2003年日本オペレーションズ・リサーチ学会
春季研究発表会

標的問題を用いた暗号技術の研究

関西大学　＊桐山　明人　KIRIYAMA　Akito
01402374　関西大学　仲川　勇二　NAKAGAWA　Yuji

1．はじめに

本研究は，離散最適化問題の計算困難性を利用した暗号技術の提案，及び実行テストによる性能評価を目的としている．暗号化に利用するのは離散最適化問題の中でも目的関数に標的値を導入した標的問題である．

ここでは標的問題を解くための方法として，仲川により提案されたモジュラ法を用いた．モジュラ法は複数のモジュールに対し深測操作を行い，順に結合して決定空間を縮小していくというものである．モジュラ法は離散最適化問題を解くための方法として非常に有効である．また，本研究では複数制約問題を扱うが，これを解くために代理乗数を用いて複数制約を単一制約として計算する代理制約法を用いた．

2．標的問題

本研究で扱う暗号化方法は，その数学的背景として非線形かつ離散値をとる標的問題を使っている．標的問題は次のように定式化される．

$$\text{target: } f(x)=\sum_{i=1}^{n} f_i(x_i) \geq f^T \quad (1 \leq i \leq n)$$

$$\text{s.t.} \quad g_j(x)=\sum_{i=1}^{n} g_{ij}(x_i) \leq b_j \quad (1 \leq i \leq n, 1 \leq j \leq m)$$

ここで，f_i，g_{ij}はそれぞれx_iに関する目的関数と制約関数，f^Tは標的値，b_jは許容値を意味する．標的問題では全ての制約を満たし，かつ目的関数の値が標的値以上となる解を列挙する．

唯一の最適解を見つける場合と違い，f^Tを小さくしすぎると解集合が巨大なものになってしまうので注意が必要である．

3．暗号化方法

標的問題暗号では目的関数$f(x)$と制約関数$g_j(x)$ $(1 \leq j \leq m)$を暗号化のための共通鍵として送信者と受信者が保持する．この関数は具体的には変数の値に対応する関数の値を配列として表現したものである．なお，関数の値は$\mathbb{Z}_p$上の0を除く整数（pは素数）とする．（ここで$\mathbb{Z}_p$は$\bmod p$演算を導入した0以上$p-1$以下の整数の集合を表す．）暗号化の手順を以下に示す．

Step 1．平文ベクトル$x=(x_1,\ldots,x_n)$に変換用ビット列qを適用して変換し，入力ベクトル$x'=(x_1',\ldots,x_n')$を生成する．

Step 2．関数乗数r_f，$r_{g_j}(1 \leq j \leq m)$を1で初期化する．

Step 3.1 $\sum_{i=1}^{n}\left(f_i(x_i')\times r_f\right)$を計算し，$f^T$以上になるまで$r_f$を増加させる．$r_f \geq p$になったらStep 1に戻る．$f^T$以上になれば$f_i'(x_i') = f_i(x_i')\times r_f$とする．

Step 3.2 $\sum_{i=1}^{n}\left(g_{ij}(x_i')\times r_{g_j}\right)$を計算し，$b_j$以下になるまで$r_{g_j}$を増加させる．$r_{g_j} \geq p$になったならStep 1に戻る．$b_j$以下になれば$g_{ij}'(x_i') = g_{ij}(x_i')\times r_{g_j}$とする．

Step 4．$f'(\boldsymbol{x}') \geq f^T$，$g_j'(\boldsymbol{x}') \leq b_j$として標的問題を解き，整列した解集合の中での$\boldsymbol{x}'$の順番を$t$とする．

Step 5．変換用ビット列q，関数乗数r_f及び$r_{g_j}(1 \leq j \leq m)$，順番tを暗号文として送信する．

ただし，ここで演算子×は積をpで除した剰余を意味する．

f^T及びb_jは$1\times n$以上$(p-1)\times n$以下の範囲で決めておく．f^Tを大きく（b_jを小さく）設定すると，解集合を小さくできるがStep 3で計算をやり直す確率が高くなる．また解集合の大きさは，制約の数や変数の個数によっても当然変わってくる．解集合が大きくなりすぎると計算に長い時間を必要とし，記憶容量を過大に消費してしまう．今回は実行可能な規模の問題として，暗号ブロック 64bit（８変数２５６項目）・４制約という条件で実験を行なった．

４．実行テストによる性能評価

このアルゴリズムに従って作成したプログラムを用いて実行速度を計測した．最終的な解の個数が平均で１０個程度になるように調整した場合，実質的な計算速度は50bit/sec程度となった．

また，平文ベクトルを変換する際に排他的論理和を用いているが，それによって暗号文に線形性が現れていないかを調査した．

５．今後の研究課題

標的問題暗号では暗号ブロックを長くすると，解集合を絞り込むことが急激に難しくなってしまう．暗号ブロックを長くしようとした場合，解集合を効率よく絞り込むための方法を用意する必要がある．また，関数乗数r_f，r_{g_j}の決定にランダム性を導入したり，pから関数自体を自動生成するようにして鍵サイズを縮小したりすることも考えられる．

この暗号技術は従来の方法と比べて実行速度や鍵のサイズなどに不利な点がある一方，関数を乱数で生成しているため線形性が現れにくく，離散最適化問題特有の計算困難性があり，それが解読困難性に結びついている．計算方法の工夫や応用分野への適用方法の検討も含め，今後さらに研究を進めていく予定である．

参考文献

[1]仲川勇二：“離散最適化問題のための新解法”，電子情報通信学会論文誌，Vol.J23-A, No.3, pp.550-556（1990）

[2]Stinson,D.R.，桜井幸一監訳：“暗号理論の基礎”，共立出版（1996）