講演番号： 24

# 2 次元セル・オートマトンを利用した暗号

A－7

Cryptosystem by Two-dimensional Cellular Automaton

佐藤哲平† 安細 勉† 蓬莱 尚幸†

Teppei SATO† Tsutomu ANSAI†† Hisayuki HOURAI†

† 茨城工業高等専門学校 電子情報工学科

† Electronic and Computer Engineering, National Institute of Technology, Ibaraki College

†† 茨城工業高等専門学校 電気電子システム工学科

††Electrical and Electronic System Engineering, National Institute of Technology, Ibaraki College

## 1. はじめに

セル・オートマトンの一種であるライフゲームは、単純なルールで次世代が決定されるにもかかわらず、多様で複雑な振る舞いをすることから、この性質をスクランブル処理に利用する暗号の研究が行われている。(1)

しかし、ライフゲームはセル・オートマトンの 1 つのルールに過ぎず、暗号化に最も適したルールであるとは限らない。そこで、セル・オートマトンのルールを変更した場合の暗号の安全性はどのように変化するか、2 値から 3 値のセル・オートマトンに変えた場合はどうか、など様々な発展が考えられる。

本研究では、セル・オートマトンのルールを変更した場合の安全性の変化を検証し、考察する。

## 2. 課題

2-1. セル・オートマトンのプログラムの作成

本研究では、セル・オートマトンのルールを変更して暗号の安全性をテストするため、任意のルールで動作するセル・オートマトンのプログラムが必要である。

2-2. 暗号化プログラムの作成

今回の暗号は Feistel 構造を用いたブロック暗号であり、F 関数とラウンド鍵の生成にセル・オートマトンを用いる。

## 3. 解決方法

3-1. セル・オートマトンのプログラムの作成

高速化のため Bitboard という手法を用いた。(2) Bitboard により、シフト演算と論理演算を用いることで、ほとんど条件分岐を使用することなく、すべてのセルの次世代の状態を一度に求める事が可能となった。暗号化においては、変化が全体に波及することが望ましいため、セル・オートマトンはトーラスになっている。

3-2. 暗号化プログラムの作成

本研究では、Feistel 構造のブロック暗号で暗号化するプログラムを作成した。

3-2-1. ラウンド鍵の生成

暗号化プログラムの内部では、鍵と同じサイズの決まったビット列を XOR したものをラウンド鍵生成に使う。

3-2-2. F 関数

そのラウンドのラウンド鍵を、XOR したあと、セル・オートマトンとして 1 回更新する。

## 4. 評価方法

4-1. 0、1 の数え上げ

ランダムに生成した平文を暗号化した暗号文の 0 と 1 それぞれの数を集計し、暗号文のビットに偏りがないかを検証する。

4-2. ポーカー検定

暗号文のビット列を 4 ビットずつで区切った数列をポーカー検定にかける。

4-3. 入力の差分が出力に与える影響の検証

微小な差分のある 2 つの平文を同じ鍵で暗号化し、それぞれの出力の変化した場所としなかった場所を観察する。

## 5. 評価

まず、本研究で評価したのはライフゲームを含めた 5 種類のルールである。

5-1. 0、1 の数え上げ

実験した 5 種類のルール全てにおいて、0、1 の数は概ね同じであり、有意水準 5%のカイ 2 乗検定に合格した。

5-2. ポーカー検定

実験した 5 種類のルール全てにおいて、カイ 2 乗値は若干の差はあるものの、有意水準 5%のカイ 2 乗検定に合格した。

5-3. 入力の差分が出力に与える影響の検証

実験した 5 種類のルール全てにおいて、入力の差分の場所と出力の変化した場所には、2 つのゆがんだ円の形の範囲で変化するという法則性が見られた。ただし、おおよその変化する範囲が特定出来るだけで、平文や鍵を変えると同じ差分でも違った変化をするため、ビット単位ではどこが変化するか特定することはできない。また、それぞれのルールで変化する位置はほとんど同じであったが、範囲の大きさには違いが見られた。実験した 5 種類のルールのうち、ライフゲームを用いた暗号化の時の変化の範囲が最も小さくなっていた。

## 6. 考察

5-1、5-2 の結果から、セル・オートマトンのルールを変更しても、暗号文のビット列はランダムであると言える。

また、5-3 の結果から、セル・オートマトンのルールを変更することで、暗号の安全性が変化していることが分かり、差分攻撃に対しては、ライフゲームよりも有効なルールがあることも発見された。

## 7. 結論

セル・オートマトンのルールを変更することで、暗号の安全性は変化することが分かり、ライフゲームよりも相対的に安全性の高いルールを発見することができた。

セル・オートマトンのルールは無限と言っていいほど大量にあるが、今回検証したのは 5 種類のみであったので、さらに安全性の高いルールを見つけること、また、3 値のセル・オートマトンを用いた場合の安全性の検証などが今後の課題として挙げられる。

## 参考文献

(1) 井上 聡(2009)『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』

(2) 『Bitboard 版ライフゲームの拡張 - Tosik の雑記』<http://d.hatena.ne.jp/tosik/20071120/1195495618>(2015/12/1 アクセス)