共通鍵暗号のしくみと安全性評価

松井　充

共通鍵暗号は，送信者と受信者がもつ共通の秘密情報をもとに秘匿や認証の機能を実現する，いわば古典暗号の現代ディジタル版ともいえるものであるが，高速・小型であるなど，その高い実用性のゆえに，現在の暗号通信のほとんどすべての場面で用いられている．ここでは，代表的な共通鍵暗号について，そのしくみと性能，ならびに安全性評価の考え方と主な解読手法について概説する．

キーワード：ブロック暗号，ストリーム暗号，暗号解読，暗号評価

1．はじめに

現代共通鍵暗号は，数十ビットから数百ビットの情報（これを共通鍵という）を送信者と受信者があらかじめ共有しておき，この情報が第三者には知られないとの前提で，二者間の安全な秘匿・認証機能を実現しようとするものである．共通鍵暗号は公開鍵暗号にくらべて小型・高速に実現でき，きわめて幅広い範囲で利用されている．

共通鍵暗号は，ストリーム暗号とブロック暗号に大別される．ストリーム暗号は，本質的には擬似乱数生成メカニズムであり，この擬似乱数と平文を加算（一般的には排他的論理和）して暗号文を生成する．これに対し，ブロック暗号は平文そのものを攪拌して暗号文を生成する．現在では両方式とも数多くの標準や商用製品に採用されている．

本稿では，これら共通鍵暗号のしくみやその性能について述べるとともに，共通鍵暗号の安全性評価の考え方について説明する．暗号の安全性とは，暗号の解読のされにくさであるため，安全性評価の研究とは解読手法の研究にほかならない．ここでは共通鍵暗号の代表的な解読手法をいくつかとりあげ，その原理と有効性について解説を行う．

2．ストリーム暗号とブロック暗号

2.1　ストリーム暗号の原理と歴史

1910年代にVernamによって発明されたOne-Time Padと呼ばれるストリーム暗号は，平文と同じ長さの使い捨ての乱数を送受信者が共有しておき，この乱数と平文を排他的論理和して暗号文とするものである．One-Time Padは情報理論的に安全，すなわち解読者が無限の計算能力をもっていると仮定しても暗号文から平文のいかなる情報も得ることができないことがShannonによって1949年に証明されている[1]．

One-Time Padはいわば理想の暗号であるが，一方で平文と同じ長さの秘密情報を送信者と受信者が常に共有しているという前提は，現代の暗号通信では多くの場合非現実的である．そこで実際のストリーム暗号では，固定長の共通鍵から，十分長い良質な擬似乱数列を生成するものをもちい，この乱数と平文と排他的論理和して暗号文を生成する構成をとる．

ストリーム暗号では，その内部でLFSR（線形帰還シフトレジスタ）が用いられることが多い．LFSRは周期が簡単に計算できるとともに，出力データの出現頻度がほぼ均一であるという特性をもっているためである．実際には，図1に示すように，複数のLFSRと非線形関数を組み合わせて構成するのが典型的な例である．

ストリーム暗号は伝送路のノイズを復号時に拡大しないという特長をもっているため，無線音声秘話などノイズに敏感な秘匿通信に適している．例えば携帯電

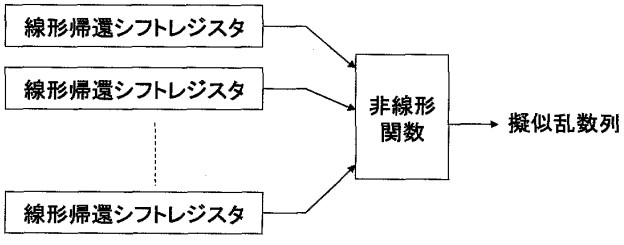

図1　LFSRを用いたストリーム暗号の一例

まつい　みつる
三菱電機㈱ 情報技術総合研究所
〒247-8501 鎌倉市大船5-1-1

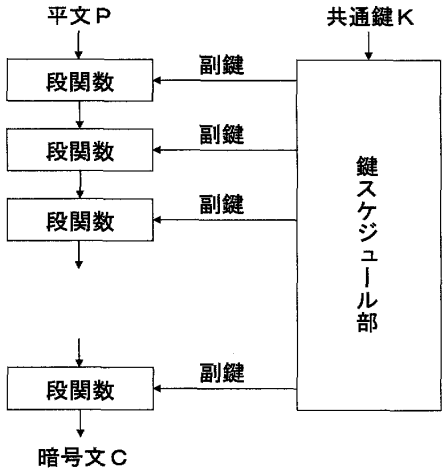

図2　ブロック暗号の基本構造

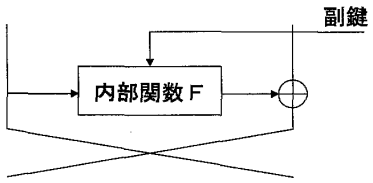

図3　Feistel 型ブロック暗号の段関数

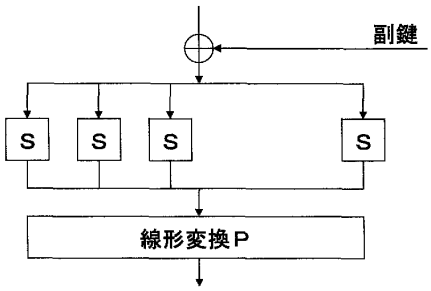

図4　SPN 型ブロック暗号の段関数

話における暗号化は通常ストリーム暗号を用いて行われる．また無線 LAN の暗号化で用いられるストリーム RC 4[2]は，インターネットにおける標準的な暗号通信規格である SSL プロトコルでも利用されている．

2.2　ブロック暗号の原理と歴史

ブロック暗号は，データをブロックと呼ばれる単位に分割し，ブロックごとにデータを非線形変換する方式である．通常ブロックサイズは 64 ビットまたは 128 ビットが用いられる．その内部構造は，図 2 に示すように，段関数（ラウンド関数）と呼ばれる小さな関数を直列に積み重ねるとともに，この各関数には，鍵スケジュール部によって変換された共通鍵が入力されるという形式がもっとも広く採用されている．

ブロック暗号の歴史は 1970 年代なかばに制定された米国政府標準暗号 DES[3]にはじまる．DES は 56 ビットの鍵をもつ 64 ビットブロック暗号であり，20 年以上にわたり事実上の世界標準として幅広く用いられてきた．しかしながら計算機の性能向上と暗号解読法の進歩によって，90 年代後半に完全解読されるにいたり，その役割を終えた．

米国における DES の後継暗号としては，早くから TripleDES と呼ばれる DES を直列に三重に重ねた方式が用いられてきたが，2001 年に新たな政府標準暗号 AES[4]が制定されたのちは，AES への暗号の世代交代が徐々に進んでいる．AES は鍵長が 128 ビット，192 ビット，256 ビットの 3 種類をサポートし，ブロックサイズは 128 ビットである．

一方日本では，NTT が 1980 年代に開発したブロック暗号 FEAL[5]が通信分野で広く用いられてきた．その後三菱電機が開発したブロック暗号 MISTY[6]をもとに欧州で設計された KASUMI[7]が，第三世代携帯電話の国際標準である W-CDMA 方式の標準暗号に採用され，現在世界中で利用されている．また NTT と三菱電機が共同開発した Camellia[8]がインターネット標準暗号に認められるなど，日本発のブロック暗号も世界標準の地位を確立している．

ブロック暗号の段関数の構成法として有力なものとして，図 3 に示す Feistel 型と図 4 に示す SPN 型がある．Feistel 型は暗号化と復号がほとんど同じ構造で実現できるため，プログラムサイズを小さくできるという特長がある．DES や Camellia はこのタイプに属している．これに対して AES が採用する SPN 型は並列度が高く，高速処理に適しているという特長がある．MISTY, KASUMI は Feistel 型に近い構造をもつが，再帰構造により高速化・小型化を実現している．

3.　共通鍵暗号の性能

共通鍵暗号の存在価値はその性能（速度とサイズの両方を意味する）にあるといっても過言ではない．数年前までは PC 上でのソフトウエアでの処理性能が暗号の主要なベンチマークであったが，小型携帯通信機器の普及にともない，低消費電力の暗号ハードウエアが求められることが多くなっているうえ，論理の書き換えが可能な FPGA の大容量化や高性能化とあいまって，現在ではソフトウエアとハードウエアでの性能が同じ重要性をもって議論されるようになった．

高速なブロック暗号は，最新の PC 上のソフトウエアでは 10-20 cycles/byte の暗号化速度を実現するこ

表1　Camelliaのハードウエア性能

	ASIC 三菱電機0.18μ CMOS ASIC ﾗｲﾌﾞﾗﾘ	FPGA Xilinx社 Virtex1000Eｼﾘｰｽﾞ
速度 優先	3.2 Gbit/sec 355 Kgates	223.7 Mbps 1678 Slices
サイズ 優先	71.6 Mbps 6.37 Kgates	79.7 Mbps 1124 Slices

とができる．これは1コアあたり200-400 Mbyte/secに相当する．一方，組み込みマイコン向けアプリケーションで例えば認証機能を実現するような場合は，プログラムサイズ，特にRAMサイズの削減が要求されることがしばしばである．小型なブロック暗号ではROMサイズ1～2 KB，RAMサイズ数十バイト程度ときわめて小さなプログラムで実装できる．

一方，ブロック暗号ハードウエアでは，内部コンポーネントの並列化あるいは共有化によって，性能とサイズのバラエティをさまざまとることができるのが普通である．表1にCamellia暗号を例に，ASICとFPGAのそれぞれの場合に，速度優先で設計した場合の性能，サイズ優先（小型化）で設計した場合の性能をあげる．これらはいずれもパイプライン処理を行わない場合のデータであり，パイプライン処理を行うと速度はさらに数倍高速化される．

一方ストリーム暗号は，ブロック暗号のように1つのアルゴリズムでソフトウエアとハードウエアの両方で高い性能をめざすよりも，ソフトウエア向け暗号とハードウエア向け暗号が比較的はっきり分かれる傾向にある．高速なソフトウエア向けストリーム暗号は，ブロック暗号よりさらに高速で，最新のPC上では1 GB/sec以上の速度を実現するものも少なくない．一方でハードウエア向けストリーム暗号では2-3 Kgatesという小型化を実現する方式も存在する．

4．共通鍵暗号の安全性評価

共通鍵暗号の安全性評価における一般的な前提条件は，解読者は鍵の値を知ることなく，任意の長さの平文やそれに対応する暗号文の情報を得ることができるというものである．ここで，解読者が平文については，その統計量だけを知っていると仮定する場合を暗号文単独攻撃，平文そのものを知っていると仮定する場合を既知平文攻撃，平文を自由に操作できると仮定する場合を選択平文攻撃と呼ぶ．この中で選択平文攻撃がもっとも解読者にとって有利な条件であるが，ユーザ認証など選択平文攻撃が現実的となる通信が存在するため，そのような状況でも暗号は十分な安全性を有しなければならない，すなわち鍵の秘匿性が担保されなければならない．

一方で，鍵の長さをkビットとするとき，解読者は2^k通りのすべての鍵候補で暗号文を復号してみることで，必ず正しい鍵に到達することができる．したがって共通鍵暗号の安全性の評価においては，2^k以下の計算量で，鍵を高い確率で推定するアルゴリズム（Key Recovery Attack）が存在するかどうかを検証する．そのようなアルゴリズムがひとつでも存在すればその暗号の理論的解読は成功したとみなす．

また鍵を推定できなくとも，ランダムに選ばれた1つの鍵で暗号化された暗号文と，ランダムに生成されたデータとの区別を有意な確率で行うアルゴリズム（Distinguishing Attack）が存在すれば，やはりその暗号の理論的解読は成功したとみなされる．

暗号の安全性評価研究においては，解読者がもつ情報量と計算能力はきわめて大きいことを前提とするため，理論的解読が必ずしも実システムでの暗号解読には直結しないことには注意しなければならない．一方で，このような高い安全性を満足する暗号アルゴリズムを設計する研究が，暗号学の進歩を促しているのも事実である．以下代表的な共通鍵暗号の評価・解読手法についていくつかとりあげよう．

4.1　乱数評価

ストリーム暗号によって生成される擬似乱数列に統計的偏りが存在すると，ただちにdistinguishing attackが成立する．乱数性を評価するための統計的検定にはさまざまなものが知られているが，暗号でよく用いられるのは米国NISTによる乱数検定手法である[9]．ここでは15種類の検定手法が記述されている．

また擬似乱数列が，段数の短いLFSRの出力と等価になると，その線形性のゆえにこのLFSRの初期状態を容易に回復することができる．この段数を線形複雑度とよび，ストリーム暗号の重要な安全性指標のひとつである．与えられたビット列から，それを出力する最短のLFSRを求めるアルゴリズムとしてBerlekamp-Massey法が知られている．

4.2　全数探索解読

暗号鍵を1つずつすべて試行する解読法は全数探索解読あるいはBrute Force Attackと呼ばれる．この

解読は方法論的にはもっとも単純なものであるが，解読者に必要な情報量が少ないという点で，強力な解読ということができる．この解読に対する安全性指標は暗号の鍵長を意味している．

DESの鍵は56ビットであったが，この全数探索は1997年にインターネットに接続された数万台のPCで成功した[10]．またDESの全数解読専用ハードウエアが1998年に開発され56時間で解読に成功した[11]など，56ビットの鍵長は，現実的に解読が可能である．現在では，共通鍵暗号では100ビット程度の鍵長が必要であるというのがコンセンサスになっている．

米国NISTでは，十分な安全性をもつ鍵長として，2010年までは80ビット，2030年までは112ビット，それ以降は128ビットを推奨している[12]．

4.3 差分解読法

差分解読法は1990年にBihamとShamirによって提案されたブロック暗号の解読手法であり[13]，ブロック暗号のはじめての汎用的な解読原理として画期的なものであった．この解読法によってDESははじめて全数探索解読よりも高速に解読可能なことが示された[14]．

差分解読法の原理は，平文に関する差分値ΔPと暗号文の差分値ΔCを一組固定するとき，ランダムな平文Pと鍵Kに対して次の確率を（オフラインで）計算することから出発する．ここで加算は可換群演算であれば何でもよいが，通常排他的論理和をあらわす．

$$DP(\Delta P, \Delta C) = Prob_{P,K}\{ENC(P,K)+ENC(P+\Delta P,K)=\Delta C\} \quad (1)$$

ここで，もし暗号関数ENCが理想的にランダムな暗号文を生成すると仮定すると，どのようなΔPとΔCの組に対しても$DP(\Delta P, \Delta C)$は，ブロックサイズbに対して$1/2^b$程度となることが期待される．したがって$DP(\Delta P, \Delta C)$が$1/2^b$よりも有意に大きい値をとるようなΔPとΔCを解読者が見つけることができれば，選択平文攻撃のシナリオでdistinguishing attackが成立する．また鍵の値によって(1)の確率（正確には鍵を固定した場合の確率）が異なることを利用すれば，key recovery attackを行うこともできる．一般にこの解読法に必要な平文と暗号文のペアの数は$DP(\Delta P, \Delta C)$に反比例する．

したがって差分解読法に対するブロック暗号の安全性指標は$DP(\Delta P, \Delta C)$の最大値であるが，一般に与えられた暗号アルゴリズムに対してこの値を計算することは，（この指標が計算できるように設計された暗号以外では）難しい．そこで実際には以下の値$DCP(\Delta P, \Delta C)$を安全性指標とみなすことが多い．ここでRND_iは第i段の段関数であり，P_i，C_i，K_iはそれぞれRND_iの入力，出力，副鍵である．この値が十分小さければ，ほとんどの場合実際的には差分解読法に対して安全といってよい．

$$DCP(\Delta P, \Delta C) = \prod Prob_{P_i, K_i}\{RND_i(P_i, K_i) + RND_i(P_i+\Delta P_i, K_i)=\Delta C_i\} \quad (2)$$

4.4 不能差分解読法

差分解読法のバリエーションは数多く存在するが，そのなかでも不能差分は有力なもののひとつである．不能差分とは$DP(\Delta P, \Delta C)$が確率0で成立する，すなわち，どのような平文と鍵に対しても$ENC(P,K)+ENC(P+\Delta P,K)=\Delta C$が絶対に成り立たないような$\Delta P$と$\Delta C$を見つけることから出発する．

例えば5段のFeistelタイプのブロック暗号は，段関数が一対一であれば，必ず不能差分が存在することが知られている．このことを利用して$2^{b/2}$程度のデータ量でdistinguishing attackが成立する．また不能差分は，key recovery attackにおいて鍵候補を絞り込む目的でも有効に利用することができる．

4.5 線形解読法

線形解読法は1993年に筆者によって提案されたブロック暗号の解読手法であり[15]，アルゴリズムの線形近似を利用することが特徴である．差分解読法とおなじく汎用的な解読手法であり，原理的に既知平文攻撃で成立する．この解読法によってDESのはじめての解読実験が行われた[16]．

線形解読法の原理は，平文に関するマスク値ΓPと暗号文に関するマスク値ΓCの組を固定するとき，ランダムな平文Pと鍵Kに対して，次の値を（オフラインで）計算することから出発する．ここで記号・は内積をあらわす．

$$LP(\Gamma P, \Gamma C) = |2\times Prob_{P,K}\{\Gamma P\cdot P=\Gamma C\cdot ENC(P,K)\}-1|^2 \quad (3)$$

もし暗号関数ENCが理想的にランダムな暗号文を生成すると仮定すると，どのようなΓPとΓCの組に対しても$LP(\Gamma P, \Gamma C)$は$1/2^b$程度となることが期待される．したがって$LP(\Gamma P, \Gamma C)$が$1/2^b$よりも有意に大きい値をとるようなΓPとΓCを解読者が見つけることができれば，既知平文攻撃のシナリオで，ブロ

ック暗号のdistinguishing attackが成立する．また鍵の値によって(3)の値（正確には鍵を固定した場合の値）が異なることを利用すれば，key recovery attackを行うこともできる．一般に，この解読法に必要な平文と暗号文のペアの数は$LP(\Gamma P, \Gamma C)$に反比例する．

したがって線形解読法に対するブロック暗号の安全性指標は$LP(\Gamma P, \Gamma C)$の最大値であるが，一般に与えられた暗号アルゴリズムに対してこの値を計算することは，（この指標が計算できるように設計された暗号以外では）難しい．そこで実際には以下の値$LCP(\Gamma P, \Gamma C)$を安全性指標とみなすことが多い．この値が十分小さければ，ほとんどの場合実際的には線形解読法に対して安全といってよい．

$$LCP(\Gamma P, \Gamma C) = \prod |2 \times Prob_{P_i, K_i}\{\Gamma P_i \cdot P_i = \Gamma C_i \cdot RND_i(P_i, \mathrm{K}_i)\} - 1|^2 \quad (4)$$

差分解読法と線形解読法では，安全性の指標は異なるものの，その理論は共通の枠組みで議論することができる．実際，差分解読法と線形解読法にある種の双対性があることが知られている[17]．

4.6 鍵関連攻撃

共通鍵暗号の解読理論では，通常暗号鍵は固定されているとの前提で，解読者に平文や暗号文へのアクセスを許すのが普通であるが，この前提をさらに拡張し，解読者に鍵の任意のビットの反転を許すのが鍵関連攻撃である．したがって解読者は，例えば同じ平文を異なった2つの鍵で暗号化させた暗号文を得ることが可能となる．

このような状況はやや特殊ではあるが，例えば共通鍵暗号の鍵の配送を，ストリーム暗号的に乱数を排他的論理和するロジックで行っている場合に対応する．鍵関連攻撃の概念はBihamによってはじめて導入された[18]．

鍵関連攻撃は，ブロック暗号の場合，鍵スケジュール部が簡単な構造である場合に成立する．したがって鍵関連攻撃に対処するためには鍵スケジュール部に十分な非線形性が必要となる．一方でブロック暗号の小型・高速化の観点から鍵スケジュール部はできるかぎり軽いものが望ましいため，鍵関連攻撃にどの程度まで対処すべきかはその暗号が利用される状況に依存する．

4.7 代数的解読法

暗号アルゴリズムとは，平文と暗号文と鍵とを結ぶ恒等式であるため，平文と暗号文を既知と仮定すれば，これは鍵を未知数とする方程式とみなすことができる．この方程式を代数的に解くことによって鍵を導出する解読を一般に代数的解読法と呼ぶ．通常，暗号の方程式は代数式として非常に複雑になるため，解の公式を作ることは望むべくもない．

しかしながら，この方程式を正規多項式として表現した場合の次数や項数が非常に少ない場合は，代数的解読法が有効な手段になる．暗号アルゴリズムの方程式の特長は，平文と暗号文の組をとりかえることによって，同じ変数（鍵）をもつ数多くの連立方程式が得られる点にあり，このため見かけ上複雑に見える式が変数変換などによって簡単になることがある．

代数的解読法はブロック暗号，ストリーム暗号ともに適用できるが，特にストリーム暗号の内部状態を推定する方法として有力とされている．

5. サイドチャネル情報を用いた暗号評価

4節では主に暗号アルゴリズムの数学的安全性について述べたが，最近は暗号の「実装の安全性」も活発に研究されている．これは，暗号が実システムで動作する環境をもとに，暗号の演算時間やデバイスの消費電流など解読者がアクセス・取得できる物理情報（これをサイドチャネル情報という）から秘密情報を取得する方法を研究するものである．

この手法は，ICカードなど身近な暗号デバイスで，しかも比較的簡単な装置で実現できることが大きな特徴である．図5はサイドチャネル攻撃の実験系の一例で，ここではFPGAに実装された暗号アルゴリズムの電流消費量情報をPC内にとりこみ，統計処理を行うことによってチップ内の暗号鍵を推定するものである．

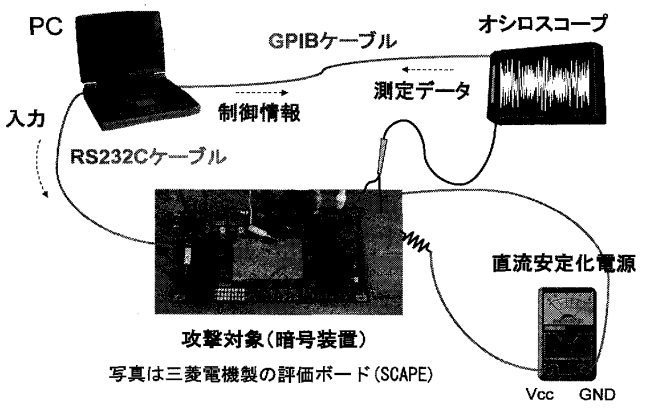

図5 サイドチャネル攻撃（電流攻撃）評価環境

この他にもアクセス速度の異なる複数のメモリをもつプロセッサ上で，このアクセス時間の差に着目して秘密情報を解読する方法（Cache Attack）や，意図的にデバイスに一時的なエラーを起こさせることで秘密情報を解読する方法（Fault Attack）など，さまざまな方法が考案・実証されている．

これらの攻撃はもちろん暗号アルゴリズムの構造と密接に関係するものの，暗号アルゴリズムの数学的構造だけで対処できるものではない．暗号の実利用環境に応じて脅威と対策コストの観点から実装方法が考えられるべきものである．サイドチャネル攻撃の最近の進展は，暗号理論と暗号実装がますます密接にリンクするようになった結果といえる．この話題については国際会議CHES（Cryptographic Hardware and Embedded Systems）で毎年最新の結果が発表される．詳細についてはhttp://www.chesworkshop.org/を参照されたい．

参考文献

[1] C. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical Journal, 28(4), pp. 656-715 (1949).

[2] Anonymous: "RC 4 Source Code," CypherPunks mailing list (September 9, 1994), available at http://groups.google.com/group/sci.crypt/msg/10a300c9d21afca0 (1994).

[3] National Bureau of Standards, "Data Encryption Standard," Federal Information Processing Standards Publication 46, U. S. Department of Commerce (1977).

[4] National Institute of Standards and Technology, "Advanced Encryption Standard," Federal Information Processing Standards Publication 197, U. S. Department of Commerce (2001).

[5] 清水明宏，宮口庄司，"高速データ暗号アルゴリズムFEAL," 電子情報通信学会論文誌，Vol. J 70-D, No. 7, pp. 1413-1423 (1987).

[6] M. Matsui, "New Block Encryption Algorithm MISTY," Proceedings of Fast Software Encryption '97, Lecture Notes in Computer Science 1267, pp. 64-74 (1997).

[7] European Telecommunications Standard Institute, "UMTS; Specification of the 3GPP Confidentiality and Integrity Algorithms," 3GPP TS 35.pp. 201-204 (1999).

[8] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima and T. Tokita, "Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms-Design and Analysis," Proceedings of Selected Areas in Cryptography 2000, Lecture Notes in Computer Science 2012, pp. 39-56 (2000).

[9] National Institute of Standards and Technology, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," Special Publication 800-22 rev. 1, U. S. Department of Commerce (2008).

[10] "DESCHALL Press Release," http://home.earthlink.net/~rcv007/despr4.htm (1997).

[11] Electronic Frontier Foundation, "Cracking DES," http://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_des_faq.html (1998).

[12] National Institute of Standards and Technology, "Recommendation for Key Management," Special Publication 800-57, U. S. Department of Commerce (2007).

[13] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," Proceedings of CRYPTO '90, Lecture Notes in Computer Science 537, pp. 2-21 (1990).

[14] E. Biham and A. Shamir, "Differential Cryptanalysis of the Full 16-Round DES," Proceedings of CRYPTO '92, Lecture Notes in Computer Science 740, pp. 487-496 (1992).

[15] M. Matsui, "Linear Cryptanalysis Method for DES Cipher," Proceedings of Eurocrypt '93, Lecture Notes in Computer Science 765, pp. 386-397 (1993).

[16] M. Matsui, "The first experimental cryptanalysis of the data encryption standard," Proceedings of CRYPTO '94, Lecture Notes in Computer Science 839, pp. 1-11 (1994).

[17] M. Matsui, "New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis," Proceedings of Fast Software Encryption '96, Lecture Notes in Computer Science, pp. 205-218 (1996).

[18] E. Biham, "New Types of Cryptanalytic Attacks Using Releated Keys," Journal of Cryptology, Vol. 7, No. 4, pp. 229-246 (1994).