}^{114} \oplus b_{63}^{114} \oplus s_{25}^{114} \\ & \oplus s_3^{114} s_{64}^{114} \oplus s_{46}^{114} s_{64}^{114} \oplus b_{63}^{114} s_{64}^{114} \\ & \oplus s_3^{114} s_{25}^{114} s_{46}^{114} \oplus s_3^{114} s_{46}^{114} s_{64}^{114} \oplus b_{63}^{114} s_3^{114} s_{46}^{114} \\ & \oplus b_{63}^{114} s_{25}^{114} s_{46}^{114} \oplus b_{63}^{114} s_{46}^{114} s_{64}^{114} \end{aligned}$$

114 段の条件付差分特性より，Δz_{114} は Δb_{10}^{114}，Δb_{31}^{114}，Δb_{43}^{114}，Δb_{56}^{114}，Δb_{63}^{114}，Δs_{46}^{114}，Δs_{64}^{114} から構成される．このとき，$\Delta b_{31}^{114} = 1$ であり，その他の差分は未知である．以上から Δz_{114} は

$$\begin{aligned} \Delta z_{114} = {} & \Delta b_{10}^{114} \oplus \Delta b_{31}^{114} \oplus \Delta b_{43}^{114} \oplus \Delta b_{56}^{114} \oplus \Delta b_{63}^{114} \\ & \oplus \Delta(s_3^{114} s_{64}^{114}) \oplus \Delta(s_{46}^{114} s_{64}^{114}) \oplus \Delta(b_{63}^{114} s_{64}^{114}) \\ & \oplus \Delta(s_3^{114} s_{25}^{114} s_{46}^{114}) \oplus \Delta(s_3^{114} s_{46}^{114} s_{64}^{114}) \\ & \oplus \Delta(b_{63}^{114} s_3^{114} s_{46}^{114}) \oplus \Delta(b_{63}^{114} s_{25}^{114} s_{46}^{114}) \oplus \Delta(b_{63}^{114} s_{46}^{114} s_{64}^{114}) \end{aligned}$$

から算出される．

値が未知の差分について解析を行い，その確率を算出する．解析の過程は以下の通りである．初めに，それぞれの差分について拡散の過程を遡ることによって未知差分の確率を解析する．具体的には，$\Delta b_{10}^{114} = \Delta b_{79}^{45}$，$\Delta b_{43}^{114} = \Delta b_{79}^{78}$，$\Delta b_{56}^{114} = \Delta b_{79}^{91}$，$\Delta b_{63}^{114} = \Delta b_{79}^{98}$，$\Delta s_{46}^{114} = \Delta s_{79}^{81}$，$\Delta s_{64}^{114} = \Delta s_{79}^{99}$ のように遡ることができる．それぞれのビットに関して，未知差分の原因となる箇所まで遡り，更新関数に基づいて解析を行う．更新関数は線形演算と非線形演算に分解できる．線形演算および非線形演算の差分をそれぞれ $\Delta(linear)$ および $\Delta(nonlinear)$ とおく．$\Delta(nonlinear)$ については，定理 2 より，内部状態の値ごとに差分を決定することができる．このとき内部状態の取りうる全てのパターンについて差分を計算し，$\Delta(nonlinear)$ の確率を導出する．確率 $\Pr(\Delta(nonlinear) = 0)$ は $\Delta(nonlinear) = 0$ となった回数と全体のパターン数から得られる．確率 $\Pr(\Delta(nonlinear) = 1)$ は $1 - Pr(\Delta(nonlinear) = 0)$ から得られる．$\Delta(linear)$ については，その原因となる入力から差分の確率を得る．以上から $\Delta(linear)$ および $\Delta(nonlinear)$ の確率を計算する．これは Δz の確率についても同様である．

条件付差分特性を解析した結果，Δz_{40}，Δz_{44}，Δz_{50} が Δz_{114} に強く影響していることが確認された．これらは全て未知の値である．はじめに Δz_{40}，Δz_{44}，Δz_{50} の値について確率を計算する．次にこれらの値について場合分けを行い，それぞれの場合について Δb_{10}^{114}，Δb_{43}^{114}，Δb_{56}^{114}，Δb_{63}^{114}，Δs_{46}^{114}，Δs_{64}^{114} の値の確率を計算する．最後に Δz_{114} の値について確率を計算する．結果として，$\Pr(\Delta z_{114} = 0) \approx 0.500119$ が得られる．したがって，提案する識別攻撃は理論的にも確認できる．

5.4.5 鍵回復攻撃

識別攻撃を用いた鍵回復攻撃について検討する．内部状態の更新値 s_{79}^4 は

$$\begin{aligned} s_{79}^4 = {} & s_3^0 \oplus s_6^0 \oplus s_{16}^0 \oplus s_{26}^0 \oplus s_{28}^0 \oplus s_{41}^0 \oplus s_{49}^0 \oplus s_{54}^0 \oplus 1 \\ & \oplus b_4^0 \oplus b_5^0 \oplus b_7^0 \oplus b_{13}^0 \oplus b_{34}^0 \oplus b_{46}^0 \oplus b_{59}^0 \\ & \oplus s_6^0 s_{28}^0 s_{49}^0 \oplus s_6^0 s_{49}^0 \oplus b_{66}^0 s_6^0 s_{49}^0 \oplus b_{66}^0 s_{28}^0 s_{49}^0 \oplus b_{66}^0 s_{49}^0 \end{aligned}$$

で与えられる．5.4.1 節に示した条件より，s_{79}^4 は

$$s_{79}^4 = s_{54}^0 \oplus b_{13}^0 \oplus 1$$

のように変形される．鍵および IV をそれぞれ k と x とおく．ランダムに選択した鍵から識別攻撃の成立が確認できた場合，秘密鍵が 5.4.1 項に示した条件を満たしていると考えられる．そのとき，以下の等式が得られる．

$$k_{13} = x_{54}$$

攻撃者は x_{54} を任意に選択可能である．したがって IV を任意に選択して distinguisher を観測することにより，上記の等式より，1 ビットの鍵の情報が復元できる．1 ビットの鍵回復に要する計算量は $2^{32} + 2^{32} = 2^{33}$ となる．残りの 40 ビットの weak key を全数探索することで，41 ビットの鍵回復が計算量 $2^{33} + 2^{40} \approx 2^{40.01}$ で成立する．

5.5 逆方向の解析における条件設定

Grain v1 に対する条件設定方法について述べる．逆方向の更新関数より差分の拡散に関する等式は

$$\begin{aligned} \Delta z_t = {} & \Delta b_0^{t+1} \oplus \Delta b_1^{t+1} \oplus \Delta b_3^{t+1} \oplus \Delta b_9^{t+1} \oplus \Delta b_{30}^{t+1} \oplus \Delta b_{42}^{t+1} \oplus \Delta b_{55}^{t+1} \oplus \Delta b_{62}^{t+1} \oplus \Delta s_{24}^{t+1} \\ & \oplus \Delta(s_2^{t+1} s_{63}^{t+1}) \oplus \Delta(s_{45}^{t+1} s_{63}^{t+1}) \oplus \Delta(b_{62}^{t+1} s_{63}^{t+1}) \\ & \oplus \Delta(s_2^{t+1} s_{24}^{t+1} s_{45}^{t+1}) \oplus \Delta(s_2^{t+1} s_{45}^{t+1} s_{63}^{t+1}) \\ & \oplus \Delta(b_{62}^{t+1} s_2^{t+1} s_{45}^{t+1}) \oplus \Delta(b_{62}^{t+1} s_{24}^{t+1} s_{45}^{t+1}) \oplus \Delta(b_{62}^{t+1} s_{45}^{t+1} s_{63}^{t+1}) \\ \Delta s_0^t = {} & \Delta s_{12}^{t+1} \oplus \Delta s_{22}^{t+1} \oplus \Delta s_{37}^{t+1} \oplus \Delta s_{50}^{t+1} \oplus \Delta s_{61}^{t+1} \oplus \Delta s_{79}^{t+1} \oplus \Delta z_t \\ \Delta b_0^t = {} & \Delta s_0^t \oplus \Delta b_8^{t+1} \oplus \Delta b_{13}^{t+1} \oplus \Delta b_{20}^{t+1} \oplus \Delta b_{27}^{t+1} \oplus \Delta b_{32}^{t+1} \oplus \Delta b_{36}^{t+1} \oplus \Delta b_{44}^{t+1} \oplus \Delta b_{51}^{t+1} \oplus \Delta b_{59}^{t+1} \\ & \oplus \Delta b_{61}^{t+1} \oplus \Delta b_{79}^{t+1} \\ & \oplus \Delta(b_8^{t+1} b_{14}^{t+1}) \oplus \Delta(b_{32}^{t+1} b_{36}^{t+1}) \oplus \Delta(b_{59}^{t+1} b_{62}^{t+1}) \\ & \oplus \Delta(b_{20}^{t+1} b_{27}^{t+1} b_{32}^{t+1}) \oplus \Delta(b_{44}^{t+1} b_{51}^{t+1} b_{59}^{t+1}) \\ & \oplus \Delta(b_8^{t+1} b_{27}^{t+1} b_{44}^{t+1} b_{62}^{t+1}) \oplus \Delta(b_{14}^{t+1} b_{20}^{t+1} b_{59}^{t+1} b_{62}^{t+1}) \oplus \Delta(b_{32}^{t+1} b_{36}^{t+1} b_{51}^{t+1} b_{59}^{t+1}) \\ & \oplus \Delta(b_8^{t+1} b_{14}^{t+1} b_{20}^{t+1} b_{27}^{t+1} b_{32}^{t+1}) \oplus \Delta(b_{36}^{t+1} b_{44}^{t+1} b_{51}^{t+1} b_{59}^{t+1} b_{62}^{t+1}) \\ & \oplus \Delta(b_{20}^{t+1} b_{27}^{t+1} b_{32}^{t+1} b_{36}^{t+1} b_{44}^{t+1} b_{51}^{t+1}) \oplus \Delta z_t \end{aligned}$$

となる．

5.5.1 差分による条件設定

$\Delta s_2 = 1$ のとき，差分の拡散式は

$$\Delta(s_2 s_{63}) \oplus \Delta(s_2 s_{24} s_{45}) \oplus \Delta(s_2 s_{45} s_{63}) \oplus \Delta(b_{62} s_2 s_{45})$$

となる．線形演算の差分 $\Delta(linear)$ が 0 のとき，内部状態に $b_{62} = 0$，$s_{24} = 0$，$s_{45} = 1$，$s_{63} = 1$ を条件として設定する．このとき非線形演算の差分は

$$\begin{aligned}&\Delta(s_2 s_{63}) \oplus \Delta(s_2 s_{24} s_{45}) \oplus \Delta(s_2 s_{45} s_{63}) \oplus \Delta(b_{62} s_2 s_{45})\\ &= 1 \oplus 0 \oplus 1 \oplus 0 = 0\end{aligned}$$

となる．$\Delta(linear) = 1$ のとき，内部状態に $b_{62} = 1$，$s_{24} = 0$，$s_{45} = 1$，$s_{63} = 1$ を条件として設定する．このとき非線形演算の差分は

$$\begin{aligned}&\Delta(s_2 s_{63}) \oplus \Delta(s_2 s_{24} s_{45}) \oplus \Delta(s_2 s_{45} s_{63}) \oplus \Delta(b_{62} s_2 s_{45})\\ &= 1 \oplus 0 \oplus 1 \oplus 1 = 1\end{aligned}$$

となる．以上より $\Delta s_0 = 0$ となる．

$\Delta s_{24} = 1$ のとき差分の拡散式は

$$\Delta(s_2 s_{24} s_{45}) \oplus \Delta(b_{62} s_{24} s_{45})$$

となる．このとき内部状態に $b_{62} = 0$，$s_2 = 0$，$s_{45} = 1$ を条件として設定する．非線形演算の差分は

$$\Delta(s_2 s_{24} s_{45}) \oplus \Delta(b_{62} s_{24} s_{45}) = 0 \oplus 0 = 0.$$

となる．以上より Δs_0 の値は $\Delta(linear)$ に依存する．

$\Delta s_{45} = 1$ のとき差分の拡散式は

$$\begin{aligned}&\Delta(s_{45} s_{63}) \oplus \Delta(s_2 s_{24} s_{45}) \oplus \Delta(s_2 s_{45} s_{63}) \oplus \Delta(b_{62} s_2 s_{45})\\ &\oplus \Delta(b_{62} s_{24} s_{45}) \oplus \Delta(b_{62} s_{45} s_{63})\end{aligned}$$

となる．このとき内部状態に $b_{62} = 0$, $s_2 = 0$, $s_{24} = 0$, and $s_{63} = 1$ を条件として設定する．非線形演算の差分は

$$\begin{aligned}&\Delta(s_{45} s_{63}) \oplus \Delta(s_2 s_{24} s_{45}) \oplus \Delta(s_2 s_{45} s_{63}) \oplus \Delta(b_{62} s_2 s_{45})\\ &\oplus \Delta(b_{62} s_{24} s_{45}) \oplus \Delta(b_{62} s_{45} s_{63})\\ &= 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 = 1\end{aligned}$$

となる．以上より Δs_0 の値は $\Delta(linear)$ に依存する．

5.5.2 内部状態ビットによる条件設定

逆方向の解析において内部状態に設定された条件がシフトレジスタの端に来た場合，その条件が更新に利用されることで値が見えなくなる．この値は順方向の更新値であるので，その条件を満たすように更新関数から値を設定する必要がある．非線形演算における条件は以下のように与えられる．a，b，c を内部状態のビットとする．abc が上記の値の非線形演算を表す．

- a が free bit ならば，$a = 0$ とする．
- $a = 1$ かつ b が free bit ならば，$b = 0$ とする．
- $a = b = 1$ かつ c が free bit ならば，$c = 0$ とする．

他の次数の非線形演算についても同様に設定する．$s_2 s_{63}$ は以下のように条件を設定する．

- s_2 が free bit ならば，$s_2 = 0$ とする．
- $s_2 = 1$ かつ s_{63} が free bit ならば， $s_{63} = 1$ とする．

これは Grain v1 において条件が $s^0_{64} = s^0_{65} = \cdots = s^0_{79} = 1$ を満たす必要があるからである．

5.6 結言

本章では，新しい条件付差分解読法を提案した．提案手法は従来の related-key setting における手法に着目し，改良を行った．鍵初期化の順方向と逆方向の処理の両方における差分の拡散から，条件付差分特性を取得する．逆方向においては，初期状態への差分の拡散を抑制するように条件を解析し，中間状態と初期状態の間の条件付差分特性を探索した．順方向においては，差分の拡散を観測し，中間状態とキーストリームの間の差分特性を探索した．これらを結合し，初期状態とキーストリームの間の条件付差分特性を得た．提案手法を Grain v1 に適用し，識別攻撃および鍵回復攻撃を提案した．結果として weak-key setting において識別攻撃が理論的かつ実験的に確認できた．さらに weak-key の領域に含まれる鍵について，識別攻撃を用いて 1 ビットの鍵回復攻撃を実行した．

NLFSR 型のストリーム暗号はアルゴリズムの巻き戻しが可能であるため，提案手法が様々な NLFSR 型のストリーム暗号に適用されることが期待できる．

第6章　結論

本論文では代表的なストリーム暗号の 1 つである RC4 および NLFSR 型のストリーム暗号に着目し，その安全性を解読法の議論によって評価した．さらに RC4 を利用したシステムの 1 つである WEP について，その安全性向上手法を提案した．本研究は 3 つのテーマから成る．それらは，SSL/TLS における RC4 の新しい平文回復攻撃 (第 3 章)，安全かつ高速な WEP の運用方法 (第 4 章)，NLFSR 型ストリーム暗号に対する条件付差分解読法 (第 5 章) である．

第 3 章では，SSL/TLS における RC4 に対する効率的な平文回復攻撃を提案した．Vanhoef らの攻撃に着目し，single-byte bias と double-byte bias を同時に利用する手法を構築した．復元対象の平文を $\{P_{89}, P_{90}, \ldots, P_{96}\}$, $\{P_{113}, P_{114}, \ldots, P_{120}\}$, $\{P_{161}, P_{162}, \ldots, P_{168}\}$, $\{P_{201}, P_{202}, \ldots, P_{208}\}$ として，提案手法の有効性を確認する実験を行った．提案手法を対象の平文全ての復元に成功する確率で評価した．結果として，平文バイトがランダムに分布しているという仮定において，2^{29} の暗号文から $\{P_{113}, P_{114}, \ldots, P_{120}\}$ 全体を約 0.961 の確率で復元することができた．これは従来の最も効率の良い攻撃である *ABPPS attack* より高い確率である．したがって，提案手法が従来より有効な攻撃であることが確認できた．

RC4 のようにキーストリームの乱数性が不十分であるストリーム暗号の解析に提案手法が適用されることを期待する．

第 4 章では，安全な WEP の運用方法を提案した．Klein 攻撃，Korek 攻撃，SVV_10 bias の条件が成立しない IV の集合を示し，改良 Strong IV として定義した．WEP における改良 Strong IV の効率的な生成方法を提案した．提案手法により 100,000 パケットの通信を安全に行うことができる．計算機実験により，提案手法を用いた場合における WEP の暗号化に必要な時間の評価を行った．結果として，WEP と比べて 1.1 から 1.2 倍の時間が必要であることが確認できた．したがって，提案手法は WEP と同等の速度かつ安全な通信を実現できるといえる．提案手法は IV の判定プロセスおよび鍵の更新プロセスをファームウェアの更新によって従来の機器に導入可能である．

統計的性質に基づく鍵回復攻撃より，今後提案される攻撃も Klein 攻撃の条件を利用すると考えられる．提案手法は，そのような攻撃も防ぐことが可能であると考えられる．

第 5 章では，NLFSR 型ストリーム暗号に対する新しい条件付差分解読法を提案した．提案手法は従来の related-key setting における手法に着目し，related-key の仮定なしに条件付差分特性を取得する方法を提案した．鍵初期化の順方向と逆方向の処理の両方における差分の拡散から，条件付差分特性を取得する．1 ビットの差分が入力された中間状態を仮定し，中間状態と初期状態の間の条件付差分特性を逆方向の鍵初期化により解析した．同様に中間状態とキーストリームの間の差分特性を順方向の鍵初期化により解析した．これらを結合し，初期状態とキーストリームの間の条件付差分特性を得た．提案手法を Grain v1 に適用し，識別攻撃および鍵回復攻撃について議論を行った．結果として weak-key setting

において 114 段の Grain v1 に対する識別攻撃が理論的かつ実験的に確認できた．さらに weak-key の領域に含まれる鍵について，識別攻撃を用いた 41 ビットの鍵回復攻撃が確認できた．

NLFSR 型のストリーム暗号は鍵初期化部の巻き戻しが可能であるため，提案手法が様々な NLFSR 型のストリーム暗号に適用されることが期待できるといえる．

謝辞

本研究の機会を与えて頂いた神戸大学大学院工学研究科電気電子工学専攻 森井昌克教授には，熱心な御指導と貴重な御助言を賜りました．ここに謹んで感謝の意を表します．

本研究をまとめるにあたり，貴重な御教示と多くの御助言を頂きました神戸大学大学院工学研究科電気電子工学専攻 竹野裕正教授に深く感謝致します．

本研究を論文としてまとめるにあたって貴重な御教示と御助言を頂きました神戸大学大学院科学技術イノベーション研究科 太田能教授に深く感謝致します．

本研究の遂行および論文執筆にあたり，数々の有益なる御助言を賜り，御討論頂きました神戸大学大学院工学研究科電気電子工学専攻 白石善明准教授に深く感謝致します．

RC4 に対する平文回復攻撃の研究を遂行するにあたり，数々の有益なる御助言，御討論をいただきました東海大学情報通信学部通信ネットワーク工学科 大東俊博講師および神戸大学大学院工学研究科電気電子工学専攻情報通信研究室 五十部孝典研究員にこころより感謝致します．

NLFSR 型ストリーム暗号の解析に関する研究を推進するにあたって，多くの御助言と御討論をいただきました，NTT セキュアプラットフォーム研究所の藤堂洋介氏に深謝いたします．

さらに，筆者は神戸大学大学院工学研究科電気電子工学専攻 高野泰洋助教に日頃より御助言，御討論いただきました．ここに深謝の意を表します．

また岡山大学大学院の栗林稔准教授には，神戸大学大学院在籍時に多くの御助言と御討論をいただきました．ここに感謝の意を表します．

本研究を推進するにあたって日頃からの温かい励ましと貴重な御助言をいただきました神戸大学大学院工学研究科電気電子工学専攻情報通信研究室の諸氏に心より感謝いたします．

最後に，大学生活を支えて頂き，博士後期課程への進学にも理解を示してくれた両親と家族に心より感謝致します．

参考文献

[1] Alan O. Freier, Philip Karlton, and Paul C. Kocher. The SSL Protocol Version 3.0, November 1996. http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt.

[2] T. Dierks and C. Allen. The TLS Protocol Version 1.0, 1999. http://www.ietf.org/rfc/rfc2246.txt.

[3] IEEE Computer Society. Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications. IEEE Std 802.11, 1999.

[4] Nadhem J. AlFardan, Daniel J. Bernstein, Kenneth G. Paterson, Bertram Poettering, and Jacob C. N. Schuldt. On the Security of RC4 in TLS. In Samuel T. King, editor, *Proceedings of the 22th USENIX Security Symposium*, pages 305–320. USENIX Association, 2013.

[5] Takanori Isobe, Toshihiro Ohigashi, Yuhei Watanabe, and Masakatu Morii. Full Plaintext Recovery Attack on Broadcast RC4. In Shiho Moriai, editor, *FSE*, volume 8424 of *Lecture Notes in Computer Science*, pages 179–202. Springer, 2013.

[6] Trustworthy Internet Movement. SSL Pulse. https://www.trustworthyinternet.org/ssl-pulse/, accessed Jul. 8. 2016.

[7] Itsik Mantin and Adi Shamir. A Practical Attack on Broadcast RC4. In Mitsuru Matsui, editor, *FSE*, volume 2355 of *Lecture Notes in Computer Science*, pages 152–164. Springer, 2001.

[8] Sourav Sen Gupta, Subhamoy Maitra, Goutam Paul, and Santanu Sarkar. (Non-)Random Sequences from (Non-)Random Permutations - Analysis of RC4 Stream Cipher. *Journal of Cryptology*, 27(1):67–108, 2014.

[9] Pouyan Sepehrdad, Serge Vaudenay, and Martin Vuagnoux. Discovery and Exploitation of New Biases in RC4. In Alex Biryukov, Guang Gong, and Douglas R. Stinson, editors, *Selected Areas in Cryptography*, volume 6544 of *Lecture Notes in Computer Science*, pages 74–91. Springer, 2010.

[10] Ilya Mironov. (Not So) Random Shuffles of RC4. In Moti Yung, editor, *CRYPTO*, volume 2442 of *Lecture Notes in Computer Science*, pages 304–319. Springer, 2002.

[11] Daniel J. Bernstein. Failures of secret-key cryptography, 2013. FSE 2013, Invited Talk.

[12] Scott R. Fluhrer and David A. McGrew. Statistical Analysis of the Alleged RC4 Keystream Generator. In Bruce Schneier, editor, *FSE*, volume 1978 of *Lecture Notes in Computer Science*, pages 19–30. Springer, 2000.

[13] Itsik Mantin. Predicting and Distinguishing Attacks on RC4 Keystream Generator. In Ronald Cramer, editor, *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 491–506. Springer, 2005.

[14] Scott R. Fluhrer, Itsik Mantin, and Adi Shamir. Weaknesses in the Key Scheduling Algorithm of RC4. In Serge Vaudenay and Amr M. Youssef, editors, *Selected Areas in Cryptography*, volume 2259 of *Lecture Notes in Computer Science*, pages 1–24. Springer, 2001.

[15] Rafik Chaabouni. Break WEP Faster with Statistical Analysis. Technical report, EPFL, LASEC, June 2006.

[16] Andreas Klein. Attacks on the RC4 stream cipher. *Des. Codes Cryptography*, 48(3):269–286, 2008.

[17] Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin. Breaking 104 Bit WEP in Less Than 60 Seconds. In Sehun Kim, Moti Yung, and Hyung-Woo Lee, editors, *WISA*, volume 4867 of *Lecture Notes in Computer Science*, pages 188–202. Springer, 2007.

[18] Ryoichi Teramura, Yasuo Asakura, Toshihiro Ohigashi, Hidenori Kuwakado, and Masakatu Morii. Fast WEP-Key Recovery Attack Using Only Encrypted IP Packets. *IEICE Transactions*, 93-A(1):164–171, 2010.

[19] Pouyan Sepehrdad, Petr Susil, Serge Vaudenay, and Martin Vuagnoux. Smashing WEP in a Passive Attack. In Shiho Moriai, editor, *FSE*, volume 8424 of *Lecture Notes in Computer Science*, pages 155–178. Springer, 2013.

[20] IEEE Computer Society. 802.1X-Port Based Network Access Control. IEEE Std 802.11, 2001.

[21] Orinoco. Wepplus white paper. Oct. 2001.

[22] Tsubasa Tsukaune, Yosuke Todo, and Masakatu Morii. A Proposal of a WEP Operation Secure Against the Key-Recovery Attack. *IEICE Technical Report*, 111(209):11–16, 2011.

[23] Martin Hell, Thomas Johansson, and Willi Meier. Grain - A Stream Cipher for Constrained Environments, 2005. ECRYPT Stream Cipher Project Report 2005/010, 2005. Available at `http://www.ecrypt.eu.org/stream`.

[24] Christophe De Cannière. Trivium: A Stream Cipher Construction Inspired by Block Cipher Design Principles. In Sokratis K. Katsikas, Javier Lopez, Michael Backes, Stefanos Gritzalis, and Bart Preneel, editors, *ISC*, volume 4176 of *Lecture Notes in Computer Science*, pages 171–186. Springer, 2006.

[25] Simon Knellwolf, Willi Meier, and María Naya-Plasencia. Conditional Differential Cryptanalysis of NLFSR-Based Cryptosystems. In Masayuki Abe, editor, *ASIACRYPT*, volume 6477 of *Lecture Notes in Computer Science*, pages 130–145. Springer, 2010.

[26] Toshihiro Ohigashi, Takanori Isobe, Yuhei Watanabe, and Masakatu Morii. How to Recover Any Byte of Plaintext on RC4. In Tanja Lange, Kristin E. Lauter, and Petr Lisonek, editors, *Selected Areas in Cryptography*, volume 8282 of *Lecture Notes in Computer Science*, pages 155–173. Springer, 2013.

[27] Mathy Vanhoef and Frank Piessens. All your biases belong to us: Breaking RC4 in WPA-TKIP and TLS. In *Proceedings of the 24th USENIX Security Symposium, eds. J. Jung and T. Holz*, pages 97–112, 2015.

[28] Christina Garman, Kenneth G. Paterson, and Thyla Van der Merwe. Attacks Only Get Better: Password Recovery Attacks Against RC4 in TLS. In *Proceedings of the 24th USENIX Security Symposium, eds. J. Jung and T. Holz*, pages 113–128, 2015.

[29] Takanori Isobe, Toshihiro Ohigashi, Yuhei Watanabe, and Masakatu Morii. Comprehensive Analysis of Initial Keystream Biases of RC4. *IEICE Transactions Fundamentals*, E97-A(1):139–151, 2014.

[30] Toshihiro Ohigashi, Takanori Isobe, Yuhei Watanabe, and Masakatu Morii. Full Plaintext Recovery Attacks on RC4 Using Multiple Biases. *IEICE Transactions Fundamentals*, E98-A(1):81–91, 2015.

[31] A. Roos. A class of weak keys in the RC4 stream cipher, 1995. Two posts in sci.crypt.

[32] Ryoichi Teramura, Toshihiro Ohigashi, Hidenori Kuwakado, and Masakatu Morii. Generalized Classes of Weak Keys on RC4 Using Predictive State. *IEICE Transactions Fundamentals*, 94-A(1):10–18, 2011.

[33] Atsushi Nagao, Toshihiro Ohigashi, Takanori Isobe, and Masakatu Morii. Expanding Weak-key Space of RC4. *JIP*, 22(2):357–365, 2014.

[34] Serge Vaudenay and Martin Vuagnoux. Passive-Only Key Recovery Attacks on RC4. In Carlisle M. Adams, Ali Miri, and Michael J. Wiener, editors, *Selected Areas in Cryptography*, volume 4876 of *Lecture Notes in Computer Science*, pages 344–359. Springer, 2007.

[35] Bruce Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C, 1995. John Wiley & Inc (Computers).

[36] Korek. Next generation of WEP attacks?, 2004. `http://www.netstumbler.org/showpost.php?p=93942&postcount=35`.

[37] Toshihiro Ohigashi, Hidenori Kuwakado, and Masakatu Morii. A Key Recovery Attacks on WEP with Less Packets. *IEICE Technical Report*, 107(346):61–68, 2007.

[38] Subhamoy Maitra and Goutam Paul. New Form of Permutation Bias and Secret Key Leakage in Keystream Bytes of RC4. In Kaisa Nyberg, editor, *FSE*, volume 5086 of *Lecture Notes in Computer Science*, pages 253–269. Springer, 2008.

[39] Masanori Yoshida, Kazukuni Kobara, and Hideki Imai. WEP Implementation Secure Against The Key Recovery Attacks Based On Weak IV, 2006. Proceeding of The Symposium on Cryptography and Information Security (SCIS).

[40] The ECRYPT Stream Cipher Project. eSTREAM Portfolio of Stream Ciphers, 2008. Revised on September 8, 2008.

[41] Yuseop Lee, Kitae Jeong, Jaechul Sung, and Seokhie Hong. Related-Key Chosen IV Attacks on Grain-v1 and Grain-128. In Yi Mu, Willy Susilo, and Jennifer Seberry, editors, *ACISP*, volume 5107 of *Lecture Notes in Computer Science*, pages 321–335. Springer, 2008.

[42] Christophe De Cannière, Özgül Küçük, and Bart Preneel. Analysis of Grain's Initialization Algorithm. In Serge Vaudenay, editor, *AFRICACRYPT*, volume 5023 of *Lecture Notes in Computer Science*, pages 276–289. Springer, 2008.

[43] Simon Knellwolf. *Cryptanalysis of hardware-oriented ciphers the Knapsack generator, and SHA-1*. PhD thesis, Zürich, 2012.

[44] Subhadeep Banik. A Dynamic Cube Attack on 105 round Grain v1, 2014. IACR Cryptology ePrint Archive 2014: 652. Available at `http://eprint.iacr.org/2014/652`.

[45] Santanu Sarkar. A New Distinguisher on Grain v1 for 106 Rounds. In Sushil Jajodia and Chandan Mazumdar, editors, *ICISS*, volume 9478 of *Lecture Notes in Computer Science*, pages 334–344. Springer, 2015.

[46] Subhadeep Banik. Some Insights into Differential Cryptanalysis of Grain v1. In Willy Susilo and Yi Mu, editors, *ACISP*, volume 8544 of *Lecture Notes in Computer Science*, pages 34–49. Springer, 2014.

発表論文

学術論文

1. 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, vol.E100-A, no.3, Mar, 2017. (掲載予定)

2. Yuhei Watanabe, Takahiro Iriyama, and Masakatu Morii, “Proposal of WEP Operation with Strong IV and Its Implementation,” Journal of Information Processing, 2017. (掲載予定)

3. Toshihiro Ohigashi, Takanori Isobe, Yuhei Watanabe, and Masakatu Morii, “Full Plaintext Recovery Attacks on RC4 using Multiple Biases,” IEICE Trans. Fundamentals, vol.E98-A, no.1, pp.81-91, 2015.

4. Takanori Isobe, Toshihiro Ohigashi, Yuhei Watanabe, and Masakatu Morii, “Comprehensive Analysis of Initial Keystream Biases of RC4,” IEICE Trans. Fundamentals, vol.E97-A, no.1, pp.139-151, 2014.

5. 遠藤祐介, 廣友雅徳, 佐治勇樹, 渡辺優平, 森井昌克, “多値二次元コードにおける高階調度認識アルゴリズムの提案,” 電子情報通信学会論文誌 D, vol.J95-D, no.11, pp.1935-1943, 2012.

国際会議

1. Yuhei Watanabe, Yosuke Todo, and Masakatu Morii, “New Conditional Differential Cryptanalysis for NLFSR-Based Stream Ciphers and Application to Grain v1,” 11th Asia Joint Conference on Information Security (AsiaJCIS2016), 2016.

2. Toshihiro Ohigashi, Takanori Isobe, Yuhei Watanabe, and Masakatu Morii, “How to Recover Any Byte of Plaintext on RC4,” The Selected Areas in Cryptography 2013 (SAC2013), Lecture Notes in Computer Science, Vol. 8282, pp.155-173, 2013.

3. Takanori Isobe, Toshihiro Ohigashi, Yuhei Watanabe, and Masakatu Morii, “Full Plaintext Recovery Attack on Broadcast RC4,” 20th Int. Workshop on Fast Software Encryption (FSE2013), Lecture Notes in Computer Science, Vol. 8424, pp.179-202, 2013.

学術講演

1. 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, CDROM, 3D2-4, 8 pages, 2016.
2. 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, CDROM, 3D2-5, 7 pages, 2016.
3. 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) 講演論文集第 4 分冊, pp.195-200, 2015.
4. 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) 講演論文集第 4 分冊, pp.269-272, 2015.
5. 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,” 電子情報通信学会技術研究報告 (情報通信システムセキュリティ), Vol. 115, No. 81, pp.27-32, 2015 年 6 月.
6. 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 2014 論文集, CDROM, 2E1-2, 8 pages, 2014.
7. 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,” 電子情報通信学会技術研究報告 (情報通信システムセキュリティ), Vol. 113, No. 502, pp.7-12, 2014 年 3 月.
8. 渡辺優平, 大東俊博, 森井昌克, “SSL/TLS での RC4 に対する平文回復攻撃の改良,” 2014 年暗号と情報セキュリティシンポジウム, CDROM, 2F2-2, 7 pages, 2014.
9. 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,” 2014 年暗号と情報セキュリティシンポジウム, CDROM, 2F2-1, 7 pages, 2014.
10. 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 2013 論文集, pp.330-335, 2013.
11. Yuhei Watanabe, Takanori Isobe, Toshihiro Ohigashi, and Masakatu Morii, “Vulnerability of RC4 in SSL/TLS,” 電子情報通信学会技術研究報告 (情報通信システムセキュリティ), Vol. 113, No. 95, pp.19-24, 2013 年 6 月.
12. Toshihiro Ohigashi, Takanori Isobe, Yuhei Watanabe, and Masakatu Morii, “How to Recover Full Plaintext from Only Ciphertexts on Broadcast RC4,” Symposium on Cryptography and Information Security 2013 (SCIS2013), CDROM, 3B4-3, 8 pages, 2013.
13. Yuhei Watanabe, Takanori Isobe, Toshihiro Ohigashi, and Masakatu Morii, “New Biases of RC4 and its Application to Disitingushing, Key Recovery, Plaintext Recovery Attacks,” Symposium on Cryptography and Information Security 2013 (SCIS2013), CDROM, 3B4-2, 8 pages, 2013.

14. 青山直樹, 渡辺優平, 森井昌克, “埋め草コードを利用した QR コードの高誤り訂正,” 第 12 回情報科学技術フォーラム (FIT2013) 講演論文集第 4 分冊, pp.509-514, 2013.

15. 古本啓祐, 渡辺優平, 森井 昌克, “グレースケール多重化二次元コードとその応用,” 電子情報通信学会技術研究報告 (情報通信システムセキュリティ), Vol. 112, No. 315, pp.7-12, 2012 年 11 月.

16. 柏井祐樹, 渡辺優平, 森井昌克, “オフラインサイト認証可能な QR コード,” 第 11 回情報科学技術フォーラム (FIT2012) 講演論文集第 4 分冊, pp.107-112, 2012.

17. 古本啓祐, 渡辺優平, 森井 昌克, “動画像 QR コードとその応用,” 第 11 回情報科学技術フォーラム (FIT2012) 講演論文集第 4 分冊, pp.407-412, 2012.

18. 渡辺優平, 柏井祐樹, 森井昌克, “不正 QR コードの対策とそれを実現するシステムの開発,” 電子情報通信学会技術研究報告 (情報通信システムセキュリティ), Vol. 111, No. 495, pp.1-4, 2012 年 3 月.

19. 渡辺優平, 遠藤祐介, 森井昌克, “埋め草コード語を利用した QR コードの誤り訂正能力向上について,” 第 10 回情報科学技術フォーラム (FIT2011) 講演論文集第 4 分冊, pp.511-516, 2011.

神戸大学博士論文
「ストリーム暗号および無線 LAN 暗号技術の安全性に関する研究」全 70 頁
提出日　2017 年 1 月 17 日
本博士論文が神戸大学機関リポジトリ Kernel にて掲載される場合，掲載登録日（公開日）はリポジトリの該当ページ上に掲載されます.