MUGI暗号評価の現状報告
(スクリーニング評価)

平成14年1月28日

共通鍵暗号評価小委員会
委員　櫻井　幸一

A. スクリーニング評価結果の要点

(1) (一部の)Test Vectorが検証の結果
不一致。

(2)自己評価書における平成12年度詳細
評価対象暗号に対する特長が不十分。

B. 詳細評価のための要確認・検討事項

（１）Test Vectorの不一致の理由は何か？

Technical か Editorial かの確認。

（２）ストリーム暗号としての平成12年度の詳細評価対象(MULTI-S01及びTOYOCRYPT-HS1)に対する特長、とくに内部で乱数生成アルゴリズムPANAMAを使っていることから、MULTI-S01との比較・優位性、差別化の検討。

C.各評価者の総合コメント

（そのまま抜粋）

評価者1: 総合評価コメント

詳細評価を実施し、安全性の評価を行なうべきと判断します。

(1)平成12年度詳細評価対象暗号に対する特長について

- 提案者(会社)が同じである"MULTI-S01"は、本提案と同じくPANAMAを利用したストリーム暗号ですので、それとの比較(差別化)は必要です。
- また、ブロック暗号の段関数に相当する関数を利用していることから、ブロック暗号との性能(速度)比較も必要です。
- AESと同程度とは記述されていますが、数値比較は行なわれていません。

(2)想定するアプリケーション

明記されていませんが、秘匿に関するほとんどの用途に適用可能と考えられます。

評価者1: 暗号技術仕様書に対するコメント

本仕様書には、第3者が実装するための情報はきちんと記述されていました。以下、コメントです。

(1) 設計基準

設計に関する定量的な基礎数値は「秘密鍵が128ビット」とある以外は、記述されていませんでした。

(2) 複数鍵長のサポート

暗号化の際の入力は、平文、秘密鍵(128ビット)、初期ベクトル(128ビットの公開パラメータ)のみです。従って、本方式は128ビット固定長の方式です。

(3) 平成12年度詳細評価対象暗号に対する特長

本提案は、ストリーム暗号としての提案ですが、平成12年度の詳細評価対象(MULTI-S01及びTOYOCRYPT-HS1)に対する特長は記述されていません。

また、暗号方式としては、バーナム暗号に分類されますので、TOYOCRYPT-HS1に近いのですが、内部でPANAMAを使っていることから、むしろ、MULTI-S01との比較・優位性、差別化の記述が必要です。

評価者1: 自己評価書に対するコメント(1)

(1) 安全性の評価について

提案方式の安全性は、擬似乱数生成器の出来に依存しますが、部品として共通鍵暗号の技術を積極的に使用しています。

従って、詳細評価では、共通鍵暗号の解析という立場からの評価も必要です。

一方、擬似乱数生成器の(統計的)乱数性評価に関しても、より詳細な評価(NISTの評価法 "Random Number Generation and Testing" (http://csrc.ncsl.nist.gov/rng/)も検討すべきです。

(2) 第3者による評価実績、使用実績

提案方式の第3者による評価実績、使用実績は自己評価書に記載されていません。

(3) 平成12年度詳細評価対象暗号に対する特長

記述されていません。仕様書に関する総合評価コメントと同じですが、内部方式が似ているMULTI-S01との性能比較は必要です。

評価者1: 自己評価書に対するコメント(2)

記述が不明な点について

(1) 16ページの証明について

Case2(2段繰り返し表現)の最後に、a_2=f^{-1}(a_2 + C_a, 0) + C_b という記述があります。

それは、その式から5行上の式 a_2=F^{-1}(β , 0) +C_1 + F(a_1, 0) からの式変形と思われますが、もしそうなら、式変形が不適切です。式を整理すると、β =a_2+C_a （C_aはa1依存の定数)とみなせますが、β は″a_2″及び″a1依存の定数″の2つを入力とする非線形変換であることに矛盾します。

しかし、Case2における本来の主張「上記条件を満たすa2は平均一つ存在する」は、妥当な主張と思われます。

(2) 3.5.3節の主張について

バッファ間の簡単な線形和関係の例のみが記述してあります。

恐らく、著者らは「初期攪拌完了後は、これらの関係も消える」ということを主張したいと思いますが、その主張が記述されていません。

評価者2: 総合評価コメント

仕様は実装可能なレベルで記述されている。

また、設計方針などについても明確に記述されている。

安全性評価については、一般的な攻撃法から、構造特有の攻撃まで、様々な観点から行われており、統計的評価もFIPS１４０－１をカスタマイズして行われている。

実装性評価については、ソフトウェアハードウェア共に、妥当な検討がされており、処理速度や、リソース量、ハード規模などについても妥当な値であると考えられる。

ただし、仕様書についてはタイプミスと思われる記述の抜けや誤りがいくつか見られる。

また、当方の計算機環境でリファレンスコードを実行したところ、仕様書に記載されているテストベクトルの一つについて、出力値が一致しなかった。

平成１２年度詳細評価対象暗号に対する特長については応募書類に明確な記述がない。

平成１２年度詳細評価対象暗号MULTI－S01もPANAMAの構造を採用しているが、本技術では内部にAESの関数を使用している点が特長であると思われる。

評価者2: 暗号技術仕様書に対するコメント

設計方針や、元にしている技術について明確に記載されている。

仕様書については、所々でタイプミスと思われる記述の抜けや誤りがあった（例えば4ページ最終行や、１１ページ１１行目あたりなど）。

しかし、仕様そのものは特定可能であり、実装は可能であると考えられる。

また、当方の計算機環境(UltraSPARCII-Solaris8及び、PentiumIII-WindowsNT4.0)でリファレンスコードをコンパイルし、実行してみたところ、仕様書に記載のあるテストベクトルの２つと、リファレンスコードのテストベクトル１５個について、仕様書の一つ目のベクトル、及び、リファレンスコードのテストベクトル１５個は、同じものが出力された。

しかし、仕様書の二つ目のテストベクトルについては、仕様書と異なるものが出力された。出力されたベクトルを資料1に添付する。

評価者2: 自己評価書に対するコメント(1)

全体的に見て、安全性については様々な攻撃が詳しく自己評価され、
実装性についても妥当なレベルで記述されていると考えられる。
安全性評価については、統計的評価としてFIPS１４０－１の検定を長い平文長に対応するようにカスタマイズし、頻度テスト及び、連（0または1が連続している部分）のテストを行っている。
このようなFIPS１４０－１タイプの統計的評価を行うことは検討項目として妥当であると考えられる。
それ以外の攻撃についても詳細に評価されており、検討項目、及び攻撃内容について妥当であるように思われるが、専門外であるため正確には判断できない。
ただし、周期についてOFBと同等以上であるという予想など、根拠が明確に示されていないものもあり、安全性評価は今後も続けていく必要があると思われる。

評価者2: 自己評価書に対するコメント(2)

実装性評価については、MUGIが内部にAES（Rijndael）の関数を保有していることから、AESからの換算で見積もることができる。

ソフトウェアについては、リファレンスコードと自己評価書で性能が記述されているコードは違うものであると考えられるが、自己評価書に記述されている処理速度はRijndaelの処理速度から換算して妥当であると考えられる。リソース量については、ワークエリアとコード量（行）についてのみ記載されており、この内ワークエリアについては妥当であると考えられる。しかしコードのメモリ使用量は行数だけからは算出不可能であるため、妥当性を判断できない。

ハードウェアについては、速度優先方式はリソース量、処理速度共にAESから換算して妥当であると考えられる。

また、小論理方式は、リソース量、処理速度共に速度優先方式から換算して妥当であると考えられる。

平成１２年度詳細評価対象暗号に対する特長については応募書類に明確な記述がない。

平成１２年度詳細評価対象暗号MULTI－S01もPANAMAの構造を採用しているが、本技術では内部にAESの関数を使用している点が特長であると思われる。

評価者3: 総合評価コメント

- 本提案方式は、ソフトウェア・ハードウェアのいずれのプラットホームにおいても高速、または軽量な実装が可能な暗号方式として提案されている。
- ストリーム暗号でありながら、64ビット長のブロック単位の処理によって長周期性と高速性の両立を図っている。
- 単にブロック単位の処理を行っているのであれば長周期性に疑問もあるが、データ攪拌部を備えていることから特に問題ないと思われる。
- ただし、その設計においては十分な注意が必要である。

評価者3: 暗号技術仕様書に対するコメント

本提案方式は、電子政府において使用されるストリーム暗号の候補として、十分な安全性と高速性を有すると考えられる。

評価者3: 自己評価書に対するコメント(1)

本提案方式における自己評価では、擬似乱数生成器の安全性を示す要件として次の２つを挙げている。

(1)出力される系列が十分な乱数性を持つこと

(2)異なる初期値を与えた場合に出力される系列が大きく変化すること

評価者3: 自己評価書に対するコメント(2)

要件(1)に対する評価として、まず頻度テストと連テストを行っている。

頻度テストでは系列長222, 226, 230の乱数列を512組生成して、1ビット、2ビット、4ビット、8ビットの検定を行っている。また、系列長222では、連の検定も行っている。

それ以外の従来の理論的な乱数系列評価法として、系列周期、線形複雑度、分轄統治攻撃について触れている。ここで、F関数の設計、つまりS-boxと行列Mの設計には留意したいところである。

そこで、著者らはF関数の差分・線形特性、線形解読法の適用等についても調べている。

評価者3: 自己評価書に対するコメント(3)

要件(2)について、秘密鍵を固定して初期ベクトルの変化に対する出力の変動をρ関数の差分・線形パスと再同期攻撃について検討している。また、初期ベクトルを固定して、鍵を変化させたときの出力の変動を調べるために、バッファの攪拌性能、Square攻撃、バッファの相関等について検討されている。

今回の自己評価では、F関数のS-boxと行列MはAESで使用されたものであるが、本提案方式を多用するためにはS-boxと行列Mの設計法について検討する必要があると考える。

評価者4: 総合評価コメント

- PANAMAの改良を行っている点は理解できるが、安全性等の議論において、詳細評価の必要あり
- SW、HW実装においてもPANAMAとの比較データが欠如している。この点も詳細評価で検討すべき

評価者4: 暗号技術仕様書に対するコメント

仕様記述として問題ないが、設計方針・設計基準は安全性と密接に関係しており、この内容の妥当性と信頼を詳細評価する必要あり。

評価者4: 自己評価書に対するコメント

- 安全性等の議論において、詳細評価の必要あり
- 学会でも定着していない理論でもあり、攻撃可能性が十分議論されているとは思えない

★自己評価書における不明点、飛躍点

『困難である』・『不可能と思われる』等は、飛躍している。
（別紙２）に転載

- 上記抜粋の真偽性を詳細評価で検討する必要あり
- SW、HW実装においてもPAMANA, AES等との比較データが欠如しており、この点も詳細評価で検討すべき

別紙2

分割統治攻撃
(divide-and-conquer attack)

分割統治攻撃に分類される攻撃法は、内部状態の一部を推定する攻撃であり、あるラウンドにおける推定から、任意のラウンドの内部状態(一部) が記述できる場合に適用可能である。

しかし、PKSG では一般に内部状態が大きく、また、状態遷移関数を分割して、内部状態の一部のみを記述することができない。このような理由から、MUGI に対して分割統治攻撃を適用することは困難であると考える。

その他の攻撃法

別紙2

ブロック暗号に対するその他の攻撃法、例えば、差分解読法[BS93]、高階差分攻撃[Ku94]、補間攻撃[JK97] などは、いずれも選択平文攻撃である。これらの攻撃法を(乱数性の評価手法として) PKSG に適用することは困難であると考えられる。これは、ブロック暗号の場合と異なり、攻撃者は任意の出力列を得ることができないからである。したがって、乱数列に対する攻撃は既知平文攻撃のみを考えればよい。

また、任意の選択平文攻撃において、出力列から攻撃に必要な選択平文を取り出すことは計算量的に困難である。例えば、16 ラウンドの出力列から何らかのdistinguisher を構成できた場合、出力列の成す空間の元の数は$2^{64} \times 16$ であり、求める選択平文1 組を得るためには$2^{64} \times 8$ 程度の既知平文が必要である。

さらに、差分解読法を例にとって考える。差分解読法で、3.3.2 と同様に差分パスを探索する場合、まず、攻撃者はあるラウンドにおける内部状態の差分を自由に観測できる必要がある。これは、初期化が十分に行われている場合には不可能であり、したがって、差分解読法の適用は困難であると考えられる。

別紙2

線形バッファの（不）可能性

これらの非常に限定される鍵についても、さらにIV を伴った非線形な攪拌がバッファ全体に渡って行われることから、結果として、鍵セットアップでは、バッファを十分ランダムに攪拌すると結論付けられる。

別紙2

Square 攻撃

ストリーム暗号では、攻撃者は鍵か初期値のどちらかに差分を入れなければならない。

よってストリーム暗号へのSquare 攻撃の適用には、関連鍵攻撃か、選択初期値攻撃のみが考えうる。