暗号アルゴリズムの評価
PANAMA

2001 年 12 月 14 日

株式会社富士通研究所

武仲 正彦

鳥居 直哉

暗号アルゴリズムの評価

PANAMA

2001 年 12 月 14 日

－目次－

1. 評価対象アルゴリズム

本報告は PANAMA の統計的性質について解析を行った結果である。

1.2 擬似乱数生成器 PANAMA

PANAMA[*1] は、1998 年に J. Daemen 等によって提案された暗号モジュールであり、PANAMA を用いてストリーム暗号やハッシュ関数等が構成可能である。本報告では、ストリーム暗号 Multi-S01[*2] で使用されている PANAMA を使用した擬似乱数生成器について解析するものとする。

PANAMA は 256-bit の秘密鍵 K と 256-bit の乱数列番号 Q を入力とし、任意長の擬似乱数系列を生成する。PANAMA は以下の 3 つの動作モードを持つ。

・reset モード　内部状態のリセット

・push モード　秘密鍵や乱数列番号の入力

・pull モード　初期攪拌と擬似乱数列の生成

Multi-S01 では、リセット、秘密鍵と乱数列番号の入力、32 回の初期攪拌、擬似乱数列生成は次のスケジュールに従って行われる。

0.	reset	リセット
1.	push K	秘密鍵入力
2.	push Q	乱数列番号入力
3.	pull	初期攪拌 1
....	....	
34.	pull	初期攪拌 32
35.	pull	擬似乱数出力 1
....	....	
34+n	pull	擬似乱数出力 n

なお 1 回の出力で 256-bit の擬似乱数が出力される。

2. 評価項目

本報告では PANAMA の統計的性質を NIST SP800-22[*3] により検証する。

2.1 SP800-22

SP800-22 は NIST が公開している暗号アプリケーションのための乱数と擬似乱数の統計試験ツール[*4] 及びそのドキュメントである。AES 選定では、その候補に対して本ツールによる検定が行われ、その結果が報告[*5][*6] (以下 AES レポートと表記する)されている。本ツールでは、対象の擬似乱数列に対して、表 1 に示す 16 検定法 189 試験を行うことができる。

なお、本統計試験ツールは現在 Version1.4 であるが、公開されているソフトウェアには多くの不具合が含まれる。本評価においてはそれらの不具合について独自の修正、変更を行ったものを使用している。

表 1. SP800-22 で実行可能な検定法と試験

試 験番号	検定法	概要
1	Frequency Test	入力数列に含まれる０と１の個数の偏りを調べる。
2	Frequency Test within a Block	入力数列を 256-bit に区切り、その中の０と１の個数の割合の偏りを調べる。
3,4	Cumulative Sums (Cusum) Test	入力数列の 0/1 を–1/1 に変換し、先頭または一番後ろから１ビットずつその値を加算していく。加算操作中における、絶対値の最大値の偏りを調べる。
5	Runs Test	入力数列内に連(1 または 0 が連続している部分)がいくつあるかを数えて、その数の偏りを調べる。
6	Test for the Longest Runs of Ones in a Block	入力数列を 256-bit に区切り、その中の最大の連の長さの偏りを調べる。
7	Binary Matrix Rank Test	入力数列を 32×32 bits の部分数列に分割し、それを行列に書き下したときの階数の偏りを調べる。
8	Discrete Fourier Transform (Spectral) Test	入力数列を Discrete Fourier Transform によって周波数成分に分解し、各周波数におけるピークの高さが閾値を超える数を数えて、その偏りを調べる。
9 - 156	Non-overlapping Template Matching Test	9-bit の Template を用意し、入力数列中にそれらの Template がいくつ現れるかを数えて、その偏りを調べる。Template と同じビット列が出現したら、出現したテンプレート以降のビットから探索を再開する。ツールでは 148 個の Template について検定を行う。
157	Overlapping Template Matching Test	9-bit オール 1 のビット列を Template として用意する。入力数列中にその Template がいくつ現れるかを数えて、その偏りを調べる。Template が見つかっても見つからなくても１ビットずつずらしながら調べる。
158	Maurer’s “Universal Statistical” Test	入力数列において、任意の 7-bit のパターンが現れてから、次に現れるまでの距離の偏りを調べる。
159	Approximate Entropy Test	入力数列の中に、10-bit でとりうるパターン、11-bit ビットでとりうるパターンがそれぞれいくつ含まれるかを計算し、その数の偏りを調べる。
160-167	Random Excursion Test	入力数列の 0/1 を–1/1 に変換し、先頭から加算して行く。合計値が 0 の場所から、次に 0 になる場所までを一つの cycle と考え、8 種類(–4～–1, 1～4)の State の出現数の偏りを調べる。この検定法では State 別に 8

		種類の試験とする。
168-185	Random Excursion Variant Test	Random Excursion Test 同様に、数列を–1 と 1 に変換して合計していく。入力数列の先頭から最後までをまとめて扱い、18 種類(–9～–1, 1～9)の State の出現数の偏りを調べる。この検定法では State 別に 18 種類の試験とする。
186-187	Serial Test	入力数列の中に、16-bit でとりうるパターン、15-bit でとりうるパターン、14-bit でとりうるパターンがそれぞれいくつ含まれるかを計算し、その数の偏りを調べる。16-bit と 15-bit のパターンによる試験と、15-bit と 14-bit のパターンによる試験の 2 種類。
188	Lempel-Ziv Compression Test	入力数列の先頭から最後までに現れるビットパターンの偏りを調べる。
189	Linear Complexity Test	入力数列を 500-bit のブロックに分割し、それぞれの数列の線形複雑度を求め、その偏りを調べる。

入力する擬似乱数列は、ツールの制限から 1000000-bit 程度を複数系列用意する必要がある。本報告では AES レポートに従って 1048576-bit 300 系列を入力としている。

本ツールの出力は、「合格率」と「分布」の 2 種類ある。本ツールでは 1000000-bit 程度の擬似乱数列に対して 189 個の試験を行う。各試験では、対象の擬似乱数列が正規分布もしくは χ^2 分布のどのあたりに位置するかを P-Value という 0～1 の値で表現する。出力の「合格率」は、P-Value が 0.01 以上を合格とし、入力 300 系列の合格率である。AES レポートでは合格率 0.9633 以上(1%棄却)をその試験の合格とみなしており、本報告でもそれに従っている。

一方「分布」は、入力 300 系列分の P-Value の分布が一様かどうかを見るもので、各系列の P-Value を 10%ごと 10 区間で集計し、その 10 区間に含まれる数を χ^2 統計量に変換し P-Value で評価する。本報告では 1%棄却として 0.01 未満をその試験の不合格としている。

3. 評価方法

SP800-22 では、与えられた擬似乱数列の統計的な検定法について述べられているが、与える擬似乱数列の生成方法については何も述べられていない。そこで本報告では、擬似乱数列の生成についても可能な限り AES レポートに従って行うこととする。AES レポートでは、暗号アルゴリズムの特性を検討するために、暗号アルゴリズムの一部を使用して攪拌過程が検討可能な Partial round test と暗号アルゴリズム全体で擬似乱数列を生成する Full round test の 2 種類のテストをおこなっている。本報告でも PANAMA を使用して Partial round test と Full round test を行った。

3.1 Partial round test

Partial round test では AES レポートに従った擬似乱数列生成を行う。PANAMA を 256-bit のブロック暗号とみなし、秘密鍵を鍵、乱数列番号を平文、32 回の初期攪拌を Round とみなすことで Partial round test を行う。AES レポート中の擬似乱数列生成方法 8 種類のうち、乱数生成器で使用されることはないと考えられる CBC mode は行わないこととした。その代わりに、PANAMA では鍵と平文(乱数列番号)の扱いが同じであることを考慮して、Plaintext/Ciphertext Correlation と同様に鍵との相関を見る Key/Ciphertext Correlation を追加した。以下に各擬似乱数列生成法の詳細を示す。これらの擬似乱数列生成法では、秘密鍵や乱数列番号に偏りがある場合に、出力の系列間に偏りがあるかどうかを評価できる。これらの方法で生成した擬似乱数系列に対して試験を行い、その結果を Round 順に並べることで、入力された鍵や乱数列番号の攪拌されてゆく様子が観測できる。

3.1.2 Low Density Key

Low Density Key は鍵が 0 に偏ったものを使用した場合の、出力の偏りを調べるための擬似乱数生成法である。鍵と平文に使用する値は次の通り。

平文: 256-bit 乱数 1 パターン

鍵:256-bit オール 0 の鍵が 1 個(1 個中 1 個)、

256-bit 中 1 ビットだけが 1 の鍵が 256 個(256 個中 256 個)

256-bit 中 2 ビットだけが 1 の鍵が 3839 個(32512 個中 3839 個)

1 つの平文に対して鍵を 4096 個変更しながら出力 256-bit を生成し、合計 4096×256=1048576-bit の擬似乱数列を生成する。平文を 300 通り変更して 300 系列の擬似乱数列を生成する。

3.1.3 Low Density Plaintext

Low Density Plaintext は平文が 0 に偏ったものを使用した場合の、出力の偏りを調べるための擬似乱数生成法である。鍵と平文に使用する値は次の通り。

鍵: 256-bit 乱数 1 パターン

平文:256-bit オール 0 の平文が 1 個(1 個中 1 個)、

256-bit 中 1 ビットだけが 1 の平文が 256 個(256 個中 256 個)

256-bit 中 2 ビットだけが 1 の平文が 3839 個(32512 個中 3839 個)

1 つの鍵に対して平文を 4096 個変更しながら出力 256-bit を生成し、合計 4096×256=1048576-bit の擬似乱数列を生成する。鍵を 300 通り変更して 300 系列の擬似乱数列を生成する。

3.1.4 High Density Key

High Density Key は鍵が 1 に偏ったものを使用した場合の、出力の偏りを調べるための擬似乱数生成法である。鍵と平文に使用する値は次の通り。

平文: 256-bit 乱数 1 パターン

鍵:256-bit オール 1 の鍵が 1 個(1 個中 1 個)、

256-bit 中 1 ビットだけが 0 の鍵が 256 個(256 個中 256 個)

256-bit 中 2 ビットだけが 0 の鍵が 3839 個(32512 個中 3839 個)

1 つの平文に対して鍵を 4096 個変更しながら出力 256-bit を生成し、合計 4096×256=1048576-bit の擬似乱数列を生成する。平文を 300 通り変更して 300 系列の擬似乱数列を生成する。

3.1.5 High Density Plaintext

High Density Plaintext は平文が 1 に偏ったものを使用した場合の、出力の偏りを調べるための擬似乱数生成法である。鍵と平文に使用する値は次の通り。

鍵: 256-bit 乱数 1 パターン

平文:256-bit オール 1 の平文が 1 個(1 個中 1 個)、

256-bit 中 1 ビットだけが 0 の平文が 256 個(256 個中 256 個)

256-bit 中 2 ビットだけが 0 の平文が 3839 個(32512 個中 3839 個)

1 つの鍵に対して平文を 4096 個変更しながら出力 256-bit を生成し、合計 4096×256=1048576-bit の擬似乱数列を生成する。鍵を 300 通り変更して 300 系列の擬似乱数列を生成する。

3.1.6 Key Avalanche

Key Avalanche は鍵に 1-bit 差分がある場合の出力差分の偏りを調べるための擬似乱数生成法である。鍵と平文に使用する値は次の通り。

鍵: 256-bit 乱数 1 パターンと、その鍵と 1-bit 差分となる 256-bit 鍵 256 パターン

平文: 256-bit オール 0 固定

まず、基になる鍵と平文から出力 1 を計算し、次に 1-bit 差分となる鍵と平文から出力 2 を計算し、出力 1 と出力 2 の XOR を取ったものを 256-bit の擬似乱数とする。そして 1-bit 差分となる鍵を変えながら 256×256=65536-bit 擬似乱数列を生成する。基となる鍵を 16 通り変更して 1048576-bit の擬似乱数列を生成し、それを 300 回繰り返して 300 系列の擬似乱数列を生成する。

3.1.7 Plaintext Avalanche

Plaintext Avalanche は平文に 1-bit 差分がある場合の出力差分の偏りを調べるための擬似乱数生成法である。鍵と平文に使用する値は次の通り。

平文: 256-bit 乱数 1 パターンと、その平文と 1-bit 差分となる 256-bit 平文 256 パターン

鍵: 256-bit オール 0 固定

まず、基になる平文と鍵から出力 1 を計算し、次に 1-bit 差分となる平文と鍵から出力 2 を計算し、出力 1 と出力 2 の XOR を取ったものを 256-bit の擬似乱数とする。そして 1-bit 差分となる平文を変えながら 256×256=65536-bit 擬似乱数列を生成する。基となる平文を 16 通り変更して 1048576-bit の擬似乱数列を生成し、それを 300 回繰り返して 300 系列の擬似乱数列を生成する。

3.1.8 Key/Ciphertext Correlation

Key/Ciphertext Correlation は鍵と出力の相関がどれくらい偏ってあるかを調べるための擬似乱数生成法である。鍵と平文に使用する値は次の通り。

鍵: 乱数 1 パターン

平文: 乱数 4096 パターン

鍵と平文から出力を計算し、その出力と鍵の XOR を取ったものを 256-bit の擬似乱数とする。そして平文を変えながら 4096×256 = 1048576-bit の擬似乱数列を生成する。鍵を 300 通り変更して 300 系列の擬似乱数列を生成する。

3.1.9 Plaintext/Ciphertext Correlation

Plaintext/Ciphertext Correlation は平文と出力の相関がどれくらい偏ってあるかを調べるための擬似乱数生成法である。鍵と平文に使用する値は次の通り。

鍵: 乱数 1 パターン

平文: 乱数 4096 パターン

鍵と平文から出力を計算し、その出力と平文の XOR を取ったものを 256-bit の擬似乱数とする。そして平文を変えながら 4096×256 = 1048576-bit の擬似乱数列を生成する。鍵を 300 通り変更して 300 系列の擬似乱数列を生成する。

3.2 Full round test

AES レポートでは、対象が 1 ブロックの入力に対して 1 ブロックの出力が行われるブロック暗号のため、Partial round test で述べたような各種の擬似乱数列生成を行っている。しかし乱数生成器 PANAMA では擬似乱数列そのものが出力されるため、同様の操作では評価できないと考えられる。そこで、本節の Full round test では以下に示す方法で擬似乱数列を生成し、評価を行うこととした。

1. PANAMA に対して乱数で生成した秘密鍵と乱数列番号を入力し初期攪拌後に 314572800-bit の擬似乱数列を生成
2. 1.で生成した擬似乱数列を 1048576-bit×300 とみなして SP800-22 で統計試験を実行
3. 1.2.を 128 回繰返し、SP800-22 の「合格率」と「分布」をグラフ化

ここで、1 で使用する乱数は、SP800-22 ツールに添付されている BBS (Blum-Blum-Shub)乱数ファイルのデータを前から順に使用している。

また、手順 3 で 128 回繰り返しているのは、信頼性を向上するためである。例え真性乱数を使用して同様の統計試験を行ったとしても、「分布」ならば 100 回に 1 回程度は不合格となる。そのため、128 回同じ試験を行うことで信頼性の向上をはかっている。。

4. 評価結果

4.1 Partial round test

Partial round test の結果を図 1~16 に示す。奇数番号の図は SP800-22 出力のうち「合格率」の結果である。横軸が 2 章で示した試験項目、縦軸が初期攪拌回数で、2.1 節で述べ

たようにある初期攪拌回数におけるある試験における合格率が 96.33%未満の場合、「その試験項目は不合格である」としてその交点に点をプロットしている。

同様に偶数番号の図は SP800-22 出力のうち「分布」の結果である。横軸が 2 章で示した試験項目、縦軸が初期攪拌回数で、2.1 節で述べたようにある初期攪拌回数におけるある試験の P-value が 0.01 未満の場合、「その試験項目は 1%棄却された」としてその交点に点をプロットしている。

なお、図 1~16 は不合格となったテスト項目をプロットしたものと 1%棄却されたテスト項目をプロットしたものであるが、より詳細な情報として各テストにおける「合格率」と「分布」の攪拌過程のグラフを Appendix A1~16 に示した。

4.1.2 Low Density Key

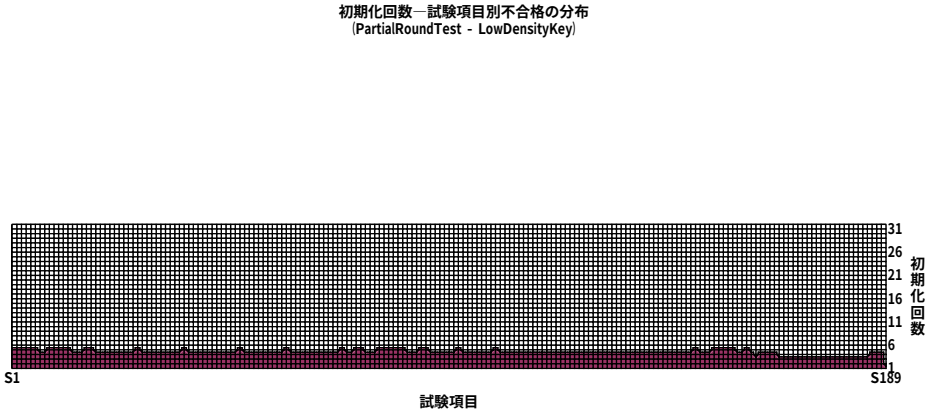

図 1 PANAMA の初期化回数による試験項目別不合格の分布(Low Density Key)

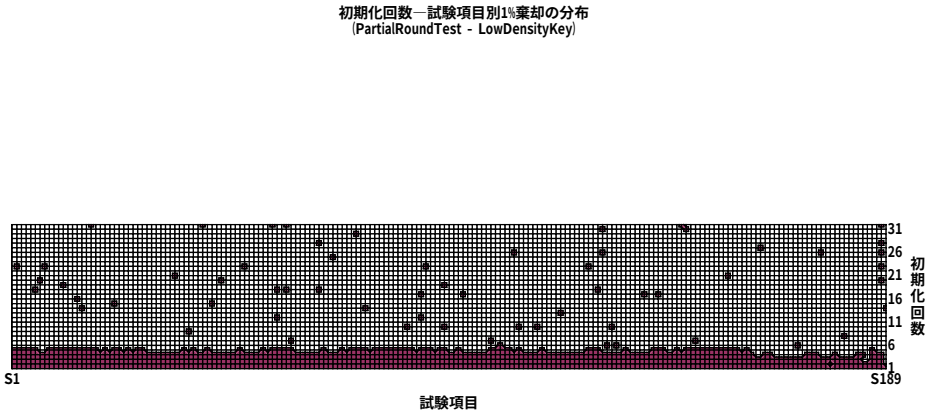

図 2 PANAMA の初期化回数による試験項目別 1%棄却の分布(Low Density Key)

図 1, 2 より、Low Density Key では PANAMA は初期攪拌 6 回程度で、入力される秘密鍵と乱数列番号が一様に攪拌されていることがわかる。但し「分布」の試験 188(Lempel-Ziv Compression Test)でやや不合格が多く起こっているようにも見える。

4.1.3 Low Density Plaintext

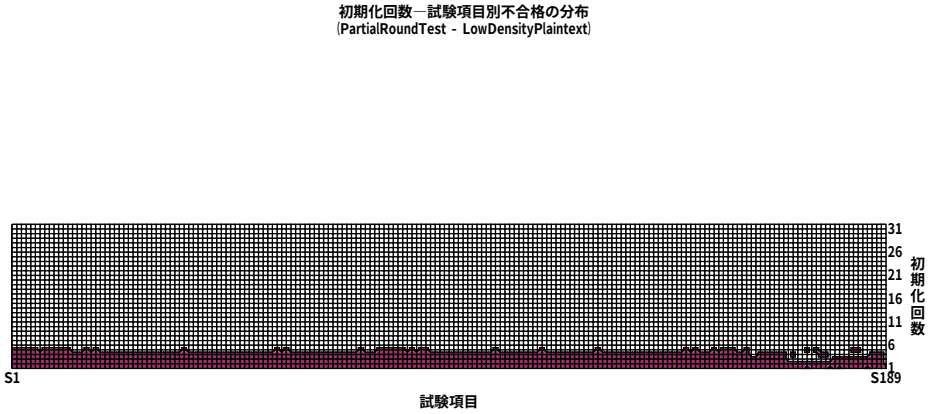

図 3 PANAMA の初期化回数による試験項目別不合格の分布(Low Density Plaintext)

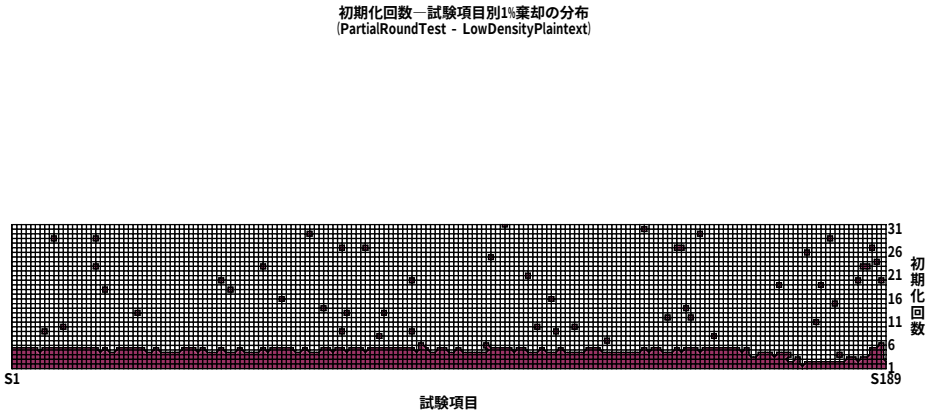

図 4 PANAMA の初期化回数による試験項目別 1%棄却の分布(Low Density Plaintext)

図 3, 4 より PANAMA は初期攪拌 6 回程度で、入力される秘密鍵と乱数列番号が一様に攪拌されていることがわかる。

4.1.4 High Density Key

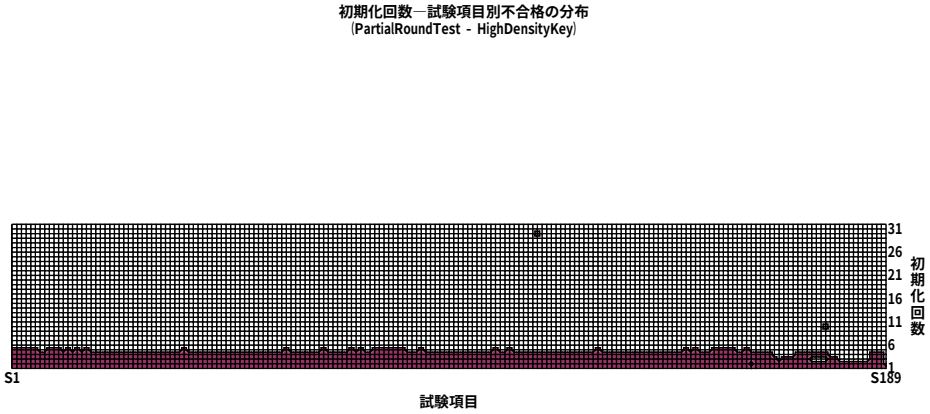

図 5 PANAMA の初期化回数による試験項目別不合格の分布(High Density Key)

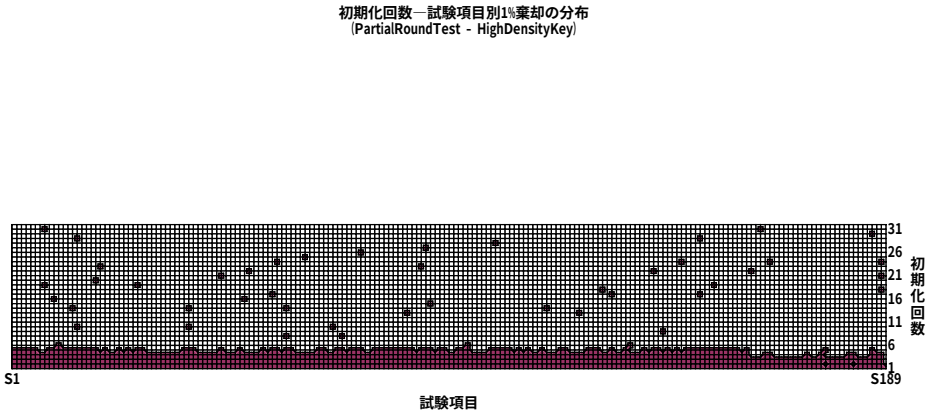

図 6 PANAMA の初期化回数による試験項目別 1%棄却の分布(High Density Key)

図 5, 6 より PANAMA は初期攪拌 6 回程度で、入力される秘密鍵と乱数列番号が一様に攪拌されていることがわかる。

4.1.5 High Density Plaintext

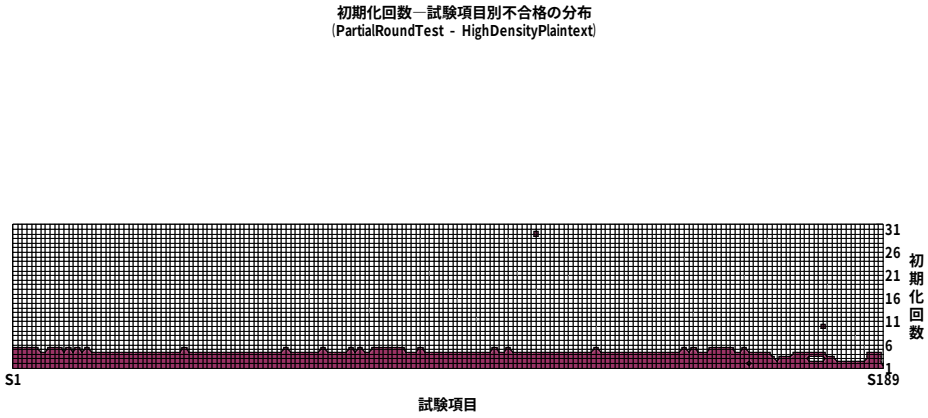

図 7 PANAMA の初期化回数による試験項目別不合格の分布(High Density Plaintext)

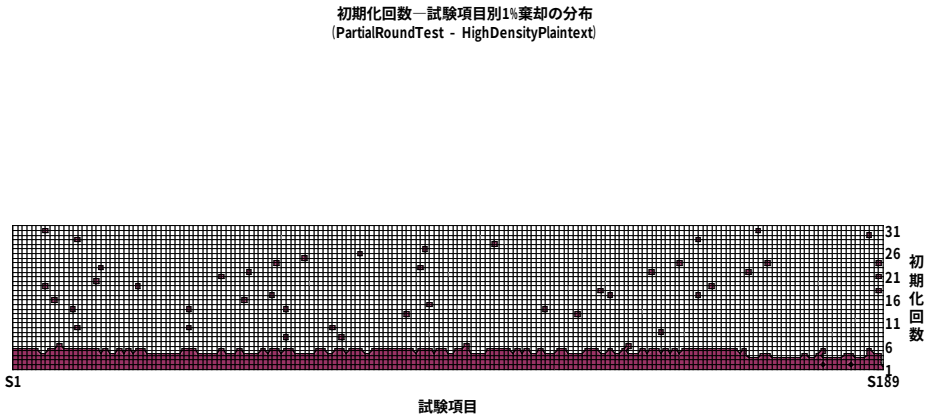

図 8 PANAMA の初期化回数による試験項目別 1%棄却の分布(High Density Plaintext)

図 7, 8 より PANAMA は初期攪拌 6 回程度で、入力される秘密鍵と乱数列番号が一様に攪拌されていることがわかる。

4.1.6 Key Avalanche

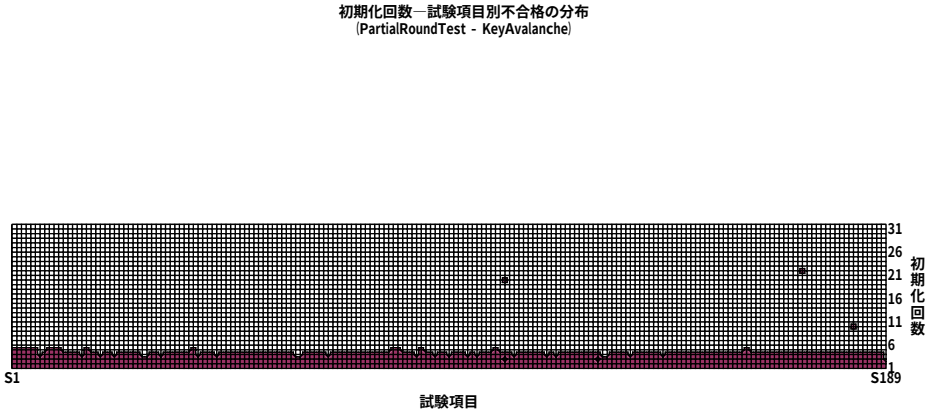

図 9 PANAMA の初期化回数による試験項目別不合格の分布(Key Avalanche)

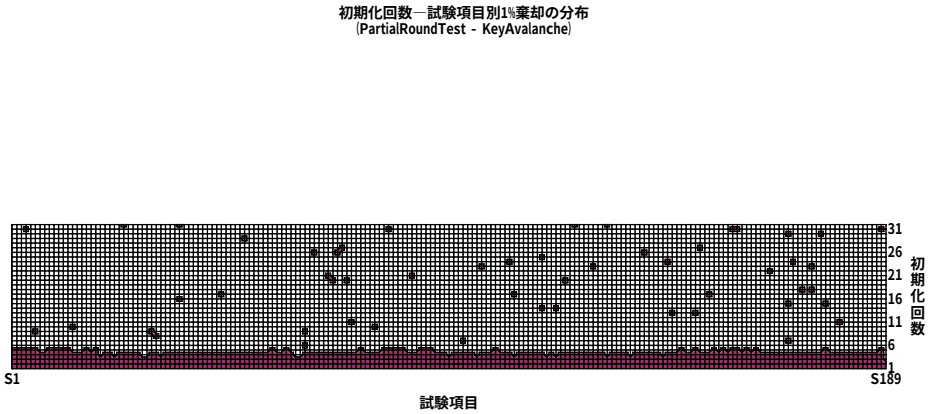

図 10 PANAMA の初期化回数による試験項目別 1%棄却の分布(Key Avalanche)

図 9, 10 より PANAMA は初期攪拌 5 回程度で、入力される秘密鍵と乱数列番号が一様に攪拌されていることがわかる。

4.1.7 Plaintext Avalanche

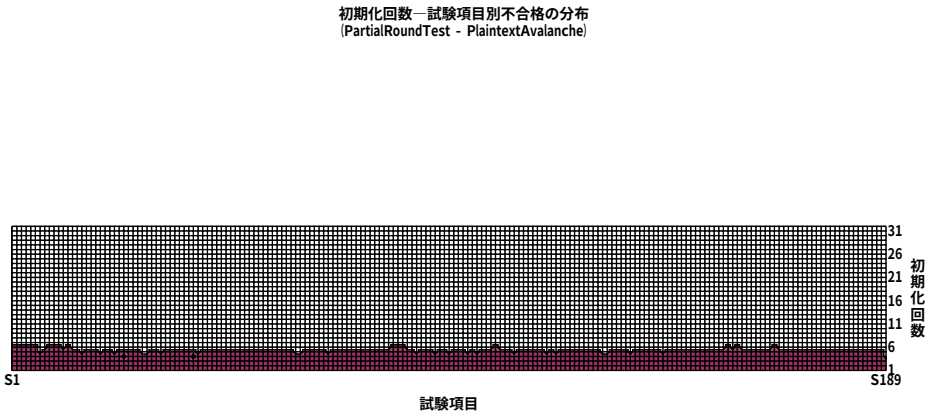

図 11 PANAMA の初期化回数による試験項目別不合格の分布(Plaintext Avalanche)

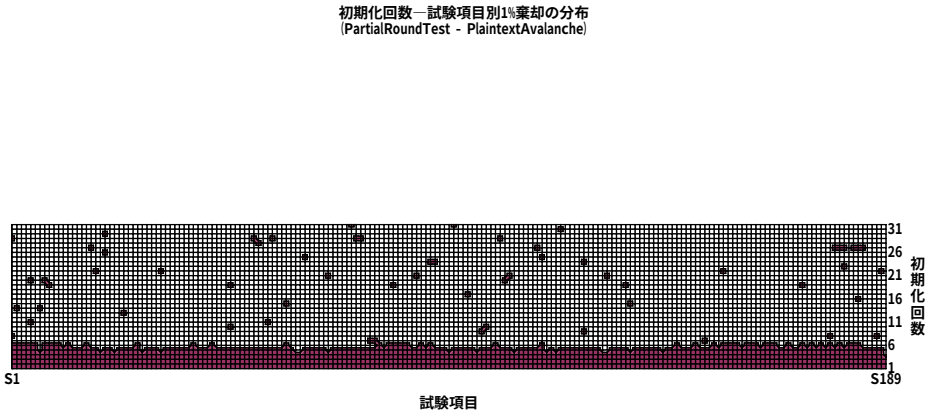

図 12 PANAMA の初期化回数による試験項目別 1%棄却の分布(Plaintext Avalanche)

図 11, 12 より PANAMA は初期攪拌 7 回程度で、入力される秘密鍵と乱数列番号が一様に攪拌されていることがわかる。

4.1.8 Key/Ciphertext Correlation

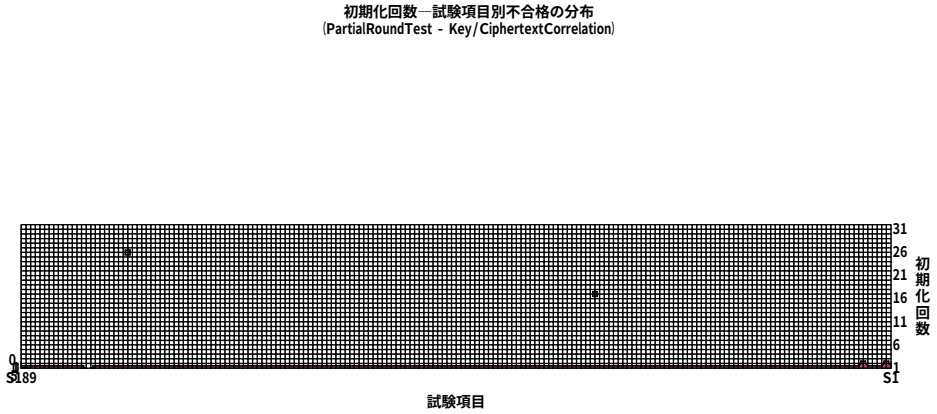

図 13 PANAMA の初期化回数による試験項目別不合格の分布(Key/Ciphertext Correlation)

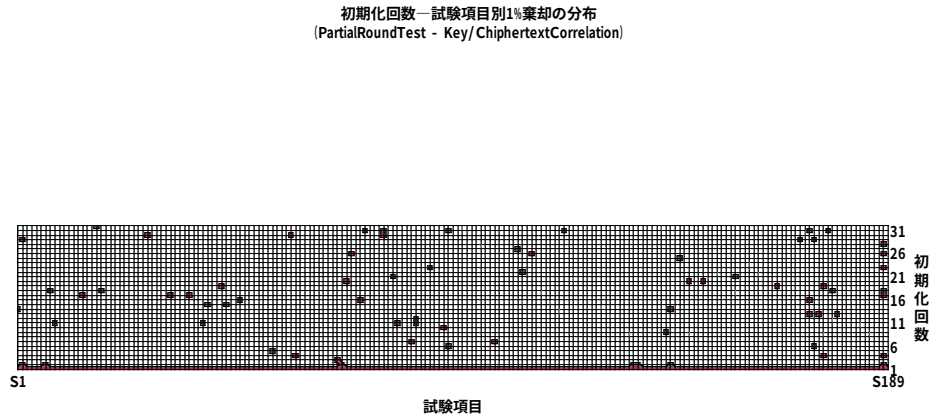

図 14 PANAMA の初期化回数による試験項目別 1%棄却の分布(Key/Ciphertext Correlation)

図 13, 14 より PANAMA は初期攪拌 3 回程度で、入力される秘密鍵と出力乱数列の相関はほとんど無くなり、一様に攪拌されていることがわかる。

4.1.9 Plaintext/Ciphertext Correlation

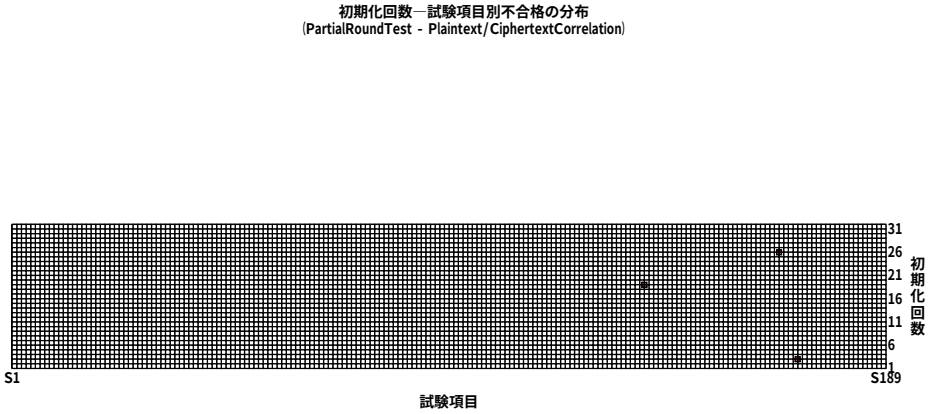

図 15 PANAMA の初期化回数による試験項目別不合格の分布(Plaintext/Ciphertext Correlation)

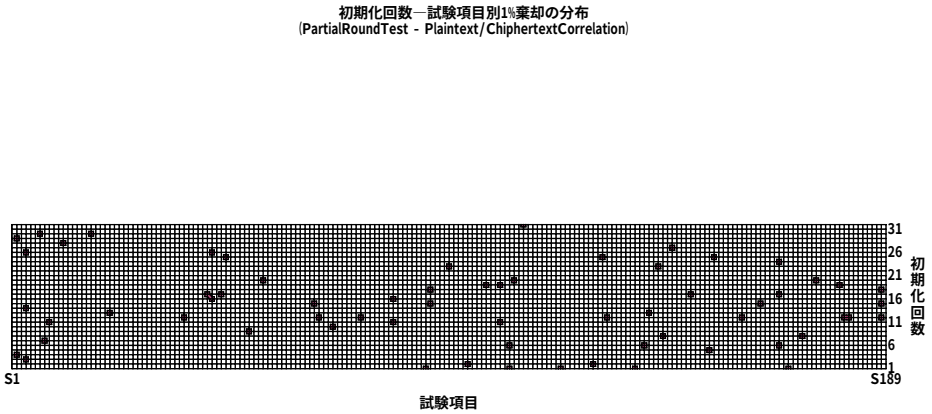

図 16 PANAMA の初期化回数による試験項目別 1%棄却の分布(Plaintext/Ciphertext Correlation)

図 15, 16 より PANAMA は初期攪拌 1 回で、入力される乱数列番号と出力乱数列の相関はほとんど無くなり、一様に攪拌されていることがわかる。

4.2 Full round test

Full round test の結果を図 17, 18 に示す。図は SP800-22 出力のうち「合格率」の結果である。横軸が 2 章で示した試験項目、縦軸が試行回数で、ある試行回のある試験における合格率が 96.33%未満の場合、「その試験項目は不合格である」としてその交点に点をプロットしている。試行回数は 128 回で同じ試験項目で 1 回以上不合格となると、擬似乱数系列はその試験項目の性質について問題がある可能性がある。

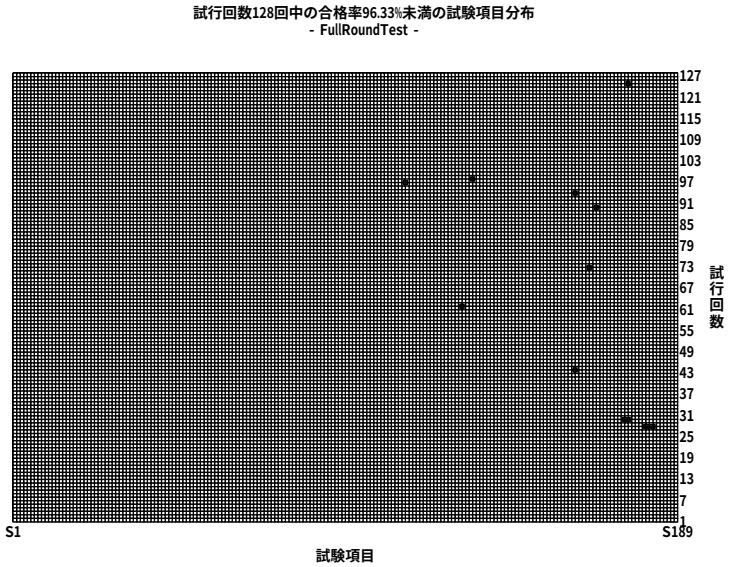

図 18 PANAMA の試行回数 128 回における不合格の試験項目分布(Full Round Test)

図 17 より、同じ試験項目で複数不合格となったものは無く「合格率」からみた場合 PANAMA の Full round test に偏りは無いと考えられる。

同様に図 18 は SP800-22 出力のうち「分布」の結果で、ある試行回のある試験の P-value が 0.01 未満の場合、「その試験項目は 1%棄却する」としてその交点に点をプロットしている。試行回数は 128 回で同じ試験項目で数回以上不合格となると、擬似乱数系列はその試験項目の性質について問題がある可能性がある。

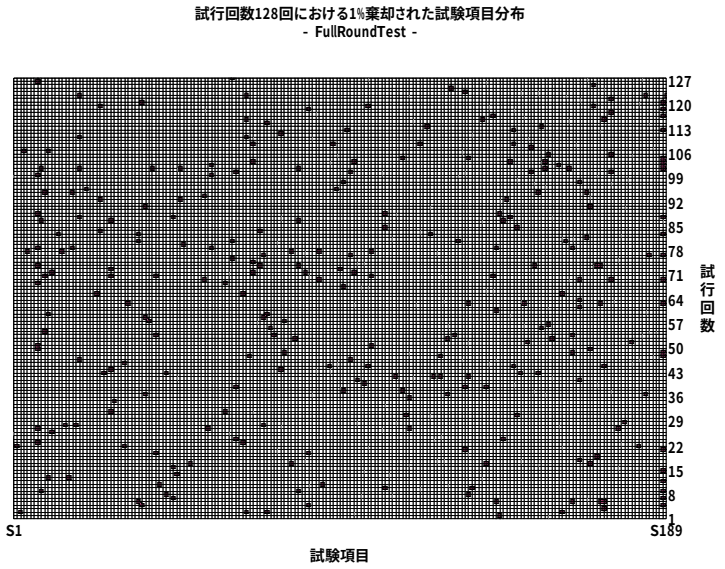

図 18 PANAMA の試行回数 128 回における 1%棄却された試験項目分布(Full Round Test)

図 18 より、「分布」では試験 8(Discrete Fourier Transfer Test)と試験 188(Lempel-Ziv Compression Test)で 10 回以上不合格となっている。これを明確に示すために 1%棄却数を棒グラフで表すと図 19 のようになる。

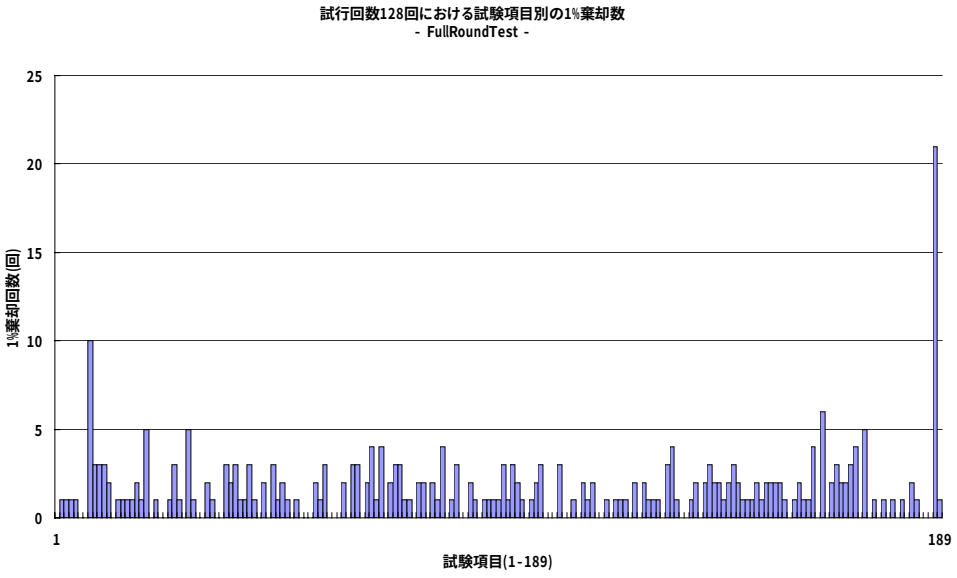

図 19 PANAMA の試行回数 128 回における項目別 1%棄却数(Full Round Test)

図 19 から、明らかに試験 8 と試験 188 が他の試験項目よりも 1%棄却数が大きいことが分かる。このことから PANAMA で長い擬似乱数系列を生成した場合、周波数成分の一様性(DFT)および、出現パターンの一様性(Lempel-Ziv)に問題がある可能性があると考えられる。

5. まとめ

PANAMA の統計的性質について SP800-22 を用いた評価を行った。PANAMA の初期攪拌における秘密鍵と乱数列番号の攪拌性を評価した結果、入力する秘密鍵や乱数列番号のデータの偏り、差分の偏り、及び入力データとの相関の全てについて、初期攪拌 7 回程度で充分な攪拌が行われていることが判明した。そのため PANAMA 仕様の、擬似乱数列が出力される初期攪拌 32 回後では、入力の偏りによる出力乱数の系列間の偏りは全く見られないと考えられる。

また、PANAMA を用いて長い擬似乱数列を出力した場合の統計的性質を評価した結果、その擬似乱数系列は多くの統計的性質で真性乱数との区別はつかないが、一部の性質については真性乱数よりも偏りが大きいことが判明した。このことから PANAMA により生成された擬似乱数列は、周波数成分の一様性と出現パターンの一様性に関しては問題がある可能性があると考えられる。

参考文献

*1: Joan Daemen and Craig S. K. Clapp, "Fast Hashing and Stream Encryption with PANAMA.", FSE98, LNCS1372, pp. 60-74, 1998

*2: 古屋聡一，渡辺大，宝木和夫，「MULTI-S01 のパディングと安全性についての考察」電子情報通信学会技術研究報告，ISEC2000-68，2000.

*3: NIST Special Publication 800-22, ``A STATISTICAL TEST SUITE FOR RANDOM AND PSEUDORANDOM NUMBER GENERATORS FOR CRYPTOGRAPHIC APPLICATIONS,''
(http://csrc.nist.gov/rng/SP800-22.pdf, http://csrc.nist.gov/rng/errata2.pdf)

*4: NIST Special Publication 800-22, ``NIST Statistical Test Suite,''
(http://csrc.nist.gov/rng/sts-1.4.tar, http://csrc.nist.gov/rng/sts.data.tar)

*5: Juan Soto, ``Randomness Testing of the Advanced Encryption Standard Finalist Candidates,''
(http://csrc.nist.gov/rng/aes-report-final.doc)

*6: Juan Soto, ``Randomness Testing of the AES Candidate Algorithms,''
(http://csrc.nist.gov/rng/AES-REPORT2.doc)

APPENDIX A

A1. Partial Round Test

Row Density Key(**「分布」出力**)

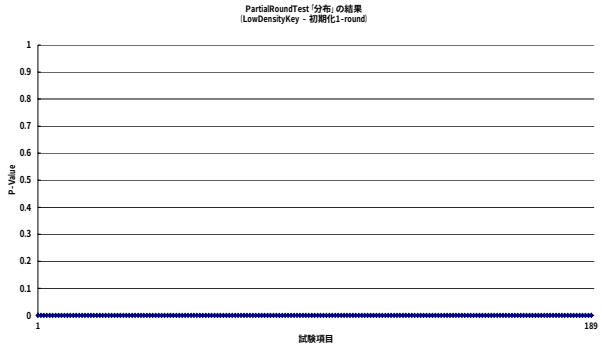

図 A1-1 初期攪拌 1 回

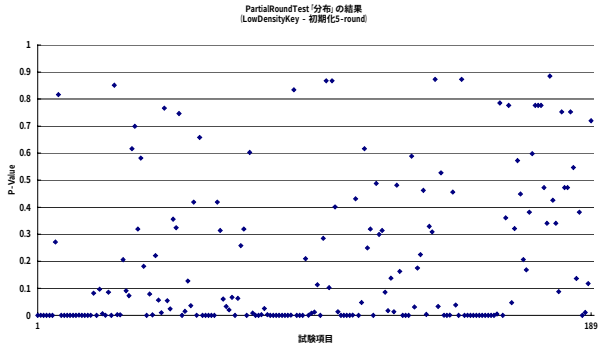

図 A1-5 初期攪拌 5 回

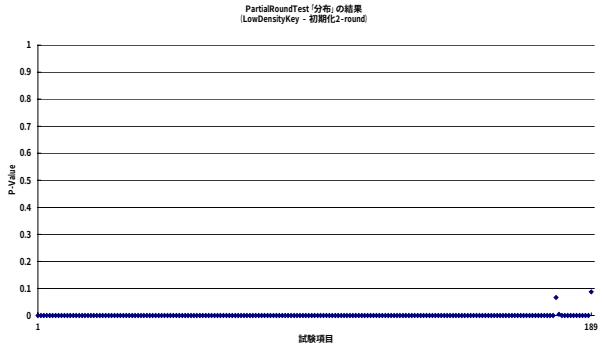

図 A1-2 初期攪拌 2 回

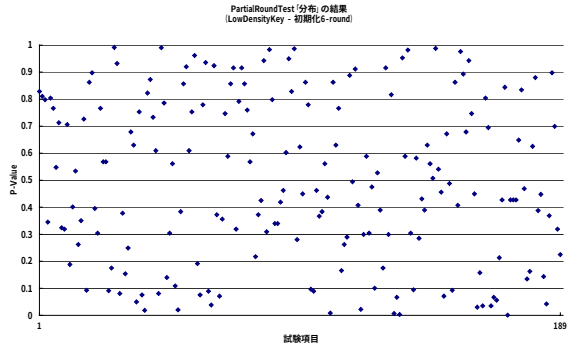

図 A1-6 初期攪拌 6 回

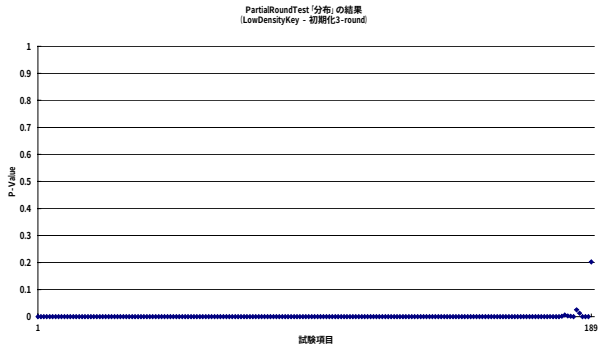

図 A1-3 初期攪拌 3 回

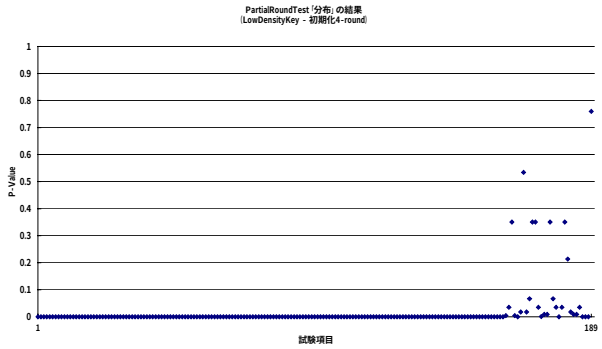

図 A1-4 初期攪拌 4 回

A2. Partial Round Test

Row Density Key(**「合格率」出力**)

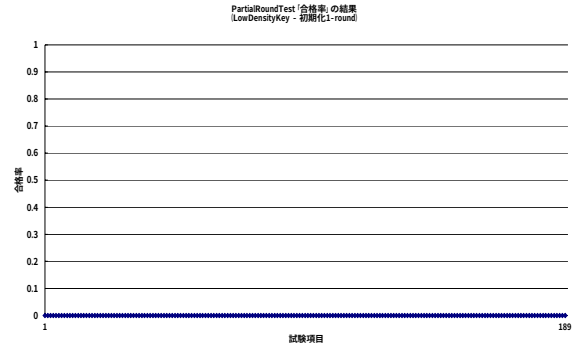

図 A2-1 初期攪拌 1 回

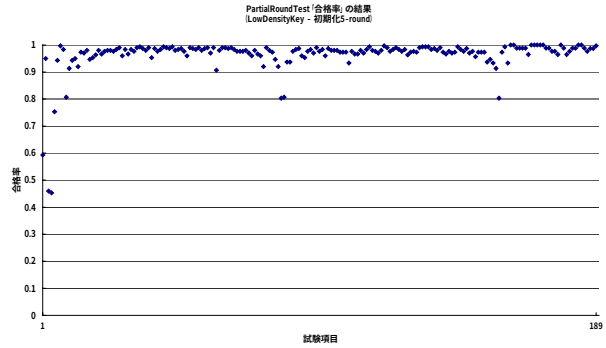

図 A2-5 初期攪拌 5 回

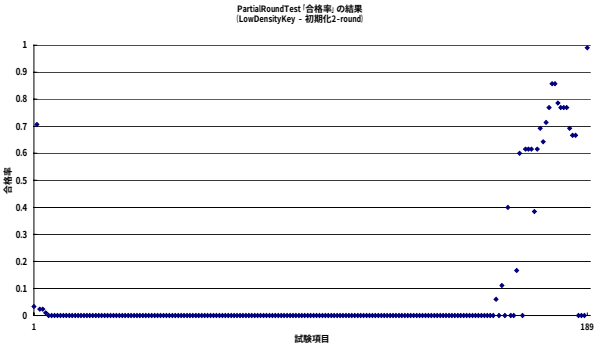

図 A2-2 初期攪拌 2 回

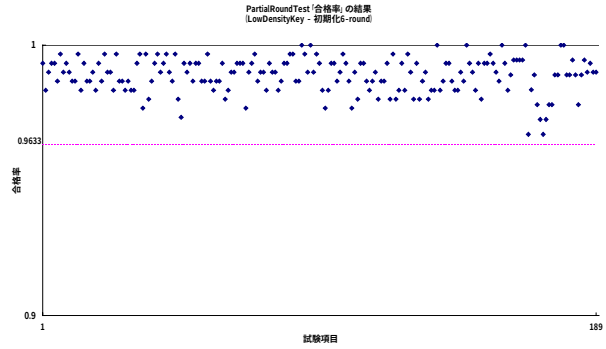

図 A2-6 初期攪拌 6 回

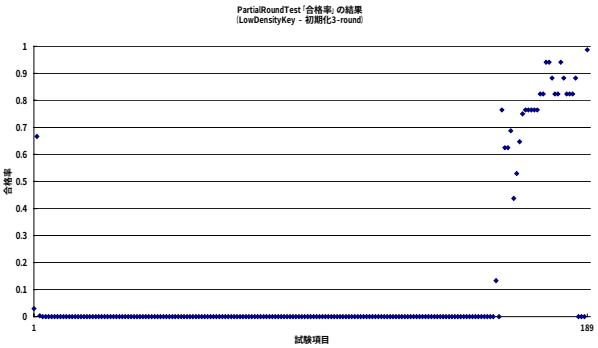

図 A2-3 初期攪拌 3 回

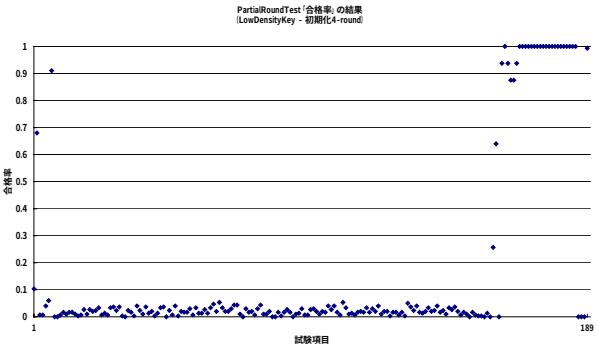

図 A2-4 初期攪拌 4 回

A3. Partial Round Test

Row Density Plaintext(**「分布」出力**)

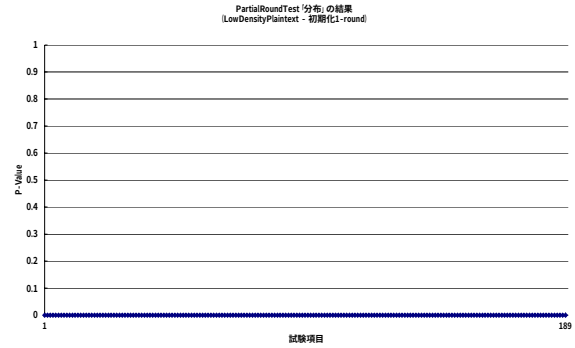

図 A3-1 初期攪拌 1 回

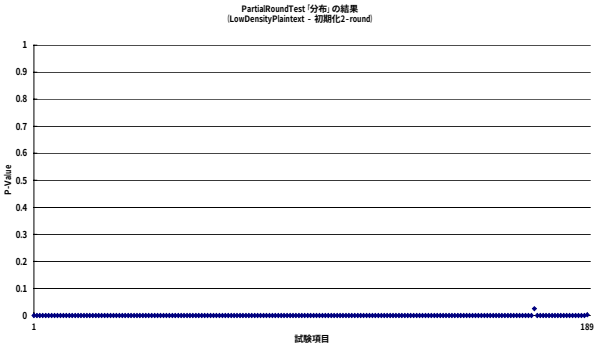

図 A3-2 初期攪拌 2 回

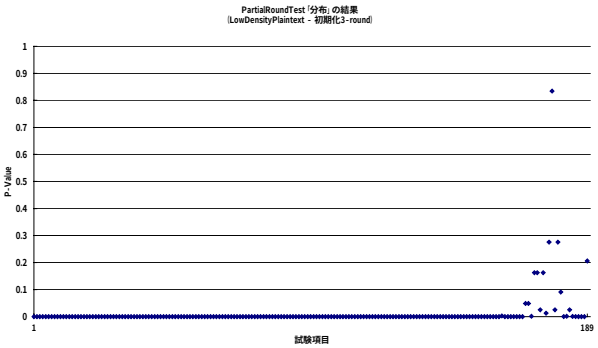

図 A3-3 初期攪拌 3 回

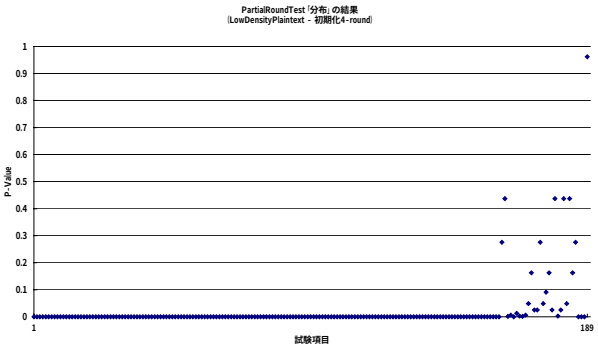

図 A3-4 初期攪拌 4 回

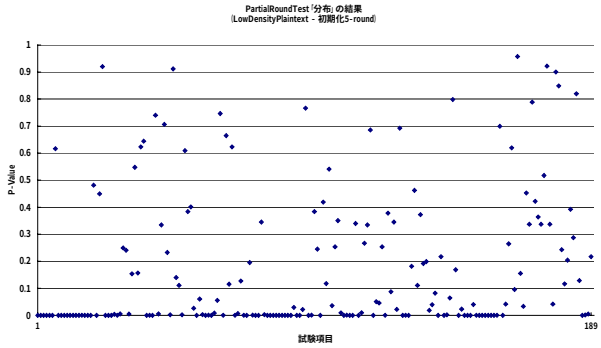

図 A3-5 初期攪拌 5 回

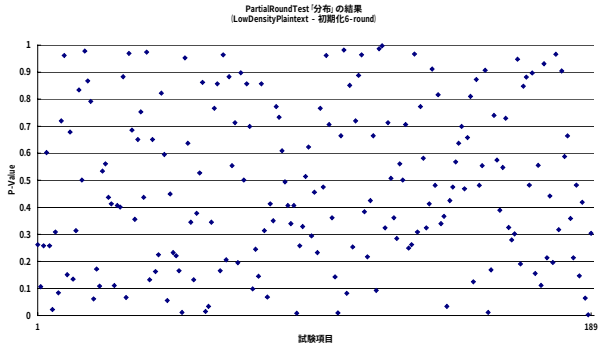

図 A3-6 初期攪拌 6 回

A4. Partial Round Test

Row Density Plaintext(**「合格率」出力**)

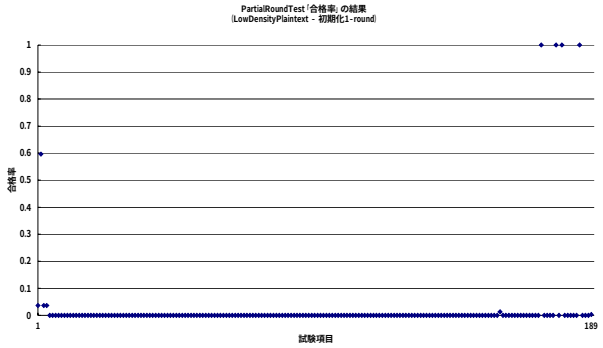

図 A4-1 初期攪拌 1 回

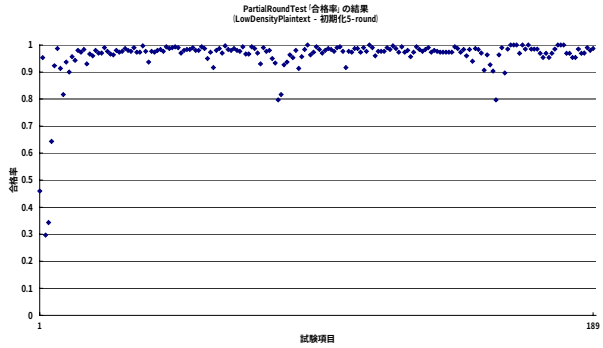

図 A4-5 初期攪拌 5 回

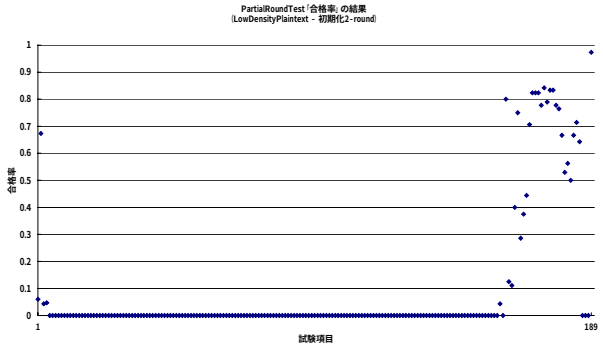

図 A4-2 初期攪拌 2 回

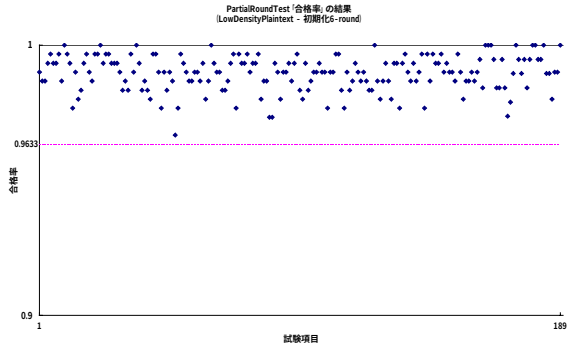

図 A4-6 初期攪拌 6 回

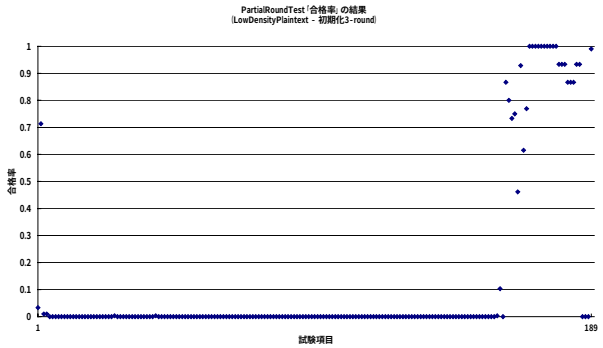

図 A4-3 初期攪拌 3 回

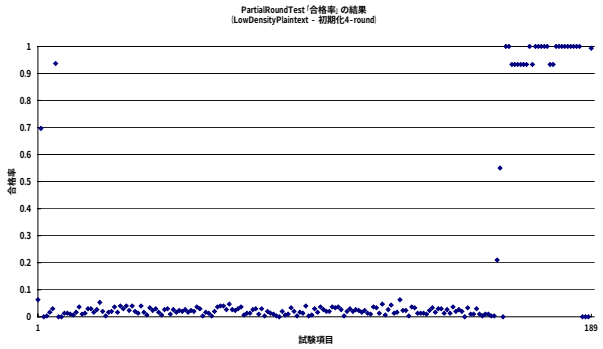

図 A4-4 初期攪拌 4 回

A5. Partial Round Test

High Density Key(**「分布」出力**)

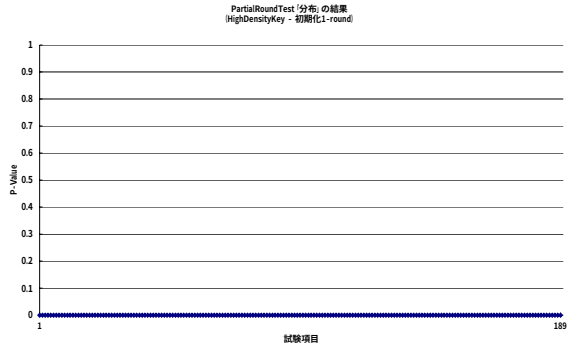

図 A5-1 初期攪拌 1 回

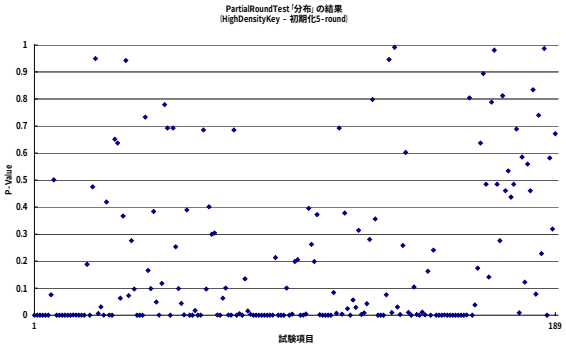

図 A5-5 初期攪拌 5 回

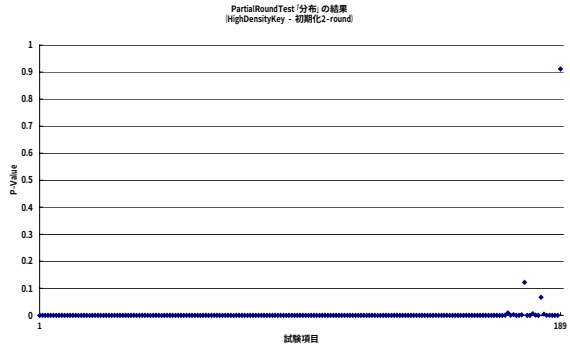

図 A5-2 初期攪拌 2 回

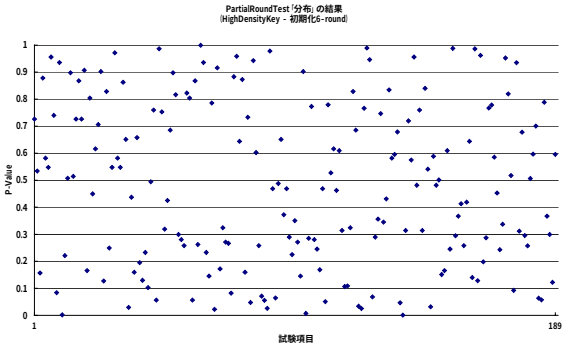

図 A5-6 初期攪拌 6 回

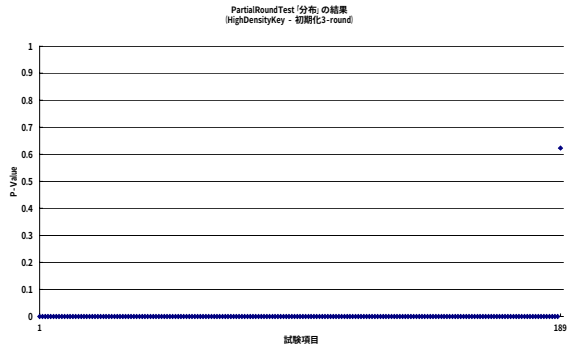

図 A5-3 初期攪拌 3 回

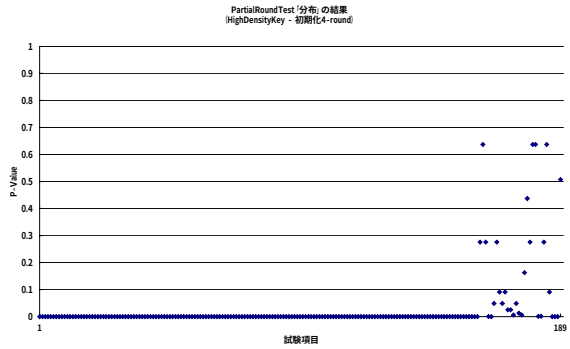

図 A5-4 初期攪拌 4 回

A6. Partial Round Test

High Density Key(**「合格率」出力**)

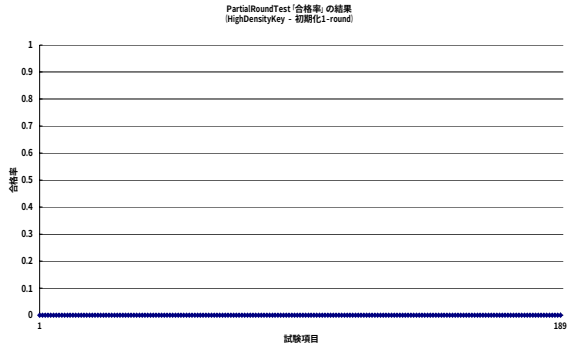

図 A6-1 初期攪拌 1 回

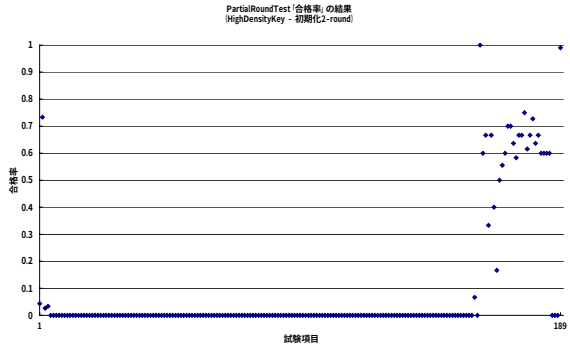

図 A6-2 初期攪拌 2 回

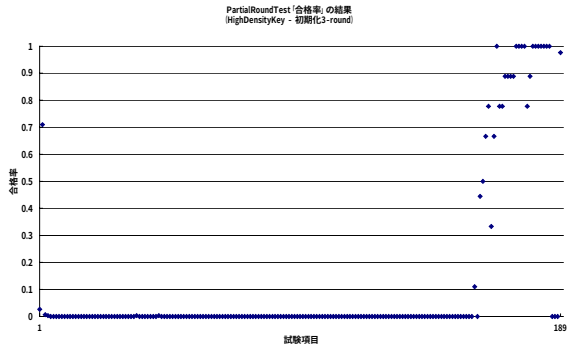

図 A6-3 初期攪拌 3 回

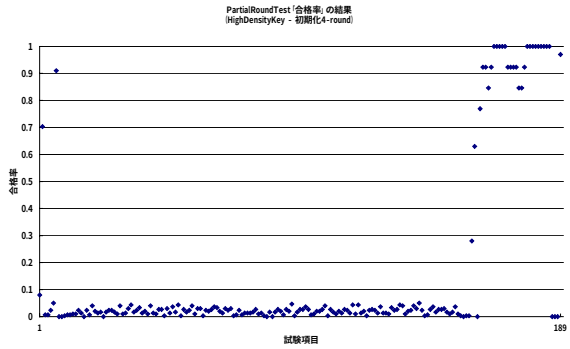

図 A6-4 初期攪拌 4 回

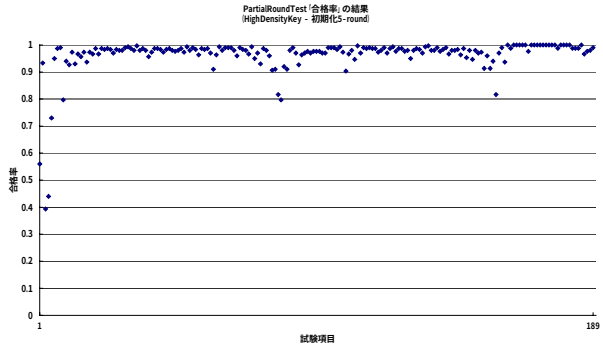

図 A6-5 初期攪拌 5 回

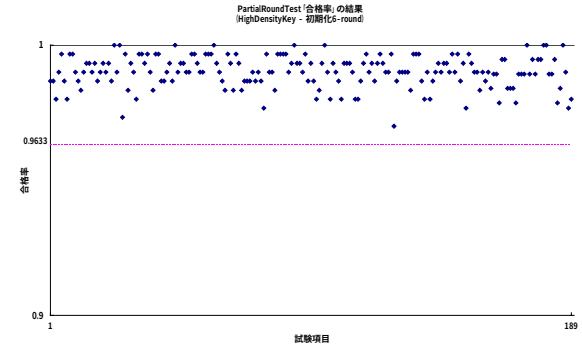

図 A6-6 初期攪拌 6 回

A7. Partial Round Test

High Density Plaintext(**「分布」出力**)

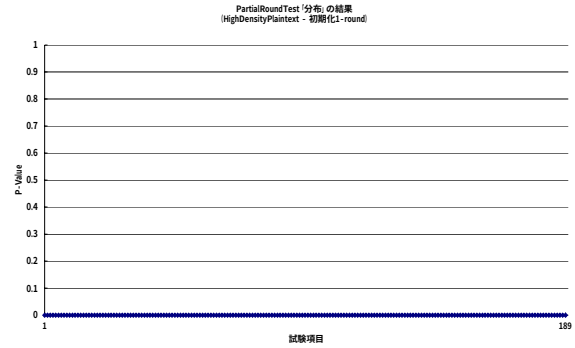

図 A7-1 初期攪拌 1 回

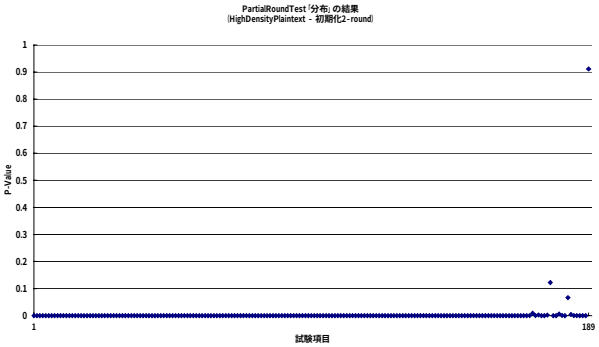

図 A7-2 初期攪拌 2 回

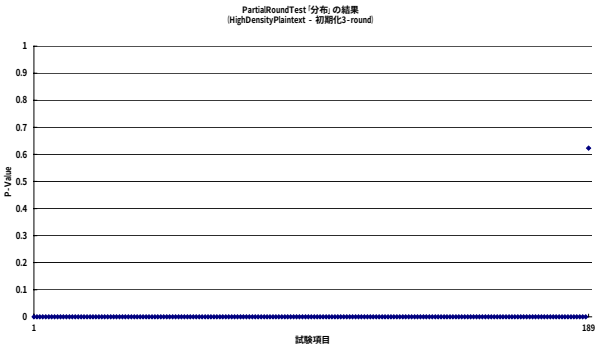

図 A7-3 初期攪拌 3 回

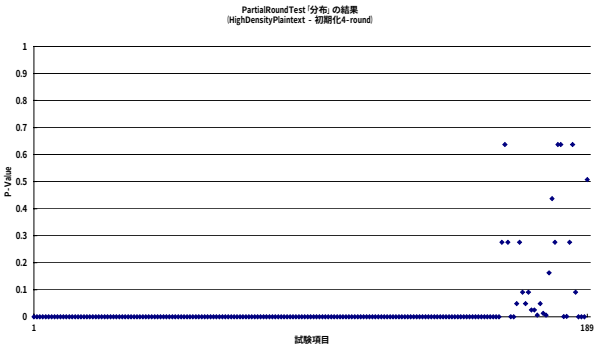

図 A7-4 初期攪拌 4 回

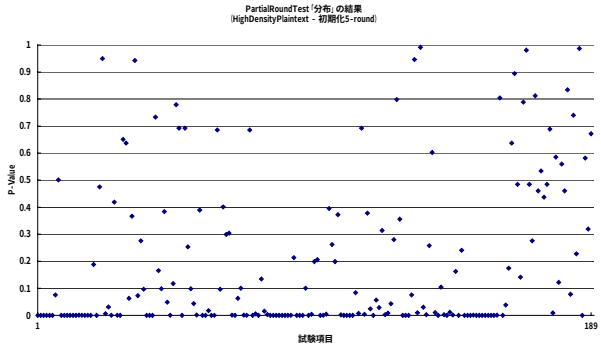

図 A7-5 初期攪拌 5 回

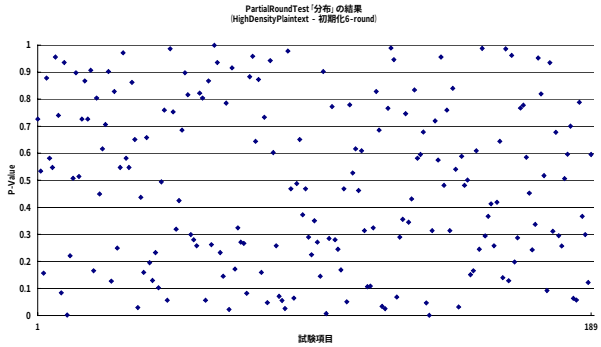

図 A7-6 初期攪拌 6 回

A8. Partial Round Test

High Density Plaintext (**「合格率」出力**)

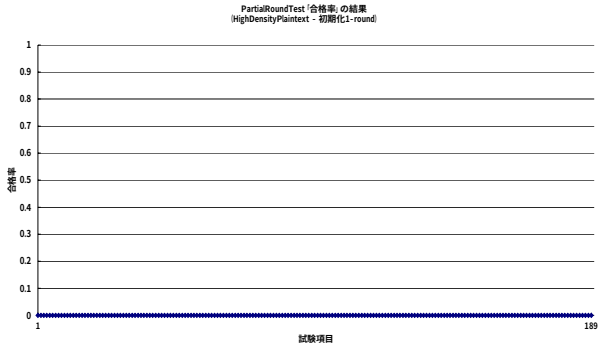

図 A8-1 初期攪拌 1 回

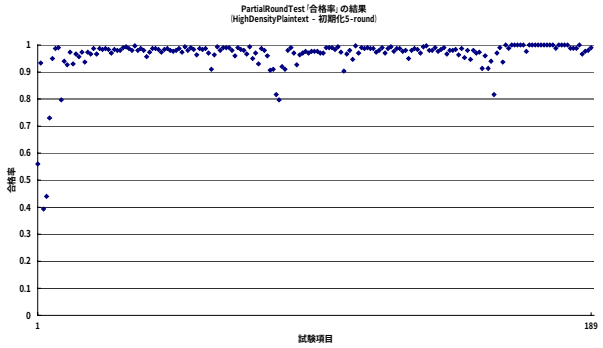

図 A8-5 初期攪拌 5 回

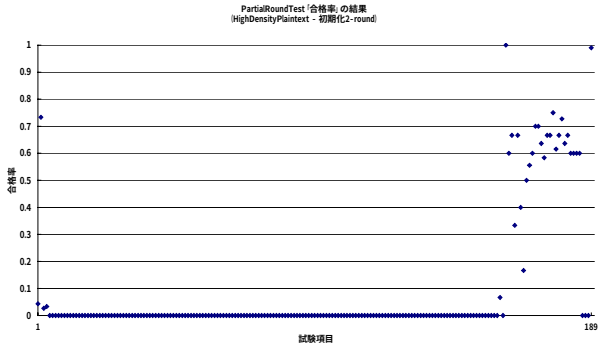

図 A8-2 初期攪拌 2 回

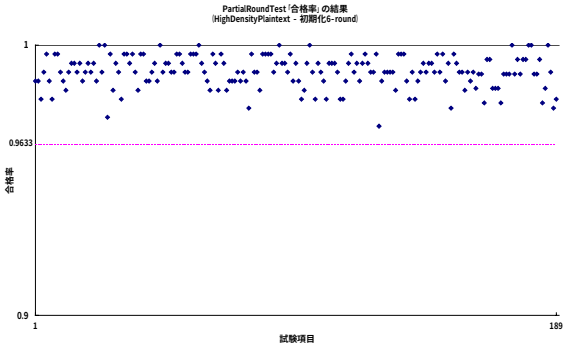

図 A8-6 初期攪拌 6 回

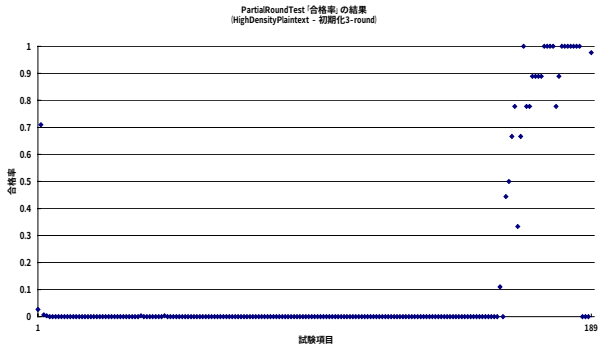

図 A8-3 初期攪拌 3 回

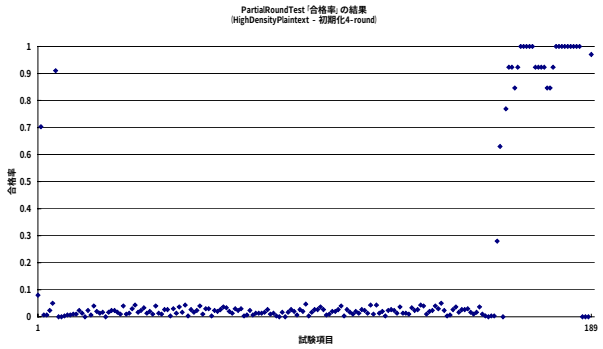

図 A8-4 初期攪拌 4 回

A9. Partial Round Test

Key Avalanche(**「分布」出力**)

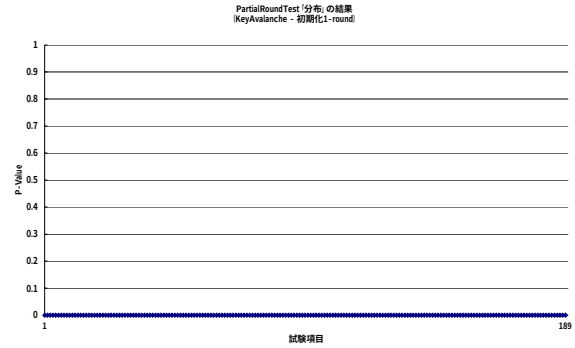

図 A9-1 初期攪拌 1 回

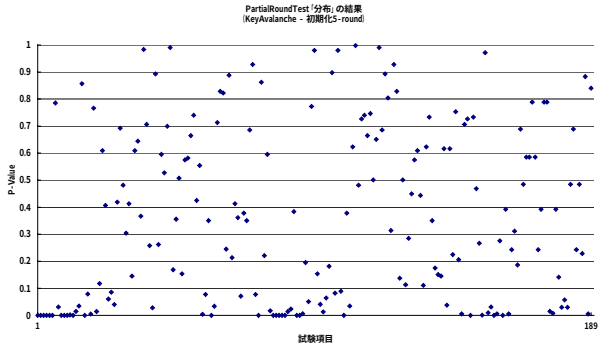

図 A9-5 初期攪拌 5 回

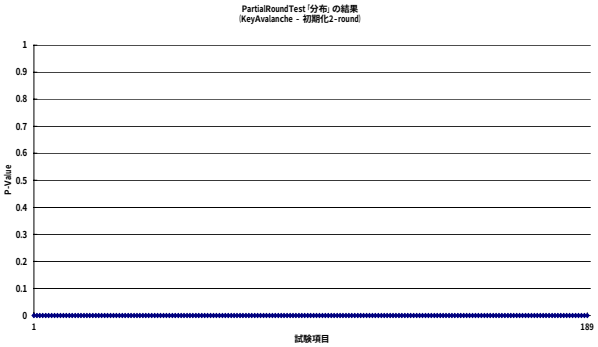

図 A9-2 初期攪拌 2 回

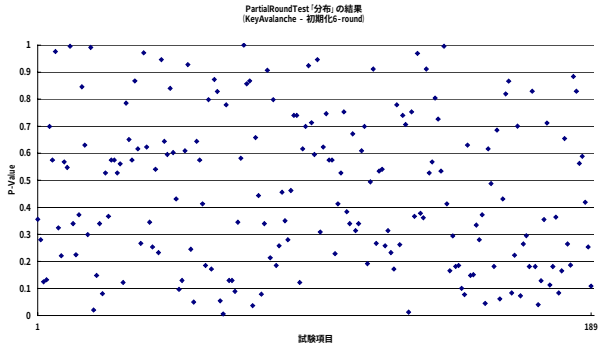

図 A9-6 初期攪拌 6 回

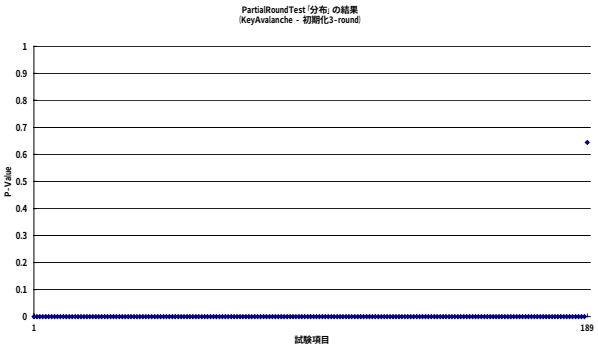

図 A9-3 初期攪拌 3 回

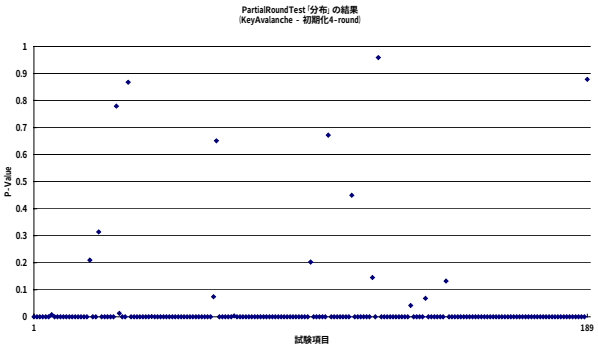

図 A9-4 初期攪拌 4 回

A10. Partial Round Test

Key Avalanche (**「合格率」出力**)

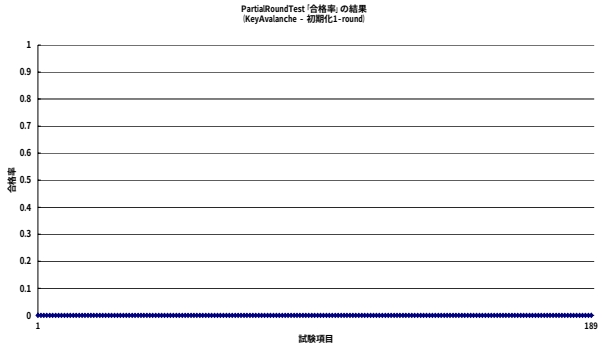

図 A10-1 初期攪拌 1 回

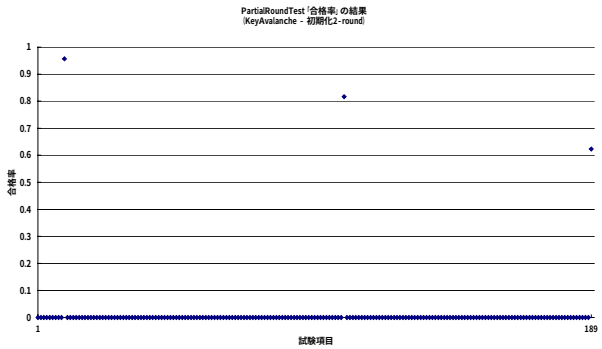

図 A10-2 初期攪拌 2 回

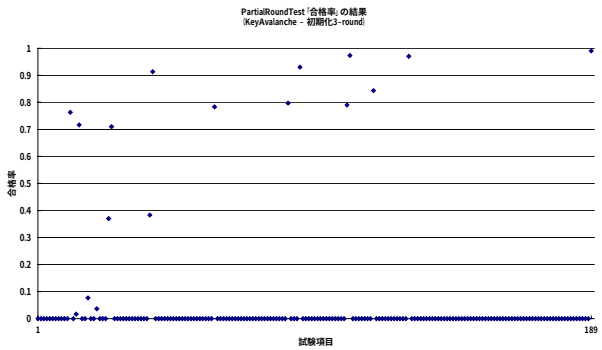

図 A10-3 初期攪拌 3 回

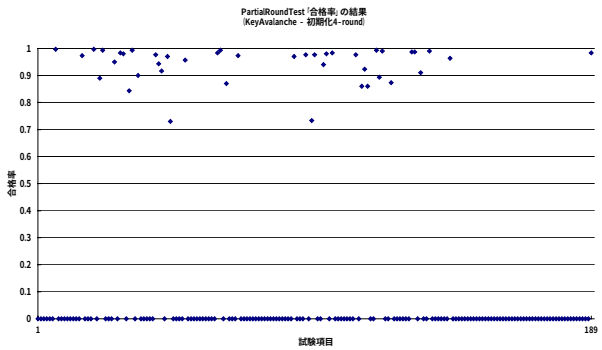

図 A10-4 初期攪拌 4 回

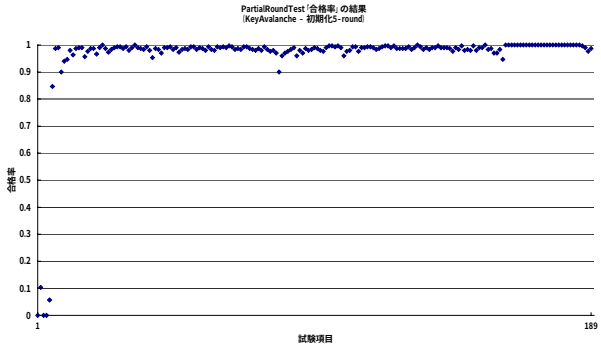

図 A10-5 初期攪拌 5 回

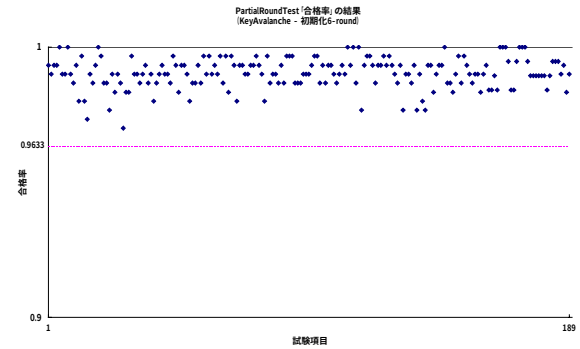

図 A10-6 初期攪拌 6 回

A11. Partial Round Test

Plaintext Avalanche(**「分布」出力**)

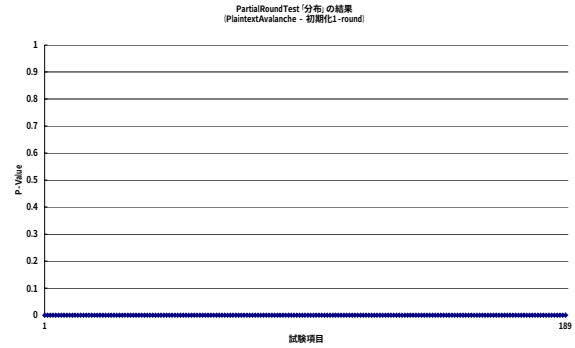

図 A11-1 初期攪拌 1 回

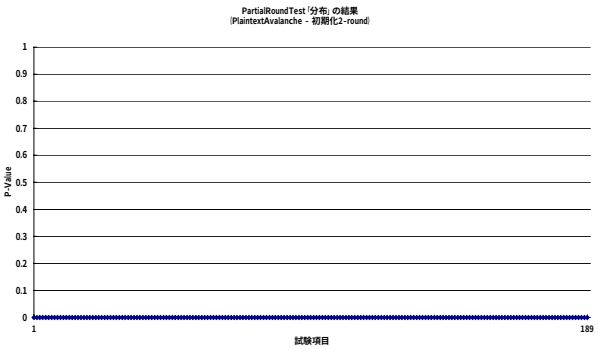

図 A11-2 初期攪拌 2 回

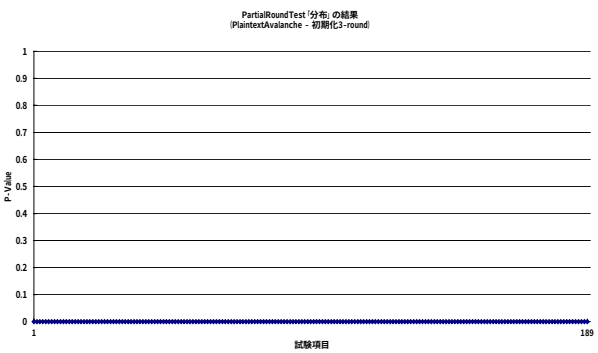

図 A11-3 初期攪拌 3 回

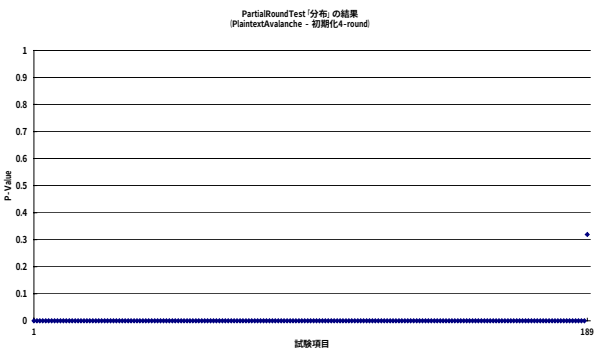

図 A11-4 初期攪拌 4 回

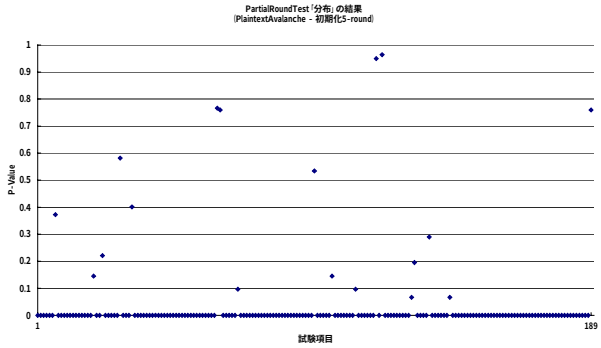

図 A11-5 初期攪拌 5 回

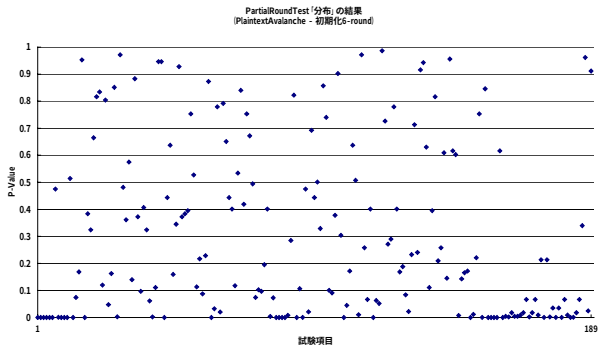

図 A11-6 初期攪拌 6 回

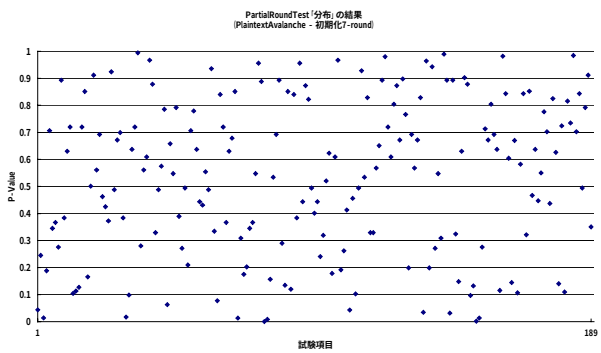

図 A11-7 初期攪拌 7 回

A12. Partial Round Test

Plaintext Avalanche (**「合格率」出力**)

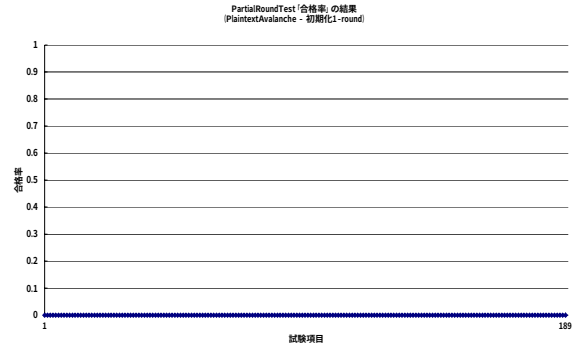

図 A12-1 初期攪拌 1 回

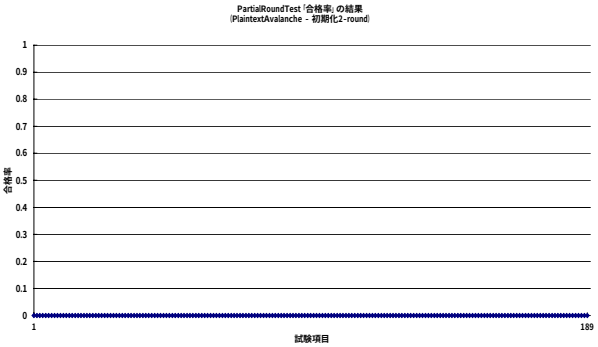

図 A12-2 初期攪拌 2 回

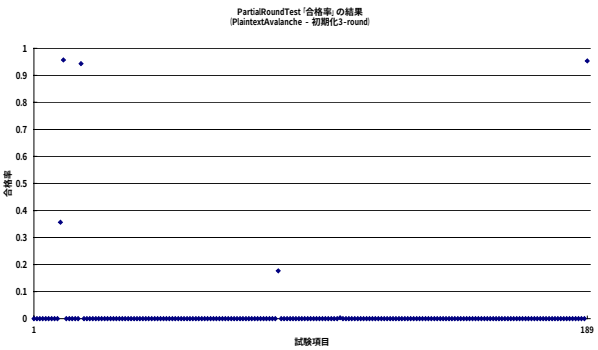

図 A12-3 初期攪拌 3 回

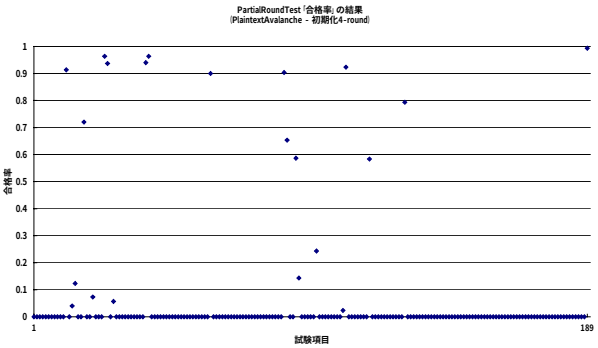

図 A12-4 初期攪拌 4 回

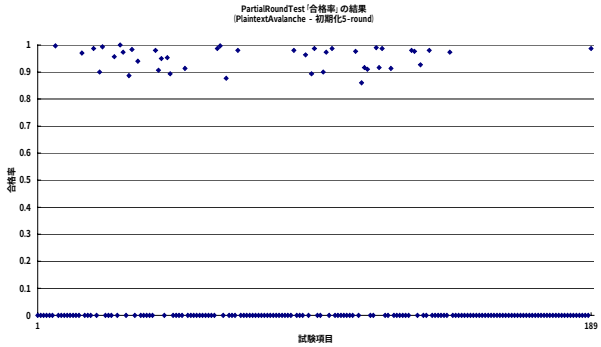

図 A12-5 初期攪拌 5 回

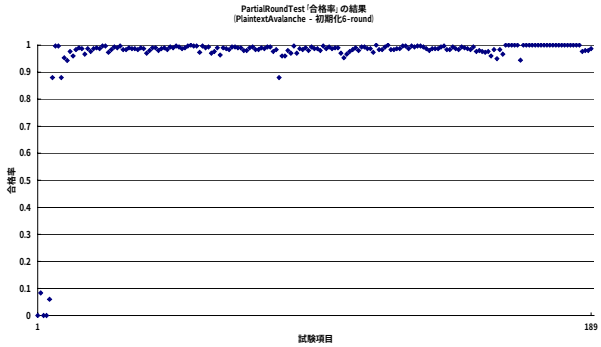

図 A12-6 初期攪拌 6 回

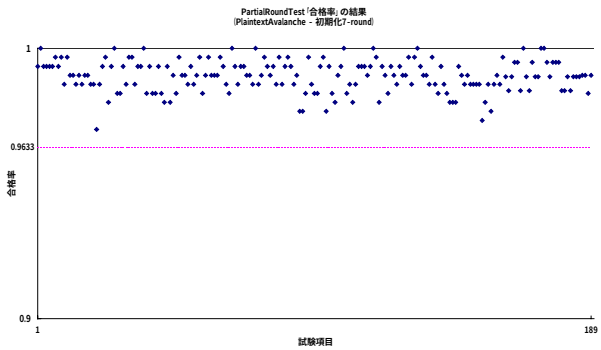

図 A12-7 初期攪拌 7 回

A13. Partial Round Test

Key/Ciphertext Correlation(**「分布」出力**)

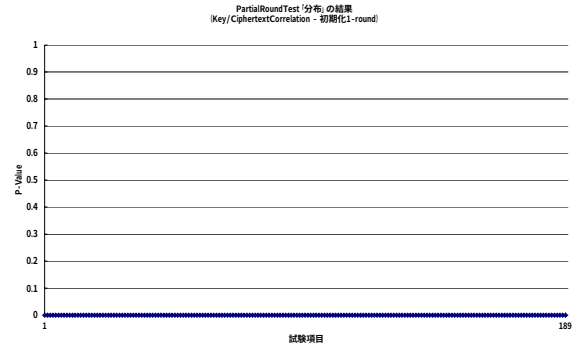

図 A13-1 初期攪拌 1 回

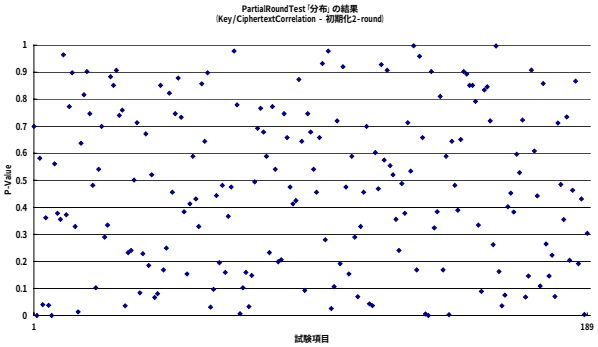

図 A13-2 初期攪拌 2 回

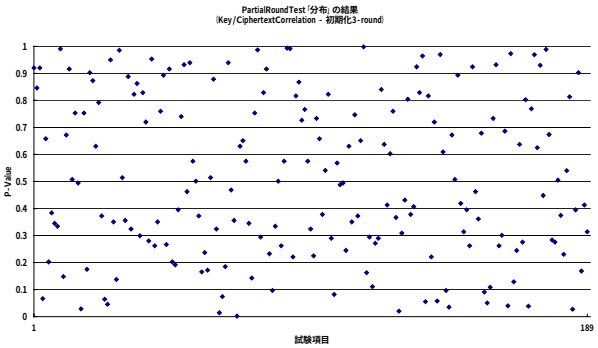

図 A13-3 初期攪拌 3 回

A14. Partial Round Test

Key/Ciphertext Correlation (**「合格率」出力**)

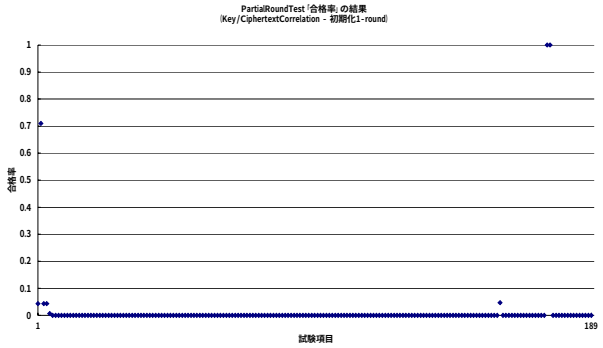

図 A14-1 初期攪拌 1 回

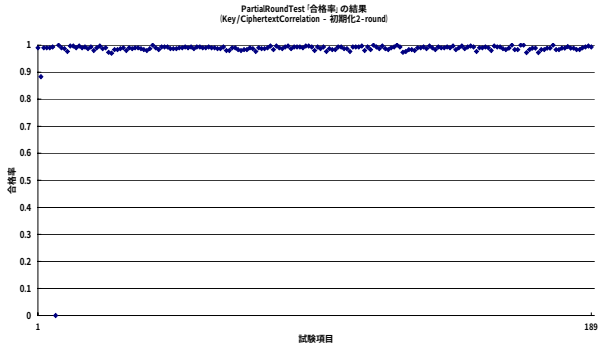

図 A14-2 初期攪拌 2 回

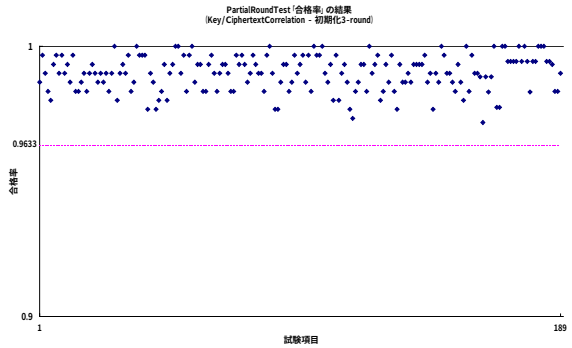

図 A14-3 初期攪拌 3 回

A15. Partial Round Test

Plaintext/Ciphertext Correlation (**「分布」出力**)

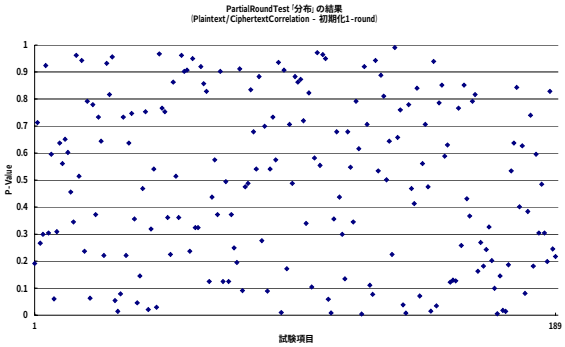

図 A15-1 初期攪拌 1 回

A16. Partial Round Test

Plaintext/Ciphertext Correlation (**「合格率」出力**)

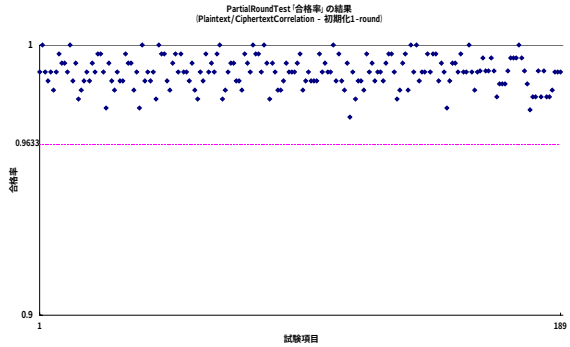

図 A16-1 初期攪拌 1 回