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

The study of block cipher algorithm with Feistel structure using the complexity of cellular automata

井上 聡[*1]
Satoru Inoue

[*1] 埼玉工業大学 工学部 情報システム学科
Department of Information Systems, Faculty of Engineering, Saitama Inst. of Tech.

The Game of Life which is well-known example of cellular automata shows the remarkable complex but fascinated dynamics in spite of its quite simple rule. In our previous study, we proposed the file encryption method based on the complex dynamics of the cellular automata (Game of Life) and showed it can completely encrypt and decrypt several kinds of file regardless its type. In our recent study, we analyze its dynamics quantitatively and statistically to ensure the safety and robustness of our proposed model.

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もつ. 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 つあるなら次世代では生となる.

・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.

・上記以外なら, 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. 本研究では, この性質を利用する暗号化方法を提案する.

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

本研究で提案する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攪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. データ攪拌部では, 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, 全く逆の操作を行う. なお, F 関数については 2.3 で述べるが, 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式を Feistel 構造という.

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.

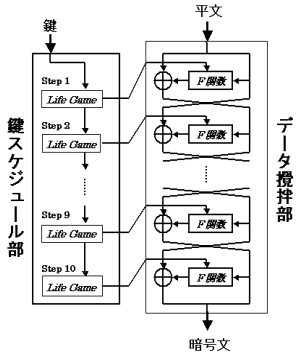

図1. 暗号化システムの全体像

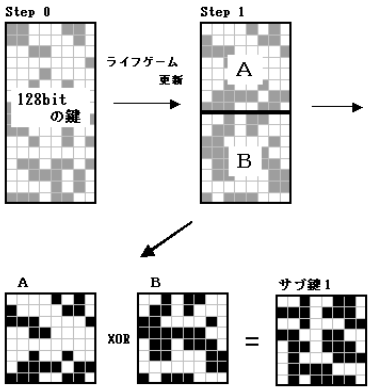

図 2. 鍵スケジュール部の流れ

連絡先:井上 聡, 埼玉工業大学, 埼玉県深谷市普済寺 1690, inoue@sit.ac.jp

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．

3. ファイルを暗号化した結果について

本研究で提案している暗号化方法は，ファイルのバイナリデータを直接暗号化しているため暗号化可能なファイルの種類は特に問わない．ここではビットマップファイルを暗号化した結果を示す．また，この方法での暗号化はファイルヘッダ部すら暗号化されているため，元ファイルの種別等の基礎データも秘匿される．ここではビットマップデータ部分がどのように攪拌されているかを示すため，あえてファイルヘッダは暗号化前のものと書き換えて表示している．

3.1 ビットマップファイルを暗号化した結果について

ここでは本アルゴリズムを用いて，ビットマップファイルを暗号化した例を示す．図 3(左)は暗号化前のファイルで，図 3(右)が暗号化後のファイルである．図 3 が示すように，双方を比較すると暗号化された画像から元のファイルの画像を推測することは不可能といえる．また暗号化と逆向きの処理を施すことにより，暗号化されたデータを元の通り復元できることを確認した[井上 2008].

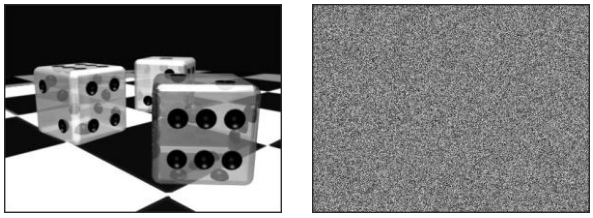

図 3. ビットマップファイルの暗号化例

4. アルゴリズム安全性の検証について

4.1 統計量的安全性の検証

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].

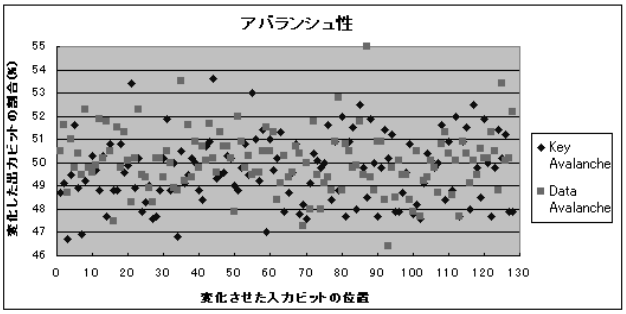

図 4. 本アルゴリズムのアバランシュ性の評価

図 4 は本研究で提案した暗号アルゴリズムのアバランシュ性を示したものである．横軸は変化させた入力ビットの位置を示し，縦軸は変化した出力ビットの割合を示している．出力の 50%(128bit の内の 64bit)が変化したときが最もランダム性が強く，50%から離れるほどランダム性は弱まり静的な状態に陥っていくことになる．同図より，変化させた入力ビットの位置によって変化した出力ビットの割合は同一ではないものの，平文・鍵どちらを変化させた場合も 50%付近に分布していることがわかる．この結果より，アバランシュ性の評価では解読に利用されるようなデータの偏りは発見できなかったことになる．

5. まとめと考察

本研究ではライフゲームを利用したファイル暗号化システムを提案，構築した．そして暗号化に利用した正規鍵を利用すれば暗号-復号が可能である可逆性があることを確認した．計量的，統計的安全性について多角的方面から評価を行った．評価方法によっては安全性が認められる部分(アバランシュ性)も存在しているが，擬似乱数生成器としての評価を行った結果では，ビットの偏在化が確認されており，暗号の脆弱性につながりそうな部分も確認されている．これらを解消するアルゴリズムの拡張がこれからの課題といえよう．

参考文献

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

[Poundstone 1987] William Poundstone :Recursive Universe, Oxford Paperbacks , 1987.

[井上 2008] 井上 聡：ライフゲームの性質を利用したファイルの暗号化に関する研究，第 22 回人工知能学会全国大会講演要旨集 , 2008.

[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.