暗号アルゴリズムの詳細評価

1. 評価対象暗号アルゴリズム

項番	暗号アルゴリズム	分類	暗号アルゴリズムの応募元
1	MULTI-S01	ストリーム暗号	株式会社日立製作所

2. 評価項目

- 周期、線形複雑度、相互情報量
- 統計的性質（1/0 等頻度性、連、一様性）

3. 評価方法及び評価結果

評価対象暗号アルゴリズムに対して、上記 6 項目の評価を行なった。その際に共通な測定条件を次に示す。

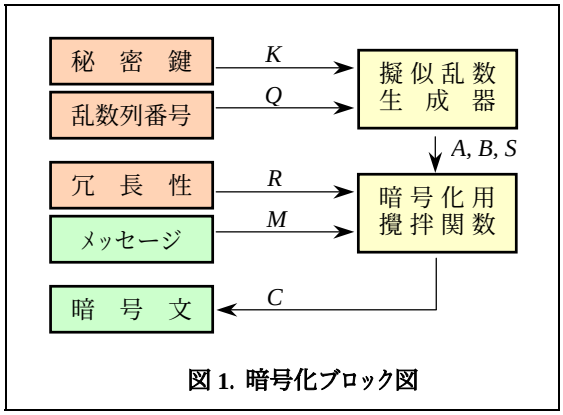

図 1. 暗号化ブロック図

測定条件と測定項目：

MULTI-S01 暗号はストリーム暗号であり、図 1 に示される手順で暗号化される。したがって、擬似乱数生成器からの出力系列の乱数性と、メッセージ系列 *M* と冗長性 *R* を既知とした場合、つまりそれぞれの値を零としたときの暗号用攪拌関数の入出力における相関について評価を行なった。

擬似乱数生成器からの出力系列の乱数性：

・周期 ・線形複雑度 ・相関値 ・1/0 等頻度性 ・連 ・一様性

暗号用攪拌関数の入出力における相関性：

・擬似乱数生成器からの入力と暗号文としての出力との相関

・メッセージ系列と暗号文としての出力との相関

擬似乱数生成器の入力と対象とするメッセージのサイズ：

MULTI-S01 暗号の擬似乱数生成器への入力は秘密鍵 *K* (256 ビット)と乱数列番号 *Q* (256 ビット)であるので、擬似乱数生成器の乱数性評価は、まず *K* と *Q* を零とした評価データを取り、次に *K* と *Q* のそれぞれに一様乱数を用いて 100 回の試行を行なった。また、暗号対象のメッセージの長さを考慮して最大値を 10M として、他に 1K，10K，100K，1M の長さで評価データを取っている。

K と *Q* を零とした評価データは、添付 Excel データの最上段 0 行（黄色）で与える。その下の段 1～100 行を一様乱数を用いた 100 回の試行による評価データとする。ただし、連と周期の評価データは除く。

単位と擬似乱数生成器のレジスタの規格:

評価を与える前に、仕様書中で定義される共通の単位を示す。

1 ワード ＝ 32 ビット　　1 ステージ ＝ 8 ワード ＝ 256 ビット

①. 周期

擬似乱数生成器から得られる乱数列の計算機シュミレーションによる周期の計測は時間的に難しい為、仕様書をもとに理論的に考察する。

擬似乱数生成器は、2 つのレジスタ

a レジスタ: 17 ワード （ワード単位）

b レジスタ: 32 ステージ （ステージ単位）

の組み合わせで構成され、pull モードと呼ばれる定常状態では図 2 に示すようにデータの受け渡しが行なわれている。したがって、この擬似乱数生成器をブロック A とブロック B の独立な構成として、それぞれの周期 N_A と N_B を求める。

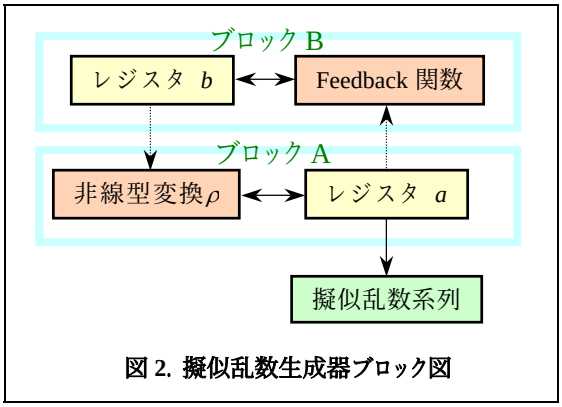

図 2. 擬似乱数生成器ブロック図

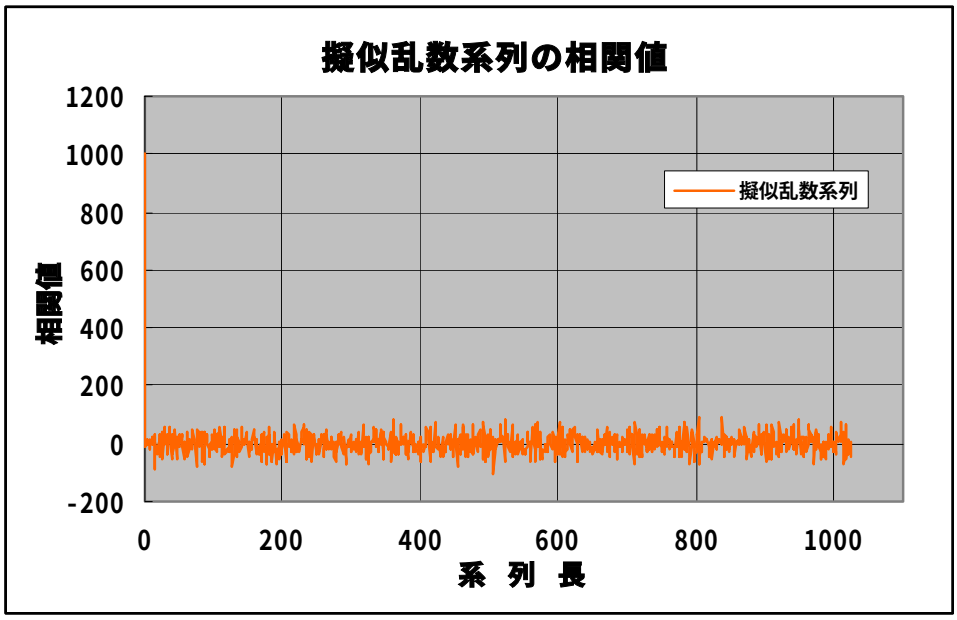

図 3. 擬似乱数系列の自己相関値

ブロック A: *a* レジスタでは、1 ワードを単位として 17 段のレジスタが構成され、非線型変換ρによってその内容が更新されている。このとき、変換ρは 4 種類の変換γ, π, θ, σの合成関数として構成されているので、*a* レジスタ以外からの入力を零と仮定し、それぞれの変換による *a* レジスタの周期 N_γ, N_π, N_θ, N_ρを求めた[参考資料(周期)]。

- 変換γ:　$\gamma(a_i) = a_i \oplus (a_{i+1 \bmod 17}$ or $(\mathrm{NOT}\ a_{i+2 \bmod 17}))$　$0 \le i \le 17$

  初期値によって、2～78812 の幅広い周期分布を持つ。

- 変換π： $\pi(a_i) = \mathrm{ROTL}_{\mathrm{i(i+1)/2\ mod\ 32}}(a_{7i\ \mathrm{mod}\ 17})$ $0 \le \mathrm{i} \le 17$

  N_π=1088 となる。
- 変換θ： $\theta(a_i) = a_i \oplus a_{i+1 \bmod 17} \oplus a_{i+4 \bmod 17}$ $0 \le \mathrm{i} \le 17$

  3～6551 まで、幅広い周期分布を持つ。(ただし、ALL-0 のときは 1)
- 変換σ： $\sigma(a_0) = a_0 \oplus 1$

  $\sigma(a_{i+1}) = a_{i+1} \oplus l_i$ $0 \le \mathrm{i} < 8$

  $\sigma(a_{i+9}) = a_i \oplus b_i^{16}$ $0 \le \mathrm{i} < 8$

  a レジスタ以外からの入力なので、無視する。

ブロック B： b レジスタは、1 ステージを単位としたレジスタで構成され、フィードバック値のシフト･ローテーションで長周期化を行なっている。このとき、シフト･ローテーションを除く部分のフィードバック関数は次式となり、長周期の擬似乱数生成する。

$$x^{32} + x^{25} + 1 = (x^2 + x + 1)(x^{30} + x^{29} + x^{27} + x^{26} + x^{24} + x^{22} + x^{21} + x^{19} + x^{18} + x^{16} + x^{15} + x^{13} + x^{12} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^2 + x + 1)$$

また、シフト･ローテーションの周期は 4 である。

以上、複数の関数の組み合わせで生成されるため、擬似乱数の周期については非常に予測し難い。また、数千回の自己相関評価では、周期 2^{20} よりも小さな相関は確認されていない。

②. 線形複雑度

線形複雑度は、擬似乱数系列の予測し難さ･解読し難さの評価尺度であるが、その値だけでは評価として不十分である。したがって、ここでは周期に対する線形複雑度の他に Profile についても測定を行なった。Profile による評価は、線形複雑度の増加の回数として評価している。ここで、線形複雑度は、解読し難さの面から、系列長に対して 1/4 の割合で増加することが望ましいとされている。

評価結果については、参考資料(線形複雑度)に示す。評価は、

Length： 生成された系列長

LC： 長さ Length の擬似乱数系列の線形複雑度（系列長を 1 として規格化した値）

No. of Steps： 長さ Length の擬似乱数系列 Profile で、線形複雑度が増加した回数（系列長を 1 として規格化した値）

として示す（Profile の様子を図 4 に示す）。

LC および No. of Steps の評価結果より、Multi-S01 で用いられる擬似乱数生成器は、線形複雑度の評価において理想的な結果が得られた。今回、時間的制約もあり、M バイト単位のメッセージに対する擬似乱数生成器評価は行なってないが、周期が M バイトを超えることを考慮すると、M バイト単位の線形複雑度による評価が極端に悪くなることは予想し難い。

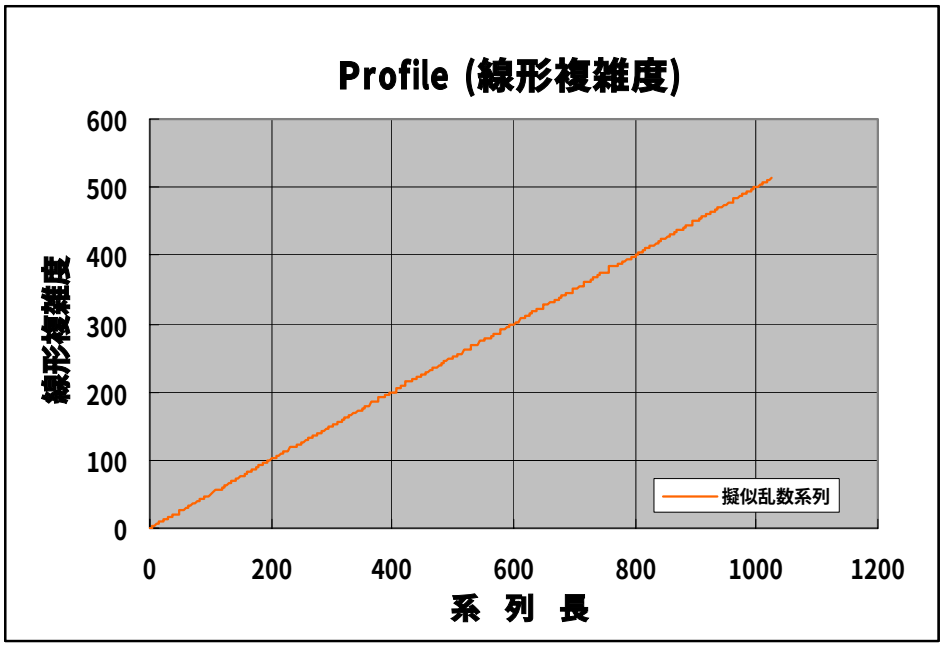

図 4. 擬似乱数系列の Profile

③. 相互情報量

暗号化処理のデータ攪拌武において、メッセージ M と冗長性 R を零として、擬似乱数生成器から出力される 2 元系列と暗号文 C の 2 進数表現による相関から得られる相互情報量を評価データとして参考資料〔相互情報量〕に示す。また、一様乱数を用いて得られたメッセージ M と暗号分 C との相互相関値(相関区間:N=1000)としても参考資料〔相互相関〕で与えている。相関結果については、各位相の相互相関値からの平均･分散･最小値･最大値で与える。

相互情報量および相互相関値の評価結果から、相互情報量は 1 に近い値を取るので一致するビットと一致しないものが等頻度となり、暗号結果からの擬似乱数系列の予測は難しい。また、相互相関値も低くいことからも、同じ事が言える。

④. 統計的性質 (1/0 等頻度性)

擬似乱数生成器から出力される系列を 2 進数で表現したとき、0 と 1 の出現回数を平均と分散で与える。ただし、系列長を 1 として規格化した値とする。

1/0 等頻度性の評価結果は、参考資料〔1/0 等頻度性〕から 1 と 0 とが、ほぼ等頻度で出現することが分かる。

⑤. 統計的性質 (連)

100 回の試行により、擬似乱数系列の連の分布を平均で与える〔参考資料〔連〕〕。

評価結果より、最も長い連(長さ *L*)の出現回数を1として、長さ *L*-1 の連の出現回数は 2、長さ *L-i* の連の出現回数はほぼ 2^i となっており、理想的な結果が得られた。

⑥. 統計的性質 (一様性)

一様性の評価は、擬似乱数系列からの出力系列を 2^i 進数(*i*=1,2,3,4)表現として、その出現分布により評価した。ただし、系列長を1として規格化した値とする。評価結果は、参考資料(1/0 等頻度性、一様性(2^2)、一様性(2^3)、一様性(2^4))で与える。

評価結果から、1/0 等頻度性の評価を含め、2^i 進数(*i*=1,2,3,4)表現における出現分布から一様性が高いことが分かる。

4. まとめ

評価時間制約から、擬似乱数生成器で出力される系列の周期については、評価の点で不十分な面もあるが。評価対象暗号アルゴリズム MULTI-S01 の安全性については、非常に高い結果が得られた。