光セルラーオートマタによる高速暗号化手法

小尾　高史・山口　雅浩・大山　永昭

社会の高度情報化の進展とともに，ネットワークを介した情報通信におけるプライバシー保護の必要性が高まっており，通信路の安全性を確保することがきわめて重要になっている．さらに今後，超高速ネットワークシステムの整備が進むことが予想されることから，高速かつ安全な暗号技術の実現が必要とされている．筆者らはこれまで並列処理に適した暗号化手法として toggle cellular automata（TCA）に基づくブロック暗号化手法を提案し，光並列演算による高速処理の可能性を検討してきた[1,2]．本稿ではこの暗号化手法の原理について述べ，画像処理装置を用いた高速演算手法と実験結果を紹介する．

1. TCA に基づく暗号化手法[3,4]

3 次元 TCA に基づく暗号化[4]では，非線形で不可逆な論理演算を行う関数により順次データを更新し，その結果と平文との排他的論理和をとることによって高い安全性をもつ暗号化を実現している．具体的には，論理演算を行う非線形関数を Φ として，3 次元 (i,j,k) 空間に離散的に並べられたバイナリーデータ列に対し，3 次元 TCA の定義式

$$a_{i,j,k}^{t+1}=\Phi(a_{i,j,k}^{t}, a_{i-1,j,k}^{t}, a_{i+1,j,k}^{t}, a_{i,j-1,k}^{t}, a_{i,j+1,k}^{t}, a_{i,j,k-1}^{t}) \quad XOR\ a_{i,j,k+1}^{t} \qquad (1)$$

を復号化に適用し，またその逆変換

$$a_{i,j,k+1}^{t}=\Phi(a_{i,j,k}^{t}, a_{i-1,j,k}^{t}, a_{i+1,j,k}^{t}, a_{i,j-1,k}^{t}, a_{i,j+1,k}^{t}, a_{i,j,k-1}^{t}) \quad XOR\ a_{i,j,k}^{t+1} \qquad (2)$$

を暗号化に適用する．このとき，図 1 に示すように，隣接項間の論理演算結果を出力する関数 Φ（Key 1）および Link ビットと呼ばれる端部項演算用ビット列（Key 2）が暗号の鍵となる．3 次元 TCA は，高い強度をもつ暗号化を容易に実現することができるとともに，2 次元的なデータの同時更新が可能であるため，並列処理に適したアルゴリズムである．

2. 画像処理装置による暗号化/復号化

ここでは画像演算を 2 次元一括処理できる画像処理装置を用いて，3 次元 TCA による暗号化を行う方法を述べる．

東京工業大学像情報工学研究施設（〒226-8503 横浜市緑区長津田町 4259）
E-mail: obi@isl.titech.ac.jp

まず更新のルールとなる関数 Φ の演算を，画像処理装置がもつ積和演算と閾値処理（look up table: LUT）機能により実現する．式（2）の $a_{i,j,k}^{t}$ に対してその項を含めた近接項列ベクトル $\boldsymbol{P}_{i,j,k}=(a_{i,j,k}^{t}, a_{i,j-1,k}^{t}, a_{i-1,j,k}^{t}, a_{i,j+1,k}^{t}, a_{i+1,j,k}^{t})^{\mathrm{T}}$ と荷重係数行ベクトル $\boldsymbol{W}=(W_{\mathrm{C}}, W_{\mathrm{N}}, W_{\mathrm{W}}, W_{\mathrm{S}}, W_{\mathrm{E}})$ を図 2 に示すように定義すると，第 k 番目の画像（Image k）と荷重係数の座標 (i,j,k) における積和演算結果 $S_{i,j,k}$ は以下のように表せる．

$$S_{i,j,k}=\boldsymbol{W}\cdot\boldsymbol{P}_{i,j,k} \qquad (3)$$

例えば，$\boldsymbol{W}=(1,2,4,8,16)$ とすれば，$S_{i,j,k}$ は 0〜31 の中の

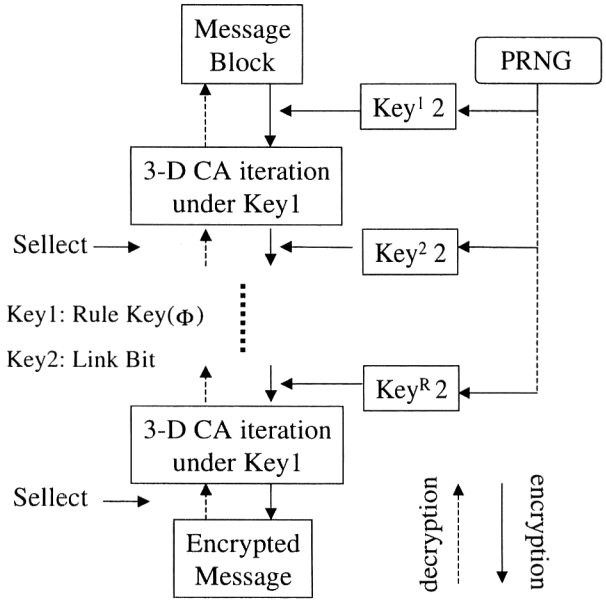

図 1　3 次元 TCA に基づく暗号化．

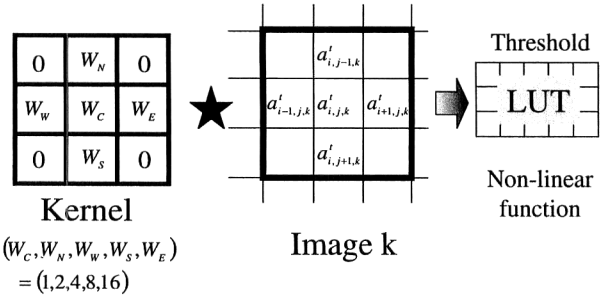

図 2　画像処理装置を用いた関数 Φ の同一平面に存在する要素間の演算．

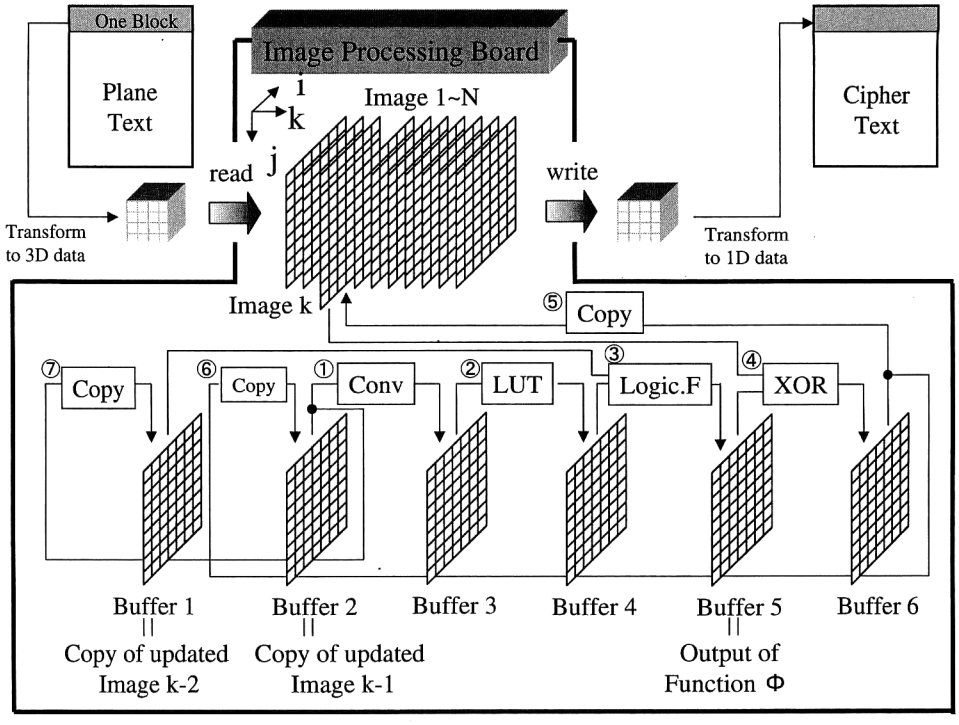

図3　画像処理装置を用いた暗号化.

表1　暗号化処理速度の比較.

	PC (PII-300)	画像処理ボード
暗号化	167 [kbit/s]	945 [kbits/s]
複号化	144 [kbit/s]	940 [kbits/s]

ある1つの値となる．このため，$S_{i,j,k}$ をLUTを用いて閾値処理することで，同一平面に存在する要素間の演算が可能となる．さらに，演算結果と第 $k-1$ 面上の項との論理演算を行い，関 Φ の値を得る．暗号化処理は，この値と第 $k+1$ 面上の平文 $a^{t+1}_{i,j,k+1}$ の間で排他的論理和を計算し，さらにこれらの処理を複数回繰り返すことにより行われる．このように3次元TCAに基づく暗号化は，平面ごとにデータの更新が可能であるため，ラインごとの更新となる2次元TCA[3]の場合と比較して並列度が向上する．一方，復号化は，関数 Φ の演算を同様の手順で行い，toggleビットである $a^{t}_{i,j,k+1}$ との排他的論理和をとることで $a^{t+1}_{i,j,k}$ を出力する．このとき，前面の更新履歴を必要としないため，3次元空間内のすべてのビットを同時に更新処理することができる．

3. 実　　験

本手法の有効性を確認するために，日立高速画像処理ボード（IP5000シリーズ）を用いて，図3に示す方法により実験を行った[5]．この画像処理ボードは，最大40面のデータを同時に書き込むことのできる演算用メモリーをもち，画像間演算・積和演算・LUT等をパイプライン処理によって高速に演算することが可能である．

反復処理の回数を16回として暗号化を行った結果，表1に示すようにコンピューターによる暗号化処理と比較し，高速な処理を実現できることが明らかになった．

本稿では，2次元の一括処理を用いて3次元TCAに基づくblock暗号を行う手法を紹介し，画像処理装置を用いた実験により，その有効性を示した．今後，多値のCAを用いることや反復回数の削減等により高速化を図ることが課題である．

文　　献

1) 角田　貢，M. Madjarova，小尾高史，山口雅浩，大山永昭：“光学系を用いたVernam暗号”，光学，**27** (1998) 104-109.
2) M. Madjarova, M. Kakuta, M. Yamaguchi and N. Ohyama: “Optical implementation of the stream cipher based on the irreversible cellular automata algorithm,” Opt. Lett., **22** (1997) 1624-1626.
3) M. Madjarova, *et al.*: “Block cipher based on back-iteration of the 2-D cellular automata,” Proc. SPIE, **3228B** (1997) 377-387.
4) M. Madjarova, *et al.*: “Data encryption based on 3-D cellular automata block-cipher algorithm,” 第59回応用物理学学術講演会予稿集，16a-A-6 (1998).
5) 鈴木裕之，ほか：“画像処理装置を用いた3次元Cellular Automataに基づくBlock暗号”，*Optics Japan '98* (1998) 19aF09.

(1998年9月10日受理)