暗号アルゴリズムの詳細評価

報告書

ストリーム暗号

TOYOCRYPT-HS1 **編**

1. 概要

テスト項目の概要と、テスト結果の概要を示します。

提案方式(TOYOCRYPT-HS1)は、ベースとなる疑似乱数生成器(TOYOCRYPT-HR1)の安全性が、安全性の根拠となります。しかし、TOYOCRYPT-HR1 は、統計的性質に関する評価、及び同等出力系列発生条件の評価を合格できないため、評価者は提案方式(TOYOCRYPT-HS1)を不合格と判断します。

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。テストデータはサンプリングを行って生成しました。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。

また、提案方式は疑似乱数生成装置 TOYOCRYPT-HR1 の出力と平文との排他的論理和を暗号文とする乱数加算型のストリーム暗号方式です。従って、下記に述べる統計的性質に関する評価は、相互情報量テストを除き、TOYOCRYPT-HR1 のテスト結果を適用可能です。

1.1.1. 0/1 等頻度性テスト

提案方式は、本テストを合格したと判断します。詳細は、別冊（疑似乱数生成の評価　0/1 等頻度性テスト TOYOCRYPT-HR1 編）を参照してください。

1.1.2. 連性テスト

提案方式は、本テストを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 TOYOCRYPT-HR1 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、本テストに合格しませんでした。詳細は、別冊（疑似乱数生成の評価　長周期連性テスト TOYOCRYPT-HR1 編）を参照してください。

1.1.4. 一様性テスト

提案方式は、本テストを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 TOYOCRYPT-HR1 編）を参照してください。

1.1.5. 線形複雑度テスト

提案方式は、本テストを合格しませんでした。詳細は、別冊（疑似乱数生成の評価　線形複雑度テスト TOYOCRYPT-HR1 編）を参照してください。

1.1.6. 相互情報量テスト

提案方式は、本テストを合格したと判断します。詳細は、別冊（ストリーム暗号の評価　相互情報量テスト TOYOCRYPT-HS1 編）を参照してください。なお、理論面からの考察については 2 章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. 周期（出力系列の再現性）について

提案方式は、本テストを合格したと判断します。詳細は、「暗号アルゴリズムの詳細評価報告書　疑似乱数生成 TOYOCRYPT-HR1 編」を参照してください。

1.2.2. 同等出力系列発生条件の評価について

提案方式は、本テストを合格しませんでした。詳細は、「暗号アルゴリズムの詳細評価報告書　疑似乱数生成 TOYOCRYPT-HR1 編」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

本評価については「暗号アルゴリズムの詳細評価報告書　疑似乱数生成　TOYOCRYPT-HR1　編」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

本評価については「暗号アルゴリズムの詳細評価報告書　疑似乱数生成　TOYOCRYPT-HR1　編」を参照してください。なお、ストリーム暗号として重要なバイトオーダーの問題について、3 章でコメントします。

1.5. 暗号解析の立場からの評価について

本評価については「暗号アルゴリズムの詳細評価報告書　疑似乱数生成　TOYOCRYPT-HR1　編」を参照してください。

1.6. ドキュメントについて

ドキュメントに関する誤植、ドキュメントの内容について、評価を行いました。4 章を参照してください。

1.7. 性能について

本暗号方式は、疑似乱数生成器 TOYOCRYPT-HR1 の出力と平文との排他的論理和をとる方式です。性能については「暗号アルゴリズムの詳細評価報告書　疑似乱数生成　TOYOCRYPT-HR1 編」を参照してください。

2. 統計的性質に関する評価について

提案方式は疑似乱数生成装置 TOYOCRYPT-HR1 の出力と平文との排他的論理和を暗号文とする乱数加算型のストリーム暗号方式です。従って、相互情報量テストを除き、TOYOCRYPT-HR1 のテスト結果を適用可能です。

本章では、相互情報量テストに関するコメントを示します。

2.1. 相互情報量に関する評価について

相互情報量は I(M;C)=H(M)-H(M|C)で定義されます。乱数加算型の場合、C=M⊕K ですから、

$$I(M;C)=H(M)-H(M|C)=H(M)-H(C\oplus K|C)=H(M)-H(K)$$

となり、H(K)=H(M)なら

上記式=0

となります。また、乱数加算でなくても M=D(K,C)という復号において、C を固定したときの K の分布と D(K,C)の分布が同じならば、同一の結論が得られます。提案方式は乱数加算型なので、乱数が真性乱数なら完全暗号になり、相互情報量は I(M;C)=0 となります。

しかし、実際は擬似乱数なので情報理論的には

$$I(M;C)=H(M)-H(K)=H(M)-128bit-120bit=H(M)-248bit$$

となります。ここで、128 次原始多項式の個数は $\frac{6(2^{128}-1)}{\pi^2}\times\frac{1}{128}\approx 2^{120}$ と見積もりました。相互情報量がどのような値になるかは、乱数が如何に真性乱数に近いかにかかっています。

別冊（ストリーム暗号の評価 相互情報量テスト TOYOCRYPT-HS1 編）に示したようにシミュレーションによるマシンテストに対しては本テストは合格しましたが、このテストは相互情報量をビット（単位は 1～3 ビット）単位の遷移として評価したものに過ぎません。

基本方式である TOYOCRYPT-HR1 の疑似乱数性に問題があるため、相互情報量は理論値(H(M)-248bit)にはならないと思われます。

3. ユーザサイドからの評価

本項目については「暗号アルゴリズムの詳細評価報告書 疑似乱数生成 TOYOCRYPT-HR1 編」を参照してください。ストリーム暗号独特の問題として、「バイトオーダーの問題」があります。本章では、この問題について記述します。

3.1. バイトオーダーの問題について

評価者が出力された乱数系列をファイルに出力する際に、困ったことを報告します。 Intel の CPU では Little-Endian のバイトオーダーを採用しています。例えば、乱数列を生成(unsigned int 型配列)して、それを char 型配列として扱う場合に注意が必要で、不用意に memcpy 関数でコピーするとよく発生する問題です（バイトオーダーによって処理を変更しなくてはならない)。評価のために頂いたテストプログラムは 4 バイトごとに乱数列を返す仕様になっていましたが、ストリーム暗号生成アルゴリズムという位置付け上、 char 型配列の引数に値を戻すようにしたほうが、テストプログラムとしては使い勝手がよいです。提案方式はハードウェア実装を念頭に開発されていますが、ソフトウェア実装が皆無とは思えないからです。

4. ドキュメントについて

「暗号技術仕様書 TOYOCRYPT-HR1」と同様の問題があります。

4.1. 仕様書の内容の確認

(1) 「暗号技術仕様書 TOYOCRYPT-HS1」の下記の記述は正しいでしょうか。ご確認願います。

#	内容
1	4.1 CLK 関数の記述について $x_{i+1} = c_i x_{127}(t), (0 \le i \le 126)$ には、排他的論理和に関する項がありません。図 7(P.10)と違います。誤植ではありませんか。