バーナム暗号に用いる疑似乱数生成アルゴリズムの比較

1090302　青野　裕太　【 福本研究室 】

1　はじめに

ネットワークに接続された環境では，個人情報などの重要な情報は盗聴の危険に曝されている．そのためAES や RSA などの暗号方式を用いて安全な通信を提供している [1]．暗号方式の一つにバーナム暗号があり，真性乱数を使い捨ての鍵として用い，鍵の秘匿により解読不可能が証明されている [2]．しかし，鍵となる真性乱数は，熱雑音などの物理乱数を元に生成するため，ソフトウェアのみの環境では生成できず利便性に問題がある．利便性を重視するとソフトウェアで生成可能な疑似乱数の利用が考えられるが，すべての疑似乱数生成アルゴリズムが真性乱数のようなランダム性を持つ乱数を生成できるとは限らない．そこで，本研究では，バーナム暗号へ適用可能なランダム性を持つ疑似乱数を得るために既存の疑似乱数生成アルゴリズムの比較を行う．

2　バーナム暗号

バーナム暗号は平文と鍵の各ビットの排他的論理和を取ることで暗号化を行う方式である．この方式は，正しい鍵を用いて復号しない限り平文の候補しか得られないため，鍵が盗聴者に知られなければ正しい情報が漏洩する可能性は極めて少ない．そのため鍵として利用される乱数にはランダム性が要求される．ランダム性とは生成された乱数列に規則性がなく，生成される乱数を予測できない予測不可能性のことを指す．しかし，疑似乱数は決定性アルゴリズムにより生成されるため，予測不可能性を満たすことは厳しく，いくつかの評価尺度を組合せることで同程度の安全性を持つと考えられ，疑似乱数を用いたバーナム暗号を実現できる可能性がある．

3　疑似乱数生成アルゴリズムの比較

本研究では，疑似乱数生成法として多く利用される線形合同法 (LCG)，高速生成可能な線形フィードバックシフトレジスタ (LFSR)，演算は複雑であるが長周期であるメルセンヌ・ツイスタ (MT) および XOR とビットシフト演算のみで構成される XorShift の 4 つのアルゴリズムを対象に比較を行う．予測不可能性の代用となる評価尺度は複数あるが，ここではバランス性の観点から比較を行う．バランス性は 0,1 が等頻度で出力される性質であり，バランス性が低いと生成される乱数に偏りが生じる．

3.1　比較方法

それぞれのアルゴリズムで生成された疑似乱数を対象にバランス性について比較を行う．各アルゴリズムにより 1024bit の乱数を生成し，2000 組の疑似乱数を理論値と比較し最大誤差と誤差の平均値を求める．ここでは 0,1 が等確率で出現する場合の 0,1 の個数を理論値という．また，実際に疑似乱数をバーナム暗号の鍵として適用し，暗号文と理論値との平均の誤差を求める．暗号化に用いる平文は，固定する場合と変更する場合に分け，変更する場合は rand() 関数から 0,1 を生成し平文とする．鍵は暗号化ごとに交換するものとして，それぞれの理論値と誤差の平均値を求める．

表 1　最大誤差と平均誤差

	最大誤差	平均誤差
LCG	43	0.7435
LFSR	53	0.7110
MT	60	0.1775
XorShift	56	0.8170

表 2　バーナム暗号へ適用したときの平均誤差

	平文変更なし	平文変更あり
LCG	0.0235	0.4265
LFSR	0.4930	0.3090
MT	0.2415	0.0065
XorShift	0.0250	0.0955

3.2　比較結果

疑似乱数の理論値と実測値の誤差との誤差の平均を表 1 に示す．MT が最小であり比較対象のアルゴリズム中では，最もバランス性が高い．平文を変更する場合としない場合に分け，バーナム暗号に適用した場合の暗号文の平均誤差を表 2 に示す．バーナム暗号に適用した場合，平文が変更された場合に MT の平均誤差が他よりも大きく低下していることが分かる．つまり，入力に関わらず安定してバランス性を保っており，MT が 4 つのアルゴリズムの中で最もバランス性が高いことを確認できる．

4　まとめ

本研究では 4 つの疑似乱数生成アルゴリズムを適用したバーナム暗号のバランス性について比較を行った．その結果，MT が対象アルゴリズムの中で最もバランス性が高いことを確認した．今後は他の評価尺度についても比較を行う必要がある．

参考文献

[1] 岡本栄司，“暗号理論入門, ” 共立出版株式会社，p.62, 1993.

[2] 若林宏，“図解入門よくわかる最新暗号技術の基本と仕組み, ” 株式会社秀和システム，p.47，2005.