3E4-2

Feistel 構造で利用するセル・オートマトンを用いたラウンド関数Fの計量的安全性と擬似乱数性の相関の検証

Inspection of the correlation between quantitative safety and pseudo randomness in round function F including the dynamics of cellular automaton used in Feistel structure

吉野　博貴[*1]
Hiroki Yoshino

井上　聡[*1*2]
Satoru Inoue

[*1] 埼玉工業大学大学院
Graduate School of Engineering, Saitama Institute of Technology

[*2] 埼玉工業大学
Saitama Institute of Technology

Dynamics of the game of life change variously and intricately though it is driven by quite simple. We previously proposed the encryption method using this property, but inspection for the safety in terms of pseudo randomness was insufficient. Therefore in this study, we inspect the pseudo random number characteristics and its associated statistical safety of our proposed system .

1. はじめに

セル・オートマトンの一例であるライフゲームは，1970 年にイギリスの数学者 John Horton Conway によって考案されたシミュレーションゲームである[Berlekamp 1982]. ゲームのフィールドは 2 次元の格子状のセルと呼ばれるマス目で構成されており、各セルは生(1)または死(0)のどちらかの状態を持つ. ある 1 つのセルに注目したとき，そのセルの次世代の状態は，次の 3 つのルールによって決定される.

・自身が死の状態のとき，周囲に生のセルが 3 つ以上あるなら次の世代では生となる.

・自身が生の状態のとき，周囲に生のセルが 2～3 つあるなら次世代でも生となる.

・上位以外では、次世代では死となる.

ライフゲームには，「簡単なルールで更新するにも拘らず，多様に変化していく」という性質がある. これまでの研究ではこの性質を利用した暗号化方法を提案したが、擬似乱数生成器としての評価が安全面の上で不十分であった. 本研究では暗号化時における擬似乱数性と，それに付随する統計量的安全性において評価・検証を行う.

2. 暗号化システムについて

2.1 暗号化アルゴリズムの概要

前研究で提案された暗号化アルゴリズムのブロックダイアグラムを図 1 に示す. このシステムは鍵スケジュール部とデータ撹拌部に分かれている. 鍵スケジュール部では暗号化処理に先立ち，鍵を拡張しサブ鍵の生成を行う. ここで生成したサブ鍵は暗号化処理の際に使用する. データ撹拌部では，サブ鍵を使って平文を暗号文に変換する処理を行う. 具体的には，入力データを左右半分に分け，右半分と鍵スケジュール部で生成したサブ鍵をF関数に通す. F関数の出力と左半分のXORを行う. この操作を左右入れ替えながら 10 回繰り返すことで暗号化処理が終了する. 復号するときは，まったく逆の操作を行う. なお，F関数については 2.3 で記述するが，入力された右半分とサブ鍵のデータを混ぜ合わせる処理を行っている. このように，2 分割したデータを交互にF関数を通過させる処理の方法を Feistel 構造という.

連絡先：吉野　博貴，埼玉工業大学大学院，埼玉県深谷市普済寺 1690 埼玉工業大学大学院，m9008nhn@sit.ac.jp

2.2 鍵スケジュール部

鍵スケジュール部では，128bit の鍵をもとにして 64bit のサブ鍵を 10 個生成する. 鍵データを 16×8 のライフゲームとして表現し，これをライフゲームのルールに従って 10 ステップ分更新する. このとき，1 ステップ更新するごとに以下の操作を行い，サブ鍵を作っていく. ライフゲームを中央で半分に区切り，8×8 の平面を 2 つ作る. この 2 つの平面の排他的論理和をとった結果をサブ鍵として暗号化処理に用いる.

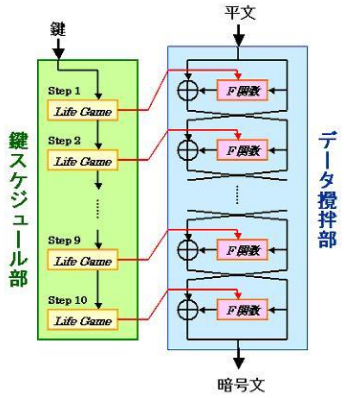

図 1 暗号化システムの全体像

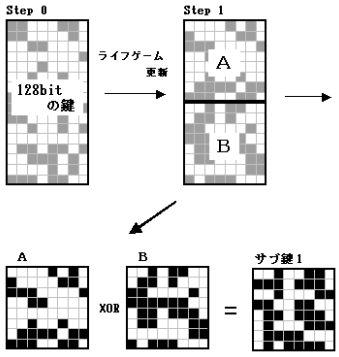

図 2 鍵スケジュール部の流れ

2.3 F関数

F関数は，データの攪拌を行う暗号化処理の中核となる部分である．入力データの右半分とラウンドごとのサブ鍵との排他的論理和をとり，それをライフゲームのルールに従って 1 ステップ更新する．これを F 関数の出力とし，入力データの左半分と排他的論理和演算を行う(図 3)．

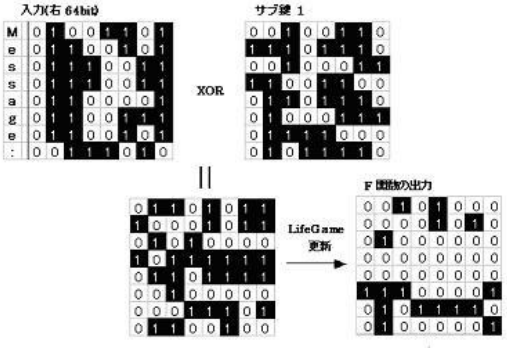

図 3 F関数の処理

3. アルゴリズム安全性の検証について

3.1 擬似乱数生成器としての評価

Feistel 構造をしている暗号方式の場合，F 関数を擬似乱数生成器と見なして評価することができる．暗号理論における擬似乱数とは，多項式時間の計算機が真の乱数と識別不能な列に含まれる数のことである．その列を生成する機器を擬似乱数生成器という．暗号用の擬似乱数に求められる条件は無作為性「統計的な偏りがなく，でたらめな数列になっているという性質」と予測不可能性「乱数列の任意の一部から他のビットを予測できないという性質」の 2 つである．真の乱数は上記の 2 つの条件を満たしているので，真の乱数と区別のできない擬似乱数が高い強度をもっていると言える[岡本 2002]．これまでの研究で F 関数を擬似乱数生成器と見なしての評価で，F 関数の出力が 0 に偏る現象が検出された．原因は F 関数内の主処理にライフゲームを利用していることにあると考えられる．ライフゲームの規則は「周囲の環境が過疎状態でも過密状態でも生き残ることはできない」という考えのもと設定されている．よって，ビットがバランスしている状態でライフゲームの更新を行うと場が過密状態であるために，次の世代で多くのセルが死亡してしまうのである[井上 2009]．今研究では，それを解消するためのアルゴリズムの拡張を課題とし，ライフゲームとは違うセル・オートマトンの条件を全通り検索する．条件ごとに平文の右半分 64bit と上記におけるF関数の処理の直後 64bit の変化量に着目し，その中でも変化量の高い条件を検出する．さらに，その中から下記の統計量的安全性に含まれる条件を絞り出す．

3.2 統計量的安全性

共通鍵ブロック暗号の安全性は，特定の攻撃法によって解読に必要な平文と暗号文のペア数や計算量によって評価する方法と，入出力相関などの統計量によって評価する方法に分かれる．統計量による評価は必ずしも具体的な攻撃法に直結するとは限らないということもあり，最近では計算量による評価が重要視されている．しかし，差分攻撃法や線形攻撃法に代表される攻撃には，データの攪拌の偏り(高い確率で成立する相関関係)を解読の糸口とするものも多く，これらの攻撃に対する安全性の指標として統計量的安全性は有効であると言える．そこで，統計量的安全性の検証として，アバランシュ特性の評価を行った．「入力の一部が変化したことにより F 関数の出力の一部が変化し，その変化が次のラウンドの出力に，より大きな変化をもたらす．」この現象をアバランシュ効果という．アバランシュ性の評価では，入力を 1bit ずつ反転させ，出力のどのビットに影響が出るかを調べる．安全性の観点では，入力に 1bit の変化を与えたとき，各出力ビットは 50%の確率で変化することが望ましい．各出力ビットの変化する確率が 50%から離れている場合，鍵または平文の小さな変化が暗号文に小さな変化しか与えないことになり，攻撃者が探索する鍵空間または平文空間の減少につながる危険性がある[辻井 2002]．

3.3 出現率

図 4 は擬似乱数生成器としての評価が高く，なおかつ統計量的安全性を保持したセル・オートマトンにおける条件の発現率を示したものである．なお，グラフの横軸は誕生，生存するために必要な周囲の生存セル数で，縦軸はそれが出現する割合である．

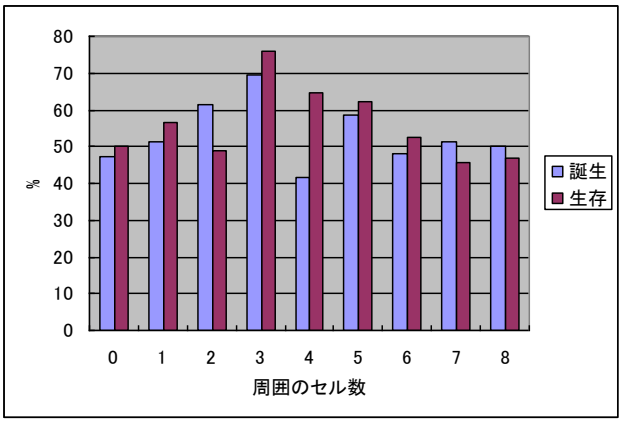

図 4 条件の出現率

4. まとめと考察

前記の図 4 から，本アルゴリズムの安全性に関して，高い確率でセル・オートマトンにおける誕生の条件に含まれる 1 ステップ前の周囲のセル数が 2, 3, 5 つのとき，また同様に生存の条件に含まれる周囲のセル数が 3, 4, 5 つのときの変化量が安定していることが見て取れる．しかし今研究では，平文の右半分 64bit とF関数の処理直後 64bit の変化量にしか着目していないため，完全に擬似乱数性と統計量的安全性を両立した条件を絞り出すには不足があると考えられる．3.1 より，擬似乱数生成器としての評価はF関数に着目することで評価値が得られるが，統計量的安全性に関しては，入力に対する出力であるので，相関を見るためにはF関数と，入力に対する出力の双方に関して着目する必要があるといえる．

参考文献

[Berlekamp 1982] Elwyn Berlekamp, John Conway and Richard Guy : Winning Ways for your Mathematical Plays , Academic Press ,1982.

[辻井 2002] 辻井 重男・岡本 栄司: 暗号のすべて～ユビキタス社会の暗号技術～, 電波新聞社 , 2002.

[岡本 2002] 岡本 栄司:「暗号理論入門［第 2 版］」, 共立出版株式会社 , 2002.

[井上 2009] 井上 聡 : セルオートマトンの複雑性を用いた Feistel 構造をもつブロック暗号アルゴリズムの検証, 第 23 回人工知能学会全国大会講演要旨集 , 2009.