1ZA-3

PC クラスタを用いた格子点探索法による RSA 暗号鍵の安全性評価

和田　拓也　津田　伸生　永瀬　宏

金沢工業大学

1. はじめに

RSA 暗号鍵の安全性を高めるには，鍵に用いる合成数を二つの素数に分解する処理に時間がかかることが望ましい.安全性評価の信頼性を高めるには，格子点探索法の探索効率を高めて，最も攻撃者にとって有利となる厳しい条件下での評価を行うことが必要となる．そこで本研究では，RSA 暗号鍵において合成数の素因数分解の方法として，1990 年代提案された格子点探索法[1]を用い,探索アルゴリズムの改良と並列処理の導入し，探索の効率化を試みた．格子点探索法では，探索間隔が N**(1/4)（N は合成数）となり，全数探索に近い処理が可能である．しかし 1990 年代までの研究[1]では，小さな合成数に対する素因数分解しか行われていないので，本研究では 10 進 50 桁以上の合成数において，RSA 暗号鍵の安全性と，安全性評価の信頼性について評価した.

具体的には,報告者らの従来研究[2]に加えて，逆探索による格子点探索の実行と，PC クラスタを用いた並列処理による効率の良い格子点探索を新たに実施した.

2. 格子点探索法とは

ある合成数 N の素因数分解問題は，式(1)の双曲線関数を 2 次元 xy 平面上に考え(図 1 左側)，整数 x と y が双曲線上の格子点からなるような N を探索するものである.

$$xy = N \quad (1)$$

双曲線は大きな N の値のときに，局所的には直線のように見える．図 1 右側に示すように，双曲線 xy=N の最近傍に位置する格子点列を線で描くと，直線が引けることを考え，その直線と式(1)が接触する格子点を探索する.

図 1 より,
格子点探索の手順（順探索）は次の通り.

① 初期格子点を設定する
② 双曲線の最近傍に位置する格子点列を線で描き，直線を引く．初期格子点と，直線と双曲線 xy=N との交点までの距離(探索間隔，図 1 参照)を求める.
③ ②の距離(探索間隔)が整数であれば 2 つの因数を計算し,探索を終了する．そうでなければ初期格子点を移動させ，②を繰り返す

同じく図 1 より，格子点探索の手順（逆探索）は次の通り.

① 初期格子点を設定する
② ①から，x 座標は，$+N^{1/4}$，y 座標は，$-N^{1/4}$ をそれぞれ加算して，位置を移動させる(但し xy>N になるように微調整をする)
③ ②の座標から，双曲線の最近傍に位置する格子点列を線で描き，直線を引く.そこから，直線と双曲線 xy=N との交点までの距離(探索間隔，図 1 参照)を求める.
④ ②の距離(探索間隔)が整数であれば 2 つの因数を計算し,探索を終了する．そうでなければ初期格子点を移動させ，②を繰り返す

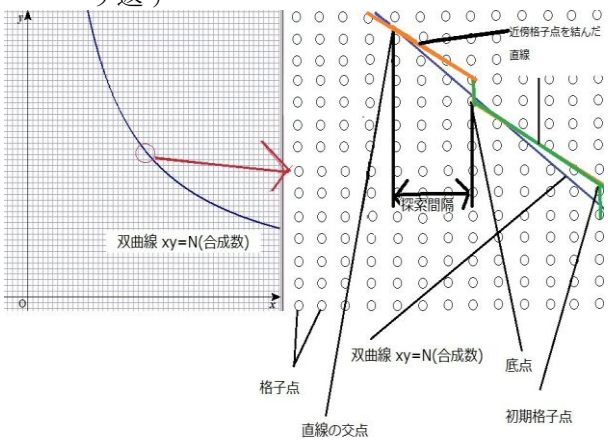

図 1　双曲線の近傍の格子点

3. PC クラスタと格子点探索法

合成数 N(式(1))の整数 x と y の双曲線上の格子点からなる探索を複数のポイントから効率よく探索ができるように PC クラスタによる格子点探索の並列処理を実現していく方法として，次の 2 つの方法を用いる．並列制御には MPI(Message Passing Interface)[3]を用いた.

① 双曲線の上部(x 軸の値が小さく，y 軸の値が

大きい)については，逆探索を集中的に実施し，双曲線の下部(x 軸の値が大きく，y 軸の値が小さい)については，順探索を集中的に実施する方法

② [(並列処理をする PC の台数)×1/2+1]等分に分割して，その分割上の点から(0<x<$\sqrt{N}$)，順探索・逆探索を同時に実施する方法

但し，①，②ともに x 座標における探索範囲は，0～$\sqrt{N}$までとする．

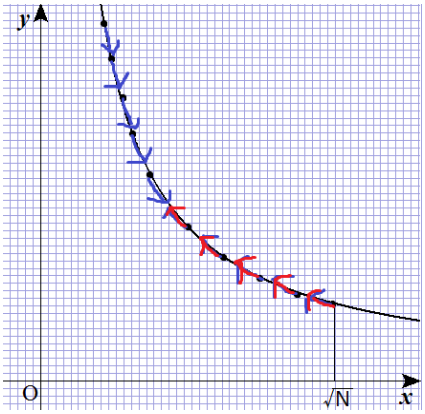

図 2　3.①の実行イメージ図

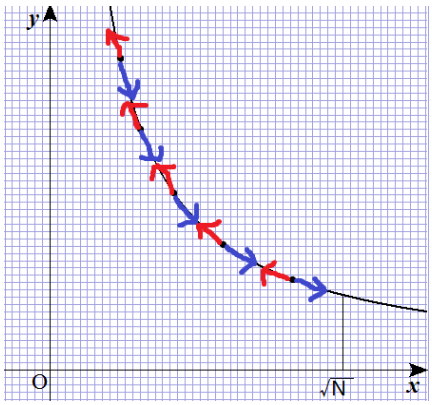

図 3　3.②の実行イメージ図

※図 2，図 3 において，
左上方向矢印:順探索
右下方向矢印:逆探索

4. 実験結果

図 2，図 3 のイメージ図をもとに，探索処理開始 1 秒から 2 秒の間でその x 座標における探索量を求める．同じ性能の PC を並列に処理した場合のシミュレーションを PC1 台で実験した．したがって，PC クラスタにおける処理ノードとホストノードとの通信のボトルネックは考慮しない．

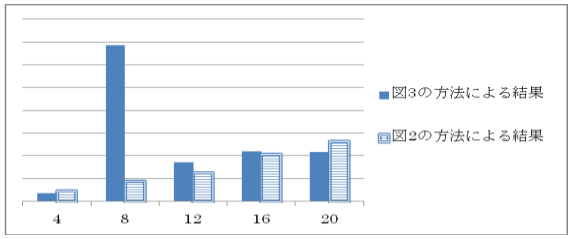

図 4　3. ①及び②の並列探索シミュレーション結果

図 4 では，以下を用いている．
- 横軸=PC 同時並列処理の台数
- 縦軸=x 軸における格子点探索の 1 秒間の探索量
- 両グラフ棒ともに，合成数 N については，同じ合成数（10 進 50 桁）を使用した

5. まとめと今後の課題

PC 複数台を用いて格子点探索の並列処理を行うことによって，PC1 台での格子点探索ではできなかった効率の良い探索が可能になった．PC1 台では，順探索と逆探索のどちらかと，格子点探索を 1 点でしかできないが，PC を複数台用いることによって順探索と逆探索を両方行うことができ，PC を 3 台以上並列処理させることによって，複数の座標点から格子点探索が行えるからである．これによって，RSA 暗号鍵の安全性評価の信頼性は高めることができると考えられる．

4. で述べたように，3. ②の方法では探索範囲の分布と PC の台数との関係が非線形な傾向を示した．原因については，現在調査中である．

また合成数の桁数を大きくすれば大きくするほど多倍長演算の精度が悪くなるのが現状である．演算の精度が悪い場合でも，探索処理は実行できる．しかし，探索効率が悪くなるため，安全性評価の信頼性は低くなる．そこで探索方向の傾きの計算に浮動小数点形式を導入するなど，更に安全性評価の信頼性を高める必要がある．

参考文献

[1]. 永瀬宏，井上清一：RSA 暗号の安全な鍵選択方式について，情報処理学会シンポジウム論文集 98 巻 12 号，pp7-12，1998
[2]. 和田拓也，津田伸生，永瀬宏：格子点探索法による RSA 暗号鍵の安全性評価，平成 23 年度電気関係学会北陸支部連合大会講演論文集，CD-ROM，2011
[3]. P. パチェコ著，秋葉　博訳：培風館 MPI 並列プログラミング，2001