

「ブロック暗号ガイドブック」について

清水 秀夫[†] 関 春樹[†] 金子 泰祥[†] 宮野 浩[‡] 金子 敏信^{*}

[†]通信・放送機構 横浜リサーチセンター

〒 221-0031 横浜市 神奈川区 新浦島町 1-1-32 ニューステージ横浜 1F

電話番号: 045-450-1245 E-mail: {shimizu hseki kaneko}@yokohama.tao.go.jp

[‡]NEC ソリューションズ インターネットソフトウェア開発本部

〒 108-8557 東京都港区芝浦 2-11-5

電話番号: 03-5476-1284 E-mail: miyano@ab.jp.nec.com

* 東京理科大学 理工学部 電気工学科

〒 278-8510 千葉県 野田市 山崎 2641

電話番号: 0471-24-1501 (内 3709) E-mail: kaneko@ee.noda.sut.ac.jp

あらまし 通信・放送機構 (TAO) の情報セキュリティ技術に関する研究開発プロジェクトが成果の一つとしてまとめた「共通鍵ブロック暗号の選択/設計/評価に関するドキュメント」(ブロック暗号ガイドブック)を紹介する。

キーワード 共通鍵ブロック暗号, ガイドブック, 通信・放送機構

On the Block Cipher Guidebook

Hideo Shimizu[†] Haruki Seki[†] Yoshiyasu Kaneko[†] Hiroshi Miyano[‡]
Toshinobu Kaneko^{*}

[†]Yokohama Research Center, Telecommunications Advancement Organization of Japan
New Stage Yokohama, 1-1-32 Shin-urashima-cho, Kanagawa-ku, Yokohama, 221-0031 JAPAN

TEL: +81-45-450-1245 E-mail: {shimizu hseki kaneko}@yokohama.tao.go.jp

[‡] NEC Corporation

2-11-5, Shibaura, Minato-ku, Tokyo 108-8557, JAPAN

TEL: +81-5476-1084 E-mail: miyano@ab.jp.nec.com

*Department of Electrical Engineering, Science University of Tokyo

2641 Yamazaki Noda, Chiba, Japan 278-8510

TEL: +81-471-24-1501(ex.3709) E-mail: kaneko@ee.noda.sut.ac.jp

Abstract We summarize the document "Technical Report on Design, Analysis and Use of Block Ciphers", which is a part of a result of Information Security Project of Telecommunications Advancement Organization of Japan.

Key Words Symmetric Block Encryption Algorithm, Guidebook, Telecommunications Advancement Organization of Japan

1 はじめに

通信・放送機構¹が1995年10月に開始した直轄プロジェクトである「情報セキュリティ技術に関する研究開発プロジェクト」²は、2000年9月末日に5年間のプロジェクト期間を終える。本稿では、プロジェクトの成果の一環として作成した「共通鍵ブロック暗号の選択/設計/評価に関するドキュメント」の概要を紹介する。以下、ガイドブックと呼称することにする。

2 ガイドブックの概要

ガイドブックはタイトルの通り、共通鍵ブロック暗号に焦点を当てている。例えば公開鍵暗号と共通鍵暗号の違いといったような一般の教科書に書いてあるようなことは一切書かれておらず、まさに共通鍵ブロック暗号のことだけを掘り下げている。

研究員が第1稿を執筆し、サブリーダーの先生方を交えた16回のレビューにより推敲を重ね、作成作業は約1年間に渡っている。

目的 ガイドブック作成の目的として以下を考えた。

- 蓄えられた知見や技術を集約して、より広く利用可能にする。
- 「研究者の皮膚感覚」を明文化する。

共通鍵ブロック暗号に関して深く掘り下げた教科書が日本語では見当たらないので、前者は意義があると考える。また後者は通常は論文等には記載されないような事由まで集積するということである。

編集方針 以上の目的を実現するために以下のような方針で編集を行った。

- 「利用者編」「設計者編」に分け、読者層を想定することで記事の視点に一貫性を持たせるようにした。
- 各記事について、その項目だけを読めば最低限の知識は得られるような構成になるべくするために、記事間の記述の重複は恐れないこととした。
- 各項目の記述をなるべく簡潔にするために、より深い知識を必要とする読者には、各自参考文献を読んでいただくことを前提とした構成になっている。そのために、参考文献は、各記事毎に記されている。

3 ガイドブックの構成

タイトルにある選択/設計/評価という3本の柱を軸に7つの章で構成した。この7つの章を対象となる読者を元に2つのパートに大別した。

Part I 共通鍵暗号の導入・選択 (利用者編) 対象となる読者は、共通鍵ブロック暗号をシステムに組み込もうとする技術者であり、組み込もうとする暗号アルゴリズムを選択する際に知っておくべきことを中心に記述している。即ち、3つの柱のうちの「選択」である。

Part I は以下の3つの章で構成されている。

¹<http://www.shiba.tao.go.jp>

²<http://www.yokohama.tao.go.jp>

第1章 導入・選択時の判断要素とその概要

共通鍵ブロック暗号をシステムに導入する際に、どのような判断要素があり、どのように考慮しなければならないかを取り上げた。

第2章 暗号解析学的な安全性と実用上の安全性との関連

まず安全性(攻撃)について最低限知っていた方がよいと思われる事柄を述べた後、実際にシステムに対する脅威を判定するための方法について述べている。

第3章 標準化について

共通鍵ブロック暗号アルゴリズムの標準化動向、および様々な暗号利用技術の国際標準を取り上げた。

Part II 共通鍵暗号の設計・評価(設計者編) 対象となる読者は、これから暗号アルゴリズムの設計を行おうとしている技術者、もしくは暗号研究を行おうとしている初学者である。様々な知見や情報を集約することで導入を容易にすることを目的としている。

Part II の前半の4,5章は「設計」に当てられ、後半の6,7章は「評価」に当てられている。

第4章 共通鍵ブロック概論

背景となる知識として、研究の流れを中心とした共通鍵ブロック暗号の歴史と、1章で取り上げた判断要素と対をなす設計思想を取り上げた。

第5章 共通鍵ブロック暗号の設計

共通鍵ブロック暗号アルゴリズムを解剖し、各パーツについて解説した。

第6章 代表的な攻撃アルゴリズム

現在、代表的と考えられる差分攻撃や線形攻撃のような攻撃アルゴリズムを取り上げ、各々について解説した。設計者はあらゆる攻撃を熟知していなければならない。

第7章 設計事例の分析

既存の暗号アルゴリズムの様々な設計から欠点を抽出し分析することで、今後の設計への教訓(反面教師)とすることを意図している。

4 まとめ

どのような目的、方針でガイドブックを作成したか、またガイドブックがどのような構成になっているのかについて述べた。

本稿で述べたガイドブックは共通鍵ブロック暗号だけを取り上げているということで言えば非常にユニークで他に類をみないドキュメントである。IT文明の拡大に伴うセキュリティ技術の重要性が増している今日、本稿で取り上げたガイドブックが、特に急峻な進歩を遂げている共通鍵ブロック暗号技術を敷衍するための一助となることを期待したい。

正誤表

p.ii (誤) 日立制作所 → (正) 日立製作所

p.ii (誤) 大熊 健司 → (正) 大熊 建司

2.4.1 CPUハードウェア攻撃—鍵全数探索攻撃	17
2.4.2 アルゴリズム解析(情報収集)型攻撃	19
2.4.3 弱い鍵	20
2.4.4 CPUハードウェア攻撃—鍵全数探索攻撃の効率を上げる方法	20
2.5 暗号の強度を示すアプローチの仕方(数学的, 実証, call for attack)による判断	21
2.6 公開鍵暗号との併用	23

3 標準化について

3.1 AES (Advance Encryption Standard)	25
3.2 ISO/IEC 9799 暗号アルゴリズム登録手続きについて	25
3.3 ISOによる暗号アルゴリズムの標準化について	27
3.4 NISSIEプロジェクト	28
3.5 暗号利用技術に関連する標準	29
3.5.1 国際標準 (ISOとISO/IEC)	30
3.5.2 金融に関するセキュリティ標準 (ANSI X3)	31
3.5.3 金融に関するセキュリティ標準 (ANSI X9)	31
3.5.4 金融に関するセキュリティ標準 (ISO)	32
3.5.5 日本工業規格 (JIS)	32
3.5.6 米政府標準 (FIPS)	33
3.5.7 RFCとInternet Standard	34
3.5.8 その他	34
3.6 ISO/IEC/SC27における共通鍵暗号に関する国際標準(抜粋)	34
3.6.1 ISO/IEC 8372: 64ビット共通鍵暗号のための利用モード	34
3.6.2 ISO/IEC 9797: メッセージ認証子 (MAC; Message Authentication Code)	35
3.6.3 ISO/IEC 9798-Part2: 相手認証メカニズム	36
3.6.4 ISO/IEC 10118-Part2: 共通鍵暗号を用いたハッシュ関数	38
3.6.5 ISO/IEC 11770-Part2: 共通鍵暗号を用いた鍵管理	39

Part I 付録, ETSIにおける暗号アルゴリズム標準化動向について

II 共通鍵暗号の設計・評価(設計者編)

Part IIのはじめに	45
4 共通鍵ブロック暗号概論	47
4.1 共通鍵ブロック暗号の歴史と背景	51
4.1.1 DES	51
4.1.2 FEALと他の暗号	52
4.1.3 差分攻撃 線形攻撃	52
4.1.4 Nybergらの証明可能安全性	53
4.1.5 その他の攻撃	54
4.1.6 DES Challenge	54
4.1.7 AES	55

目次

まえがき	i
目次	v
図目次	xi
表目次	xiii
I 共通鍵暗号の導入・選択(利用者編)	1
Part Iのはじめに	3
1 導入・選択時の判断要素とその概要	5
1.1 利用目的は何か?	5
1.2 暗号の実装を対象とした環境は何か?	6
1.3 入出力ブロック長	6
1.4 処理速度	6
1.5 安全性	7
1.5.1 アルゴリズムの公開・非公開と安全性	7
1.5.2 実装からの判断	8
1.5.3 暗号の強度とシステムの要求仕様との整合性の検証	8
1.6 評価実績/使用実績	9
1.7 設計の透明性	9
1.8 アルゴリズムの公開/非公開	10
1.9 知的財産権	11
1.10 輸出規制	11
2 暗号解析的な安全性と実用上の安全性との関連	13
2.1 暗号利用における安全性とは	13
2.2 暗号解読での攻撃概要	15
2.2.1 攻撃に必要な情報からみた分類	15
2.2.2 攻撃方法からみた分類	15
2.3 暗号解析的に評価された暗号の強度とは	17
2.4 暗号の強度とシステムの要求仕様との関連付け	17

4.2	共通鍵ブロック暗号のトピック	57
4.2.1	Confusion と Diffusion	57
4.2.2	証明可能な安全性の歴史	57
4.2.3	Key Escrow	58
4.2.4	サイドチャネル攻撃	58
4.2.5	学会	59
4.3	設計思想・方針	69
4.3.1	暗号の設計目的・用途は何か?	69
4.3.2	暗号の利用目的は何か?	70
4.3.3	どのようなプラットフォームが?	71
4.3.4	従来技術との連続性?	71
4.3.5	安全性をどう信用してもらうか	71
4.3.6	従来の暗号よりも強く	73
4.3.7	設計方針を透明に — データもシカケもトラップドアはありません	73
4.3.8	攻撃の適用困難性と安全性との関係	74
4.3.9	アルゴリズムの公開/非公開?	75
4.3.10	特許	76
5	共通鍵ブロック暗号の設計	79
5.1	暗号設計の手順	79
5.1.1	入出力仕様	79
5.1.2	性能	80
5.1.3	設計項目	80
5.1.4	設計手順	81
5.2	設計思想とテクニック	81
5.3	共通鍵ブロック暗号の基本構造	82
5.3.1	Feistel 構造	82
5.3.2	変形 Feistel 構造	84
5.3.3	SPN 構造	84
5.3.4	変形 Feistel 構造の分類	85
5.4	差分/線形攻撃に対する安全性保証の概観	87
5.4.1	最大差分/線形確率と最大差分/線形特性確率の定義	87
5.4.2	差分/線形攻撃に対する安全性の下界を保証する方法	89
5.4.3	強度概観評価尺度を用いた設計方法	91
5.4.4	最小 Active S-box の数を大きく (保証) する構造	93
5.5	ラウンド数の決定	95
5.6	S-box の設計	97
5.6.1	S-box の設計概要	97
5.6.2	Bent 関数と Perfect Nonlinear な関数	99
5.6.3	再帰的な構成法	103
5.6.4	affine 変換 + べき乗	105
5.7	拡散層の設計	106
5.7.1	拡散層の概要	106
5.7.2	拡散層の事例	107
5.7.3	分岐数を大きく (保証) する構造	109
5.7.4	データの swap 構造について	113
5.8	鍵スケジュールの設計	113
5.8.1	鍵スケジュールの概要	114
5.8.2	DES-80 プロジェクト	114
5.8.3	Strong Key Schedule	117
5.9	補助的関数	118
5.10	その他	119
5.10.1	代数的構造の異なる演算の組み合わせによる安全性の向上	119
5.10.2	ビットストライズ法	120
5.10.3	Luby-Rackoff 暗号	122
6	代表的な攻撃アルゴリズム	125
6.1	鍵探索攻撃とそのバリエーション	126
6.1.1	鍵探索攻撃	126
6.1.2	等価性、complementation 特性、simple relations を利用した攻撃	126
6.1.3	表参照攻撃	128
6.1.4	タイムメモリートレードオフ攻撃	129
6.2	差分攻撃とそのバリエーション	130
6.2.1	差分攻撃	130
6.2.2	Truncated Differential Attack (切語差分攻撃)	131
6.2.3	Impossible Differential Attack (不可能差分攻撃)	132
6.2.4	Boomerang Attack (ブーメラン攻撃)	133
6.3	線形攻撃とそのバリエーション	135
6.3.1	線形攻撃	135
6.3.2	差分線形攻撃	136
6.3.3	線形ふるい攻撃	138
6.4	代数的性質に着目した攻撃	139
6.4.1	高階差分攻撃 (Higher Order Differential Attack)	139
6.4.2	補間攻撃 (Interpolation Attack)	142
6.5	鍵スケジュールの弱点を利用した攻撃	146
6.5.1	中間一致攻撃	146
6.5.2	Slide Attack	149
6.5.3	Related-key attack (鍵関連攻撃)	150
6.6	Partitioning Attack (分割攻撃)	153
6.7	mod n Attack	155
6.8	その他の攻撃	157
6.8.1	本来の暗号を弱体化して傾向をつかむ	157
6.8.2	閉構造、Purity 構造を利用した攻撃	159
6.8.3	Multiple Modes of Operation (多重利用モード) に対する攻撃	162
6.8.4	暗号機器の物理的観測による攻撃	162
6.8.5	故障利用攻撃	163

7 設計事例の分析	165
7.1 段数が少ない暗号で問題となりやすい点	165
7.2 active S-box の数が少ない暗号で問題となりやすい点	166
7.3 鍵の bit 数が少ない暗号で問題となりやすい点	167
7.4 鍵のみに依存した可変 swap 構造で問題となりやすい点	168
7.5 問題のある鍵スケジュールの事例	170
7.6 弱鍵の事例	171
7.7 使用する演算の代数構造が共通な場合に問題となりやすい点	173
7.8 べきだけを使った暗号で問題となりやすい点	175
7.9 平文の分布の既知の偏りに起因する問題点の事例	177
7.10 F 関数の差分特性 $\alpha \rightarrow 0$ が高確率で成立する場合に問題となりやすい点	177

Part II 付録. ストリーム暗号の現状と課題	179
----------------------------------	------------

参考文献

181

索引

195