DES と AES に関するメモ

2001/06/15

すずきひろのぶ

hironobu@h2np.net

目次

DES

はじめに

DES (Data Encryption Standard)は FIPS(FIPS46)、ANSI(X3.92)、そして ISO(DEA-1)という規格として過去 20 年以上にもわたり使われてきた共通鍵暗号アルゴリズムである。DES は商用レベルの暗号ではアルゴリズムを完全に公開した初めての暗号アルゴリズムである。

FIPS46-3 ではシングル DES はレガシーサポートのためのみ利用としており、暗号化・復号化には Triple DES を利用することになっている。

DES が作られるまで

1972 年、National Institute of Standard Technology (NIST)の前身である U.S. National Bureau of Standard (NBS) がコンピュータのデータや通信の保護を目的として利用する暗号アルゴリズムの標準化作業を開始した。十分に安全性を検証し、かつ、インターオペラビリティを持ち、実用に耐えうる 1 つの暗号アルゴリズムをデータ暗号化のための標準アルゴリズム(Data Encryption Standard)を決めるのが目標であった。

1973 年 5 月 15 日に NBS は標準暗号アルゴリズムの公募を開始した。アルゴリズムには次のようなことが求められた。

- 高度なセキュリティを提供すること
- 仕様に曖昧さはなく、簡単に理解できること
- アルゴリズムが公開されていても安全であること
- アルゴリズムはすべてのユーザが使えること
- さまざまなアプリケーションへの適合性があること
- 経済的なハードウェアとしてインプリメントできること
- 処理効率が高いこと
- アルゴリズムは検証可能なこと
- などなど

最初の公募期間には 1 つもプロポーサルが提出されなかったため、NBS は 1974 年 8 月 27 日に再公募を行う。その際に唯一提出されたのが 1970 年代初期から IBM が開発を行っていた Lucifer という暗号アルゴリズムであった。

NBS はアルゴリズムの安全性を評価し、連邦規格として適切な暗号するために NSA の協力を仰いだ。IBM は Lucifer に関連するいくつかのパテントを取得していたが、NBS はアルゴリズムを連邦規格として利用するために IBM に対し知的所有権の行使の停止を求めた。IBM は NBS の要請に対して合意した。これにより後の DES は特許権に縛られることなく第三者が利用できるようになった。

1975 年 3 月 17 日 IBM の提出したアルゴリズムを公開し、パブリックコメントを求める。また同年 8 月 1 日にも再度パブリックコメントを求めている。1976 年に 2 度のワークショップを開催し応募された暗号アルゴリズムである Lucifer について議論・評価を行っている。このワークショップはアルゴリズムの設計者、暗号研究者、ベンダ、ユーザらが多数参加した。最初のワークショップでは NSA によるトラップドアが議論になり、次のワークショップでは鍵の長さが議論された[MORRIS78]。

1977 年 1 月 15 日 NBS から FIPS PUB 46 “Data Encryption Standard”が発行される。なお規格の発効日は文章の発行日から 6 ヶ月後である。DES のオペレーションモードの規格 “DES Modes of Operation”が 1980 年に発行される。さらに暗号の実装に関してのガイドライン FIPS PUB 74 が 1981 年に発行される。この文章中には Weak Key、Semi-Weak Key に関しての説明がある。NBS はこれ以外にも DES をパスワードに用いる方法(FIPS PUB 112)、DES をコンピュータデータの認証に使う方法(FIPS PUB 113)なども発行している。一連の評価においては常に NSA がアドバイスを行っていたはずであるが、どのような内容がアドバイスされたかは一切公表されていない。そのため、その後 20 年以上にわたり DES にはトラップドアが仕掛けているのでないかという疑念をもたれることになる。

年表	
年	主な内容
1972	標準化作業開始
1973	公募開始（5 月）
1974	再公募（8 月）
1975	パブリックコメント募集(3 月、8 月)
1976	ワークショップ
1977	FIPS PUB 46 発行(1 月)

Lucifer

Lucifer は IBM が開発した DES の前身となった共通鍵暗号アルゴリズムである。1960 年代後半に IBM がコンピュータ暗号技術の研究として初期は Horst Feistel が、後に Walt Tuchman が中心となり研究を進めていた。IBM のキングストン研究所とヨークタウンハイツの両方研究所が共同で開発する形を取った[COPPERSMITH2000]。

Lucifer はラウンド 16 段、ブロックサイズが 128 ビット、鍵長が 128 ビットであるブロック暗号である。Lucifer は 2 つの異なるアルゴリズム方式を組み合わせて出来ている。1 つは Feistel によって作られた SP-Net 型の暗号であり、もう 1 つは Lynn Smith によって作られた暗号である。今日 Feistel 構造と呼ばれるアイデアを最初に Lucifer に組み入れたのは Smith である。DES の重要な 2 つのコンセプトである Product cipher（2 つ、あるいはそれ以上の変換を合成して利用する手法）と Feistel cipher（暗号化するブロックを半分にしてスワップする手法）は、このようにして Lucifer に組み入れられた。Lucifer の安全性だが Ralated-Key 攻撃を使えば 2^{33} の chosen-key chosen plaintext によって解読可能[BIHAM93]である。

DES の安全性の変遷

暗号分析理論

Lucifer は DES の前身となった暗号だが、Lucifer が鍵長 128 ビットであるのに対し、DES では 56 ビットと大幅に縮小された。また DES の S-BOX 構造に関しての説明は、当時一切されなかった。そのため長い間、NSA が DES にトラップドアを仕掛けたのではないかという疑惑が持たれた。特に鍵長が短いことに関して 1977 年当時から批判[DIFFIE77]があった。

DES の安全性に関して最初に取り上げられるべきものは 1990 年に E. Biham と A. Shamir が発表した差分攻撃（Differential Cryptanalysis） [BIHAM90]である。DES に似た構造を持つ暗号に対しこの暗号分析方法は非常に有効であったが、DES に対しては有効な分析とはならなかった。DES の S-BOX 設計時に既に差分攻撃のような暗号解析方法を想定していたからである。差分攻撃に対し DES が耐性を持っていることは DES が解読されるまで伏せられていた[COPPERSMITH94]。

DES に対して最初の効果的な解読方法は､松井が 1993 年に発表した線形攻撃法 (Linear Cryptanalysis) [MATSUI93]である。線形攻撃法に対して DES は耐性を持っていなかった。翌年、線形攻撃法によって初めてフルスペックの DES (16 段)が解読された[MATSUI94]。このときの解読には HP9735/PA-RISC 99MHz のワークステーション 12 台を利用して 50 日間（前処理に約 40 日間、鍵検索に約 10 日）かかった。下山・金子による改良された線形攻撃法[SIMOYAMA98]では松井の 73.5%の処理量で済むようになり、Sun Ultra SPARC 167Mhz を 14 台、同 200Mhz を 2 台、と DEC Alpha 21164A 500Mhz を 1 台利用して約 7 日（前処理約 6 日間、鍵検索約 4 時間）で解読できるまでになった。

DES Challenge

DES Challenge は米 RSA 社が主催した DES の解読コンテストである。1 組の平文と暗号文（及び IV）を与えて鍵を探すというルールなので、基本的には DES の鍵空間に対して総当り検索を争うコンテストと同等である。この DES Challenge は、1997 年から 1998 年に合計 4 回行われた。1997 年 1 月 28 日開始された DES Challenge I は distributed.net のネットワーク分散方式により 140 日で解読された。この方法は distributed.net がインターネットに接続しているコンピュータをもっている多数のボランティアを募り、そのコンピュータ上で解読専用のソフトウェアを走らせる分散処理を行うというものである。1998 年 1 月 13 日から開始された DES Challenge II-1 も distributed.net が 39 日という期間で解読している。

1998 年 7 月 13 日から開始した DES Challenge II-2 では Electronic Frontier Foundation が DES Challenge のために設計した専用マシンを用意し 56 時間での解読に成功した。21 万ドルもの制作費かけた EFF DES Cracker [EFF98]は、鍵空間検索用に設計された専用 LSI AWT-6001 を 1536 個登載している DES Challenge 用の特殊な並列マシンである。1 つのチップは、さらに 24 個の鍵検索ユニットを内蔵している。

この EFF DES Cracker プロジェクトのプロデューサーは EFF の John Gilmore だが、実際の開発は米 Cryptography Research 社と米 Advanced Wireless Technologies 社が共同であたった。EFF DES Cracker は毎秒約 92 億個分の鍵検索を行うので、56 ビットの鍵空間のすべてを検索するとしても 9 日強しかかからない。DES Challenge III では distributed.net [DISTRIBUTED99] と EFF が協力し 22 時間 16 分で解読する成果を出している。

Triple DES

Triple DES は DES の EDE モードである。64 ビットの入力ブロックを I、64 ビットの出力ブロックを O とし、DES で鍵 K を用いての暗号化を $O=E_k(I)$、復号化を $O=D_k(I)$とするとき、Triple DES は $O = E_{k3}(D_{k2}(E_{k1}(I)))$と表現できる。FIPS 46-3 は K1、K2 および K3 の扱いたいして 3 つのモードを用意している。

- モード 1　K1、K2、K3 が独立である(168 ビット長鍵)
- モード 2　K1、K2 が独立であり、K1 と K3 が同じである(112 ビット長鍵)
- モード 3　K1、K2、K3 が同じである(56 ビット長鍵　/ DES と同等)

慣用的には 3DES と記述されるが FIPS 46-3 では TDES と表現する。

DES の構造

添付資料 “FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION “DATA ENCRYPTION STANDARD (DES)” (FIPS PUB 46-3)”を参照のこと。

補足

- DES は FIPS 46/46-1 では DES は 64 ビット長の鍵とし、56 ビットを暗号・復号に利用し、残り 8 ビットはパリティとして定義されていた。FIPS 46-2 以降では 8 ビットのパリティに関しては付帯条項として(may 条件)として扱われている。

- FIPS 46/46-1 では DES はハードウェア実装での利用が推奨されていたが、FIPS 46-2 からはソフトウェア実装、ハードウェア実装の区別による推奨はなくなった。

AES

はじめに

AES (Advanced Encryption Standard)は DES に代る米国の次世代標準暗号化アルゴリズムである。1990 年代後半にもなると DES の安全性・信頼性が低下してきたため、Triple DES(FIPS 46-3)が利用されるようになる。ところが Triple DES は、DES を 3 回繰り返すため今日の高速な CPU であってすら処理が重いという現実的な問題があった。

そのためインターネットで利用されるアプリケーション[RFC2828]を中心に IDEA、CAST、Blowfish、RC2、RC4 といった 128 ビット鍵長を持つ高速な暗号化アルゴリズムが利用される傾向が出てきた。TDES は FIPS 46-3 としてインターオペラビリティを保つための標準としては存在しているが、*de facto* スタンダードではなかった。そこで今までの DES にかわって使うべく十分に安全で、かつ高速な暗号を選ぶ必要性が出てきた。

また実際に使われている新しい暗号の多くは学術的な場で安全性を議論されており、ある程度安全だと認められているものが主であるが、それであっても徹底して安全性を議論・検証したものとはいえない。その点でも十分に安全性を議論し検証を重ねた、誰もが安心して使える暗号アルゴリズムが必要であった。

AES 選出のプロセス

1997 年に米国商務省傘下の技術標準化組織である NIST (National Institute of Standards and Technology)が DES に代る次世代標準化暗号の選定計画を開始した。まず 1998 年中に AES 候補として世界中から公募を行い、そこから約 1 年をかけ評価[NISTREP1] [NISTREP1+]し決勝戦に残る 5 つの候補に絞る。さらに約 1 年をかけて、その 5 候補の評価を行い、AES を決める。後に AES に選出された暗号アルゴリズムは FIPS (連邦標準)化される。

NIST が主催し、NSA が技術コンサルタントとして行われた。AES の審査プロセスにおいては関係するデータをすべて Web で公開する[NIST97][SMID99]している。最終審査に残る 5 候補はソースコードも含めて、アルゴリズムに関する資料すべてをダウンロードできるようになっている。またラウンド期間中、パブリックコメントを求めると同時に NIST

の Web サイトではディスカッショングループを用意するなど、オープンな形で運営されていた。

2000 年 10 月、Rijndael[RJINDAEL01][RIJMEN01]が AES として選出された。現在（2001 年 3 月）は FIPS 文章のドラフトを公開し[NIST01]、パブリックコメントを求めている最中である。2001 年の 8 月から 10 月ぐらいには正式な FIPS として発行される予定である。

年表	
1997 年 1 月	米国商務省(NIST)が AES 選定計画発表
1997 年 4 月	AES Workshop 開催
1997 年 9 月	AES 候補受付アナウンス
1998 年 6 月 15 日	提出締切り
1998 年 8 月 20~22 日	第一回 AES カンファレンス ラウンド 1 の評価期間に入る
1999 年 3 月 22~23 日	第二回 AES カンファレンス
1999 年 4 月 15 日	ラウンド 1 終了
1999 年 8 月 9 日	ファイナリスト発表 ラウンド 2 の評価期間に入る
2000 年 4 月 13~14 日	第三回 AES カンファレンス
2000 年 10 月 2 日	Rijndael を AES に選出
2001 年 2 月 28 日	FIPS ドラフト公開・パブリックコメント募集
2001 年 5 月 29 日	パブリックコメント締切り
2001 年 8~10 月	FIPS 発行予定

ラウンド

AES の選出を行った期間中はラウンドと呼ばれる 3 つの期間に分かれている。各々の呼び方と期間は下表のとおりである。

期間の呼び方	
プレ・ラウンド期間	1997 年 1 月～1999 年 7 月
ラウンド 1 期間	1998 年 8 月～1999 年 4 月
ラウンド 2 期間	1999 年 8 月～2000 年 5 月

プレ・ラウンド期間

1997 年 9 月に応募開始をアナウンスした。技術的な要求仕様の概要は以下のようなものである。

- 共通鍵暗号であること
- ブロック暗号であること
- ブロックサイズが 128bit をサポートしていること
- 鍵長が 128bit、192bit、256bit がサポートされていること

AES 候補として評価期間中における知的財産権の権利停止、AES として決定した場合、知的財産権行使を放棄する(無償使用許諾)ことなどが求められる。提出には実際に動く C と Java コード及びライセンスに関する契約書類などが必要である。応募者が提出用パッケージを用意する時に漏れがないようにと NIST が作ったチェックリストには全部で 241 項目がリストアップされている。尚、動作する評価プラットフォームは以下の通り。

- IBM PC 互換機, CPU Pentium Pro 200Mhz, メモリ 64MB
- Windows 95, Borland C++ 5.0 コンパイラ, JDK 1.1

1998 年 6 月 15 日までに世界各地から応募してきた暗号アルゴリズムは 12 ヶ国・21 アルゴリズムあった。書類の不備や応募したコードが指定プラットフォームで動作しなかったなどの理由で 6 つが受け付けられなかった。応募規定をクリアした 15 種類のアルゴリズムがラウンド 1 で評価対象となる。この段階では応募規定のみしか審査しておらず、アルゴリズムが妥当であるかの評価などは一切していない。

ラウンド 1		
暗号アルゴリズム名	国名	開発者
CAST-256	カナダ	Entrust Technologies, Inc.
CRYPTON	韓国	Future Systems, Inc.
DEAL	カナダ	R. Outerbridge, L. Knudsen
DFC	フランス	CCNRS - Ecole Normale Superieure
E2	日本	NTT, 横浜国大
FROG	コスタリカ	TecApro International S.A.
HPC	米国	R. Schroeppel
LOKI97	オーストラリア	L. Brown, J.Pieprzyk, J. Seberry
MAGENTA	ドイツ	Deutsche Telekom AG.
MARS	米国	IBM
RC6	米国	RSA Laboratories
Rijndael	ベルギー	J. Daemen, V. Rijmen
SAFER+	米国	Cylink Corporation
Serpent	英国・イスラエル・ノルウェー	R. Anderson, E.Biham, L. Kundsen
Twofish	米国	B.Schneier, J.Kelsey, D.Whiting, D.Wagner,そのほか

ラウンド 1

1998 年 8 月 20 日～22 日の期間、米国カリフォルニア州ベンチェラ市で最初の AES カンファレンスが開催された。カンファレンスでは各 AES 応募者が応募したアルゴリズムのプレゼンテーションを行った。ラウンド 1 へ進出したアルゴリズムというのは提出が受け付けられただけの意味しかない。そのため提案されたアルゴリズムの中には評価に値しないような暗号も含まれていた。評価に値するアルゴリズムの範囲ではカンファレンス開催以前に安全性に問題があると指摘されてしまった LOKI 97 や SAFER+、あるいはカンファレンス中に安全性に問題があると指摘された MAGENDA などがあった。第 2 回目の AES カンファレンス[AESCONF2]は 1999 年 3 月 22 日～23 日の期間、イタリアのローマで行われた。ここでは 28 論文の発表があった。

ラウンド 1 の間はアルゴリズムのマイナーな変更が(Tweaks)が許されることになっており、CRYPTON、HCP、MARS、SEAFER+1 の 4 つのアルゴリズムは修正を提出した。

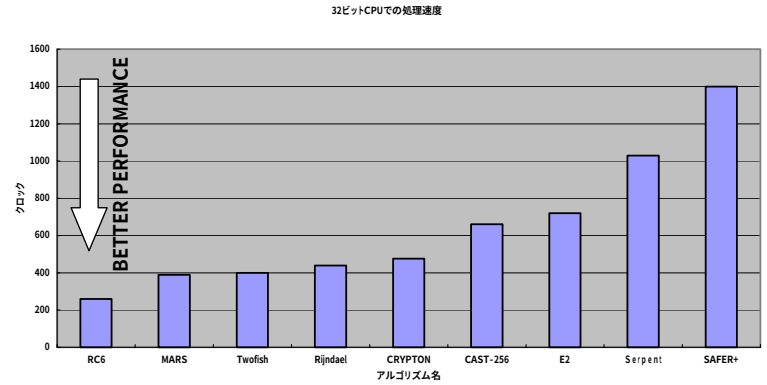
安全性に対するクレームだが、NIST が安全性に大きな問題があると指摘したアルゴリズムは以下の通り。

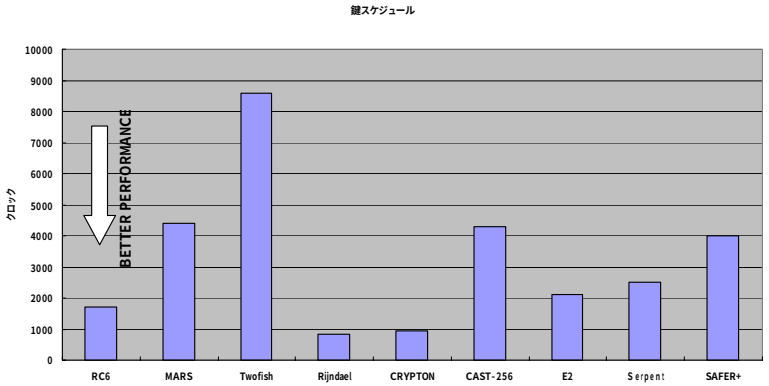
理論的に解読可能	DEAL、LOKI97、MAGENTA
解読可能な弱い鍵が多数ある	FROG、HPC

小さい点ではあるが問題がわかったと指摘した暗号は以下の通り。

CRYPTON	256bit 鍵長では多くの弱鍵がある
SAFER+	256bit 鍵長さでは related-key 攻撃と meet-in-the-middle 攻撃に対し弱さがある

最終的に MARS、RC6、Rijndael、Twofish、Serpent の 5 つがラウンド 2 に進出することになった。技術的な詳細に関しては文献[NISTREP1]を参照されたい。MARS、RC6、Rijndael、Twofish は 32 ビット CPU 上での処理速度トップ 4 を選んだのと同じ結果である。処理速度では不利な Serpent であるが、他のアルゴリズムと比較して、非常に大きなセキュリティマージンを取っているという特徴がある。





AES ファイナリスト		
アルゴリズム名	応募者	特徴
MARS	IBM	● 十分なセキュリティマージン ● 32 ビット CPU 上で高速 ● 鍵長が可変 ● 鍵スケジュール部分に修正あり
RC6	RSA	● シンプルな構造 ● 32 ビット CPU 上で非常に高速 ● 鍵長、ブロック長、ラウンドが可変
Rijndael	Daemen、Rijmen	● どのプラットフォームでも高速 ● 鍵長、ブロック長が可変 ● 大きなマイナス点がない
Twofish	Schneier、Kelsey、Whiting、Wagner、Hall、Ferguson	● 十分なセキュリティマージン ● おおよそのプラットフォームで高速 ● Space/Time のトレードオフが可能
Serpent	Anderson、Biham、Kundsen	● 非常に大きなセキュリティマージン ● ローエンドの smart card 向き ● ビットスライスによる実装

ラウンド 2

ラウンド 2 では最終候補を 5 つに絞り、ハードウェア実装時の効率などまで含め、さらに詳しく評価する。2000 年 4 月 13~14 日にニューヨークで行われた第三回 AES カンファレンス[AESCONF3]では。ハードウェア実装、64 ビットプロセッサへのインプリメント、DSP へのインプリメント、SmartCard へのインプリメントなどの発表が行われた。NSA からはハードウェア実装に関する報告があった。ちなみに AES 選出のプロセスにおいて NSA からの関与はこれ以外には見当たらない。

AES 決定について

2000 年 10 月、Rijndael が AES として選ばれた。Rijndael は SP-Network 構造をもつ SQAURE タイプの暗号アルゴリズムである。Vincent Rijmen による Rijndael 公式 Web ページには AES に提出したドキュメントも含め、リファレンスコード、他の Rijndael に関する情報を掲載しているサイトへのリンクが用意されている。

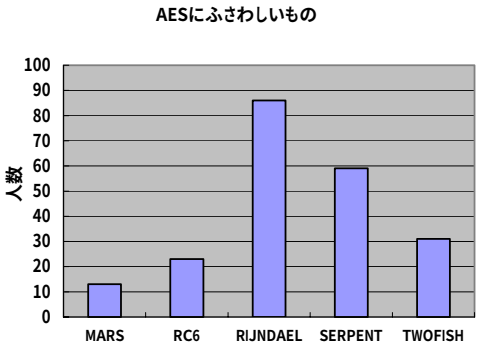
Vincent Rijmen による Rijndael 公式 Web ページ
http://www.esat.kuleuven.ac.be/~rijmen/rijndael/

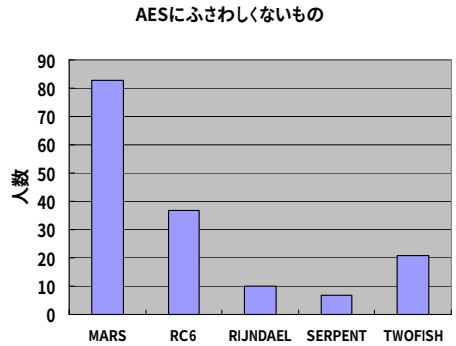
この選定につかったすべての技術的情報は Report on the Development of the Advanced Encryption Standards (AES)[AESREP2]に収められている。Rijndael はソフトウェア実装、ハードウェア実装のどちらでも暗号化・復号化の処理効率が良いバランスの取れたアルゴリズムである。安全性についても問題は発見されていない。

他のファイナリストは良い点もあるか、どこかにマイナス評価となる点を持っている。そのマイナス評価の部分をリストアップしてみると次のようになる。

アルゴリズム	マイナス評価部分
MARS	ハードウェア実装ではチップ面積が大きくなり、かつ処理速度が遅い
RC6	ハードウェア実装では処理速度が遅い・32 ビット CPU 以外では平凡な処理速度になる。
Twofish	鍵スケジュールが遅い・構造が複雑で安全性の評価が難しい
Serpent	ソフトウェア実装では処理速度が遅い
Rijndael	特に目立つ弱点はない

第三回 AES カンファレンスにてファイナリストとなった 5 つのアルゴリズムの開発者がパネラーとなり最終のプレゼンテーションを行った際、「自分の暗号以外で選ぶとしたらどのアルゴリズムを選ぶか」という質問が会場から出た。そのとき Rijndael 開発者以外はすべて Rijndael を選んだ。ちなみに Rjindael 開発者は Serpent をあげていた。このパネル終了後、参加者サーベイという形で AES にふさわしいアルゴリズムはどれかというアンケートが取られた。その結果は AES に一番ふさわしいと思われるアルゴリズムは Rijndael が最も多かった。





AES (Rijndael)の構造

付属資料 “Specification for the ADVANCE ENCRYPTION STANDARD (AES)”を参照のこと

今後の展開

AES を決めるまでのプロセスは、ガラス張りのオープンプロセスだったといえる。DES の時のような不透明なプロセスはない。約 3 年近く、世界中の暗号学者から徹底的に調べられた上で、十分に安全であり、かつ、処理効率も良いということが明らかになっている。AES(Rijndael)は、現在 FIPS 化のためのプロセス途中であるが、正式に FIPS となった後

は FIPS という規格という枠組みを越えて *de facto* スタンダードの暗号アルゴリズムとして利用されていくだろう。また技術的な面よりも、米国の次世代標準化暗号がヨーロッパ生まれという事実が *de facto* となるのに心理的にプラスに働くように思われる。ただし Rijndael 自体は AES 以外への標準化作業への応募は行っていない。そのため、今後の Rijndael の広がり方は基本的に AES として FIPS 化されるように、AES から ANSI 化、ISO 化、IETF RFC 化の道をたどるものと思われる。

参考文献

[MORRIS78] R. Morris, “The Data Encryption Standard – Retrospective and Prospects”, IEEE Communication Magazine, volume 16, number 6, Nov 1978, pp. 11-14.

アカデミック分野で最初に DES を評価した論文。

[COPPERSMITH 2000] D. Coppersmith, “The development of DES”, invited talk, CRYPTO 2000, Aug 2000.

http://www-cse.ucsd.edu/users/mihir/crypto2k/program.html

IBM での DES 開発に参加していた Coppersmith からみた当時の状況を語る。

[BIHAM90] E. Biham and A. Shamir, “Differntial cryptanalysis of DES like cryptosystems”, Advances in Cryptology --- Crypto '90 Proceedings, SpringerVerlag, Aug 1990, pp 2---21.

Differential Attack の論文。DES 自体は解読できなかったが FEAL など DES に似た構造をもった暗号には非常に有効であった。

[BIHAM93] E. Biham, “New Types of Cryptanalytic Attacks Using Related Keys”, Advances in Cryptology --- Eurocrypt '93 Proceedings, SpringerVerlag, 1993, pp.398---409.

Related Keys Attack の論文。鍵スケジュールに着目して攻撃を行う。この論文では Differential Attack には耐性を持つ LOKI91 の解読に成功している。

[DIFFIE77] W. Diffie and M. E. Hellman, “Exhaustive cryptanalysis of the NBS Data Encryption Standard”, Computer, Oct 1977, pp. 74---84.

DES の Exhaustive Attack のコストに関する有名な論文。

[COPPERSMITH94] D. Coppersmith, “The Data Encryption Standard (DES) and its strength against attacks”, IBM Journal of Research and Development, 38, 1994, pp 243---250.

DES が設計された時点で Differential Attack を既に考慮に入れていたことを述べている論文。Liner Attack で DES が解読されるまで、その事実は一切明かされていなかった。

[MATSUI93] M. Matsui, “Liner Cryptanalysis Method for DES Cipher”, Advances in Cryptology --- Eurocrypt '93 Proceedings, 1993, pp. 386---397.

Liner Attack の論文。Liner Attack によりはじめて DES が解読可能となる。ただし、この論文ではまだフルラウンドの DES の解読には成功できていない。

[MATSUI94] M. Matsui, “The First Experimental Cryptanalysis of the Data Encryption Standard”, Advances in Cryptology --- CRYPTO '94 Proceedings, 1994, pp. 1---11.

初めてフルラウンドの DES の解読に成功したことを示した論文。

[SIMOYAMA98] T. Shimoyama and T. Kaneko, “Quadratic Relation of S-box and Its Application to the Linear Attack of Full Round DES”, Advances in Cryptology --- CRYPTO '98 Proceedings, 1998, pp. 200---211.

Liner Attack を改良しさらに高速に DES を解読する方法の論文。DES 解読する暗号分析理論では、この方法が最速である。

[DISTRIBUTED99] http://www.distributed.net/des/

インターネットで接続されている大量の PC などを同時に使い DES の Exhaustive Attack を行う。

[DESCHAL99] http://www.rsasecurity.com/rsalabs/des3/

RSA 社が主催した DES を解読するコンクール。

[EFF98] the Electronic Frontier Foundation, “Cracking DES: Secrets of Encrytion Research, Wiretap Politics, and Chip Design”, O'Reilly, 1998.

http://www.eff.org/descracker.html

非営利団体 EFF (Electronic Frontier Foundation)は DES の鍵空間を探索する専用チップを大量に装備した DES Cracker を作り、DES の 56 ビットの鍵空間では安全ではないということを示した。その DES Cracker の公式ページ。

[RFC2828] R. Shirey, “Internet Security Glossary”, RFC2828, 2000.

インターネット上で使われる各種技術の用語解説の RFC。ここで現れる用語（暗号アルゴリズムの種類）は、インターネット上で広く認知されていると考えられる。

[NIST97] NIST の旧 AES ページ

http://csrc.nist.gov/encryption/aes/index2.html

[NIST01] NIST の現在の AES ページ

http://csrc.nist.gov/encryption/aes/

[RJINDAEL01] NIST が用意する Rjindael の情報ページ

http://csrc.nist.gov/encryption/aes/rijndael/

[RIJMEN01] Vincent Rijmen による Rijndael 公式 Web ページ

http://www.esat.kuleuven.ac.be/~rijmen/rijndael/

[Savad01] J. Savad, “The Advanced Encryption Standard (Rijndael)”, Savad による Rijndael の技術解説

http://home.ecn.ab.ca/~jsavard/crypto/co040801.htm

[AESQA] NIST, “ADVANCED ENCRYPTION STANDARD (AES) Questions and Answers”, 2001.

NIST が公開している AES に関する Q & A 集。

[NISTREP1] NIST, “STATUS REPORT ON THE FIRST ROUND OF THE DEVELOPMENT OF THE ADVANCED ENCRYPTION STANDARD”, 1999.

AES 選出プロセスのラウンド 1 終了時に公開された、ラウンド 1 の評価レポート。

[NISTREP1+] NIST, “addenda for STATUS REPORT ON THE FIRST ROUND OF THE DEVELOPMENT OF THE ADVANCED ENCRYPTION STANDARD”, Aug 1999.

AES 選出プロセスのラウンド 1 の評価レポートに対しての修正文章。NTT の提出した E2 に対する評価に誤りがあったので、その修正を行った文章。

[NISTREP2] NIST, “STATUS REPORT ON THE FIRST ROUND OF THE DEVELOPMENT OF THE ADVANCED ENCRYPTION STANDARD”, Oct 2000.

AES 選出プロセスのラウンド 2 終了時に公開された、ラウンド 2 の評価レポート。

[SMID99] M. Smid, “From DES to AES: Twenty years of U.S. Government Initiatives in Cryptography”, SAC '99, 1999.

NIST の M. Smid が SAC'99 で使ったプレゼンテーション資料

[AESCONF1] 第 1 回 AES カンファレンス(カリフォルニア)

http://csrc.nist.gov/encryption/aes/round1/conf1/aes1conf.htm

第一回 AES カンファレンスの公式ページ。カンファレンスで使用した各種論文などが入手できる。

[AESCONF2] 第 2 回 AES カンファレンス(ローマ)

http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm

第 2 回 AES カンファレンスの公式ページ。カンファレンスで使用した各種論文などが入手できる。

[AESCONF3] 第 3 回 AES カンファレンス(ニューヨーク)

http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm

第 2 回 AES カンファレンスの公式ページ。カンファレンスで使用した各種論文などが入手できる。

[SUZUKI00] 鈴木裕信, “3rd AES カンファレンスから”, 2000 年 7 月 SEA FORUM プレゼンテーション資料, July 2000.

http://h2np.net/hironobu/docs/AESSea2000July3.files/v3_document.htm

第 3 回 AES カンファレンス参加のレポート。

[ここまで]