暗号アルゴリズムの詳細評価

報告書

疑似乱数生成

PANAMA(MULTI-S01 **内部)編**

1. 概要

本評価報告書では、MULTI-S01 で使用される疑似乱数生成モジュール PANAMA の評価を行いました。MULTI-S01 からの PANAMA の利用方法にのみターゲットを絞って評価を行っています。

テスト項目の概要と、テスト結果の概要を示します。

テストの結果、基準を満たさなかったものは 0/1 等頻度性テストのみ（しかも、1 事例のみ）であり、評価者は提案方式(PANAMA、MULTI-S01 からの利用の場合のみ)を合格と判断します。

1.1. 統計的性質に関する評価について

テストデータを生成し、下記のテスト項目に対するテストプログラムを作成後、評価を行いました。テストデータは特殊なデータの生成とランダムサンプリングを併用しました。

もちろん、当該項目に対するテストに合格したとしても、その項目に対する安全性を保障（証明）するものではありません。

1.1.1. 0/1 等頻度性テスト

提案方式は、本テストに合格しませんでした。詳細は、別冊（疑似乱数生成の評価　0/1 等頻度性テスト PANAMA(MULTI-S01)編）を参照してください。約 40 万件のテスト結果のうち、1 件だけ基準を満たしませんでした。2 章も参照してください。

1.1.2. 連性テスト

提案方式は、本テストに合格したと判断します。詳細は、別冊（疑似乱数生成の評価　連性テスト PANAMA(MULTI-S01)編）を参照してください。

1.1.3. 長周期連性テスト

提案方式は、本テストに合格したと判断します。詳細は、別冊（疑似乱数生成の評価　長周期連性テスト PANAMA(MULTI-S01)編）を参照してください。

1.1.4. 一様性テスト

提案方式は、本テストに合格したと判断します。詳細は、別冊（疑似乱数生成の評価　一様性テスト PANAMA(MULTI-S01)編）を参照してください。

1.1.5. Avalanche 性テスト

提案方式は、本テストに合格したと判断します。詳細は、別冊（疑似乱数生成の評価　Avalanche 性テスト PANAMA(MULTI-S01)編）を参照してください。

1.1.6. 線形複雑度テスト

提案方式は、本テストに合格したと判断します。詳細は、別冊（疑似乱数生成の評価　線形複雑度テスト PANAMA(MULTI-S01)編）を参照してください。

1.2. 用途に対する適合性

次の各項目について、机上もしくはマシンテストにより評価を行いました。

1.2.1. 推測可能性評価について

入力の一部が露呈したとき、その入力に対する出力系列の推定が可能であるかは、 Avalanche テストによりある程度の評価が可能です。更に机上考察の結果を合わせ、提案方式は本テストに合格したと判断します。詳細は 3 章を参照してください。

1.2.2. 周期(出力系列の再現性)の評価について

同一鍵を使用した場合、周期が設計値より小さくなることはないか、机上考察行い、提案方式は本テストに合格したと判断します。詳細は、3 章を参照してください。

1.2.3. 同等出力系列発生条件の評価について

異なる鍵を使用して、同等（まったく同一ではない）出力系列が発生する条件があるか机上考察を行い、提案方式は、本テストに合格したと判断します。詳細は、3 章を参照してください。

1.3. 出力系列に対する入力空間の大きさについて

入力空間について机上考察を行い、提案方式は、本テストに合格したと判断します。詳細は、4 章を参照してください。

1.4. ユーザの立場からの評価について

仕様書を用いて実装する状況を想定して、評価を行いました。詳細は、5 章を参照してください。

1.5. 暗号解析の立場からの評価について

統計的性質を利用するのではなく、アルゴリズム構造から、解析を行う状況を想定して、評価を行いました。詳細は、6 章を参照してください。

1.6. ドキュメントについて

ドキュメントの内容について、評価を行いました。詳細は、7 章を参照してください。

1.7. その他

最近 NIST が乱数に関する更に詳細な評価基準を公開しました。 http://csrc.nist.gov/rng/ に詳細が記載されていますが、今回行った評価(0/1 等頻度性、一様性、連性など)以外にも、評価項目が増えています。

今回はスケジュールの都合で間に合いませんでしたが、今後、疑似乱数生成に関する評価は、この基準に従って行うべきと考えます。

2. 統計的性質に関する評価について

統計的性質では、唯一 0/1 等頻度性テストのみ合格しませんでした。詳細は、別冊（疑似乱数生成の評価 0/1 等頻度性テスト PANAMA(MULTI-S01)編）を参照してください。約 40 万件のテスト結果のうち、1 件だけ FIPS140 の基準を満たしませんでした。

しかし、他の統計的性質に関するテストにおいて合格していること、0/1 等頻度性テストについても、不合格なものはわずか 1 件のみであることを考慮すると、この件のみで疑似乱数として不合格とは即断できません。

3. 用途に対する適合性について

本章では用途に関する評価を行いました。

3.1. 推測可能性評価

入力の一部が露呈した場合，出力系列の推定可能性の評価について考察しました。PANAMA(MULTI-S01)は、次の 2 つの値を鍵とします。

鍵	サイズ	用途
秘密鍵	256bit	PANAMA の最初の Push モードで使用
乱数列番号	256bit	PANAMA の 2 回目の Push モードで使用 巨大なデータを扱う場合に、ブロック毎に切り替え

特に乱数列番号は秘密である必要はないと記載されていますので、「256bit の秘密鍵」を切り替えることによって疑似乱数性を保てるかどうかが問題となります。

入力の一部が露呈した場合の出力系列の推定可能性を数値で評価するのは困難ですが、Avalanche テストに合格することは、本テストに合格するための必要条件と考えます。

Avalanche テストに関する詳細は別冊（疑似乱数生成の評価 Avalanche 性テスト PANAMA(MULTI-S01)編）を参照してください。提案方式は Avalanche テストに合格しています。これは、「入力の一部がわかっても、出力結果に関する情報を得ることができない」ことを示唆しています。もちろん十分条件ではないことに注意してください。

3.2. 周期（出力系列の再現性）の評価

同一鍵を使用した場合、同一の出力系列が設計周期より小さい周期で発生しないか評価しました。MULTI としての用途では、2^{32} ブロック(1 ブロックは 64 ビット)毎に乱数列番号を切り替えて使用します。つまり、周期は(ブロックを単位として) 2^{32} 以上であることが求められます。 しかし、実際に周期に達するまで乱数を生成させるのは困難であるため、机上で考察しました。

PANAMA は 32 段の変形フィードバックシフトレジスタを内蔵しており、各段は 8word(256bit)から構成されています。従って、周期は 2^{32} 以上であると判断しました。

3.3. 同等出力系列発生条件の評価

本節では、異なる鍵を使って同等の出力系列を発生させる方法が可能かどうか考察しました。

秘密鍵 C と乱数列番号 Q から生成される乱数列に、簡単な変換（四則演算、論理演算など）を施したものが、別の秘密鍵 C'と乱数列番号 Q'から生成されないか机上で検討し、そのような C'と Q'は（存在するかも知れないが）容易に求められないと判断しました。

4. 出力系列に対する入力空間の大きさ

4.1. 入力空間評価

PANAMA モジュールに対する鍵の制限はなく、鍵空間は（乱数列番号を公開したとしても）2^{256} と評価できます。これは、MULTI-S01 の規定する鍵空間サイズと同一であり、充分大きな鍵空間であると考えます。

5. ユーザサイドからの評価

仕様書を用いて実装する状況を想定して、問題点がないか考察しましたが、問題点はありませんでした。

6. 暗号解析の立場からの評価

本章では、提案アルゴリズムを(アルゴリズムの逆演算を行う立場から)解析する場合の弱点などについて考察しました。しかし、自己評価書に記載されたものを含めて脅威となる攻撃は発見できませんでした。また、自己評価書に記載されている攻撃に関する評価も妥当と考えます。

7. ドキュメントについて

「暗号アルゴリズムの詳細評価報告書　ストリーム暗号　MULTI-S01 編」を参照ください。