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

(別紙様式 3)

論文内容の要旨

氏　名　渡辺 優平

専　攻　電気電子工学専攻

論文題目（外国語の場合は，その和訳を併記すること。）

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

指導教員　森井 昌克

（注）2，000字～4，000字でまとめること。

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．

（氏名：渡辺 優平　　NO. 2 ）

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．

（別紙1）　　論文審査の結果の要旨

氏名	渡辺　優平		
論文題目	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		
審査委員	区　分	職　名	氏　　名
	主　査	教授	森井　昌克
	副　査	教授	竹野　裕正
	副　査	教授	太田　能
	副　査	准教授	白石　善明　印
	副　査		印

要　　旨

概要

本論文では情報セキュリティの基盤を担う技術である共通鍵暗号の1つであるストリーム暗号の解析および安全性評価を行い，さらにそれを利用したシステムである無線 LAN の暗号技術の安全性向上手法を提案している．

第一章は序論である．

第二章は準備としてストリーム暗号の構造とその安全性評価について説明している．

第三章ではSSL/TLSにおけるRC4に対する安全性評価を行っている．
RC4は商用アプリケーションや暗号化通信プロトコルなどで広く利用されているストリーム暗号である．過去20年間の解析結果により利用が減少しているが，未だに利用が確認されている．RC4のキーストリームには1バイト単位の偏りと2バイト単位の偏りが存在し，Broadcast setting(同じ平文をユーザごとの鍵で暗号化する)において偏りを利用した攻撃が多数提案されている．本論文ではBroadcast settingにおいてRC4のキーストリームに存在する1バイト単位の偏りと2バイト単位の偏りを併用する手法を提案している．異なる種類の偏りを効率的に組み合わせることで平文回復攻撃の効率化を達成している．SSL/TLSを想定した条件下において平文解読実験を行い，2^29の暗号文を集めることにより8バイトの平文ブロックを効率的に復元することが可能であることを示している．

第四章では無線LAN暗号化方式WEPの安全性向上手法の提案を行っている．
WEP は多くの脆弱性が指摘されており，より安全な方式への移行が推奨されているが，機器の交換コストの問題など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 を用いたものと IV とキーストリームの間の統計的性質に基づいたものに分類される．したがって，それぞれの脆弱性が成立する IV を取り除くことで，安全に WEP を運用することができると考えられる．本論文ではファームウェアの更新のみで導入可能な WEP の安全な利用方法を提案している．脆弱な IV に対するフィルタリングパターンについて解析を行い，効率的なパターンを提案している．脆弱性が成立しない IV を改良 Strong IV と呼び，その IV を利用した WEP の運用方法について検討を行い，その通信において暗号化にかかる時間の評価を行っている．結果として，IV の判定を導入することで WEP を安全かつ高速に利用することができることを示している．

第五章では非線形帰還シフトレジスタ(NLFSR)で構成されたストリーム暗号に対する安全性評価を行っている．
ストリーム暗号ではキーストリームの乱数性を得るために，秘密鍵と IV に対して鍵初期化処理を行い，それぞれの情報を撹拌する．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．この性質を利用した条件付差分解読法が Knellwolf によって提案されているが，複数の関連する鍵を利用する仮定においてのみ有効である．本論文では，攻撃がより困難な仮定において，鍵初期化処理の巻き戻しを利用した条件付差分解読法を提案している．提案手法によって，weak-key setting(ある条件を満たす鍵を利用)における条件付差分特性を得ることができる．提案手法を NLFSR 型ストリーム暗号 Grain v1 に適用した結果，114 段の Grain v1 に対して識別攻撃および鍵回復攻撃が成立することを示している．これは従来より多くの段数で成立する攻撃である．

氏名	渡辺　優平

本論文では情報セキュリティの基盤技術である共通鍵暗号に対する新しい安全性評価手法とともに，暗号技術を用いたシステムの安全性向上手法の提案を行っている．本論文では，ストリーム暗号に対する現実的な利用環境を想定した解析とアルゴリズムに基づいた解析の結果が示されており，かつ既存の結果を上回る結果となっている．また，ストリーム暗号を用いたシステムである WEP の改良を行っている．以上のようにストリーム暗号に対する理論的な解析のみでなく，実際に運用する際の安全性についても重要な知見を得たものとして価値ある集積であると認める．提出された論文は工学研究科学位論文評価基準を満たしており，学位申請者の渡辺優平は博士（工学）の学位を得る資格があると認める．