6J-2

ＲＳＡ暗号向き高速剰余乗算法

森田　光
ＮＴＴ情報通信処理研究所

１．まえがき

公開鍵暗号に於いて代表的なＲＳＡ暗号では，高い安全性を得るために，１０進数で１５０桁以上の処理単位が必要であり，その高速化が不可欠である．

本論文では，ＲＳＡ暗号の主要な演算である剰余乗算の高速算法を提案する．本算法によれば，２進数でｎ桁（以下，桁は２進数を前提とする）の剰余乗算が最大ｎ回の加減算で実行でき，従来の方法[1,2]より約２倍高速となる．

２．高速剰余乗算アルゴリズム

ＲＳＡ暗号方式の暗号化処理は，$M^e \bmod N$（Mはメッセージ，ｅは公開の暗号化鍵を示し，ともにＮ未満の正整数）で表現されるべき乗剰余算を用い，復号化処理もべき乗剰余算を用いる．べき乗剰余算は剰余乗算から組み立てられる[3] ため，ＲＳＡ暗号の高速化には剰余乗算の高速化が必須である．

２．１ 本算法の原理

剰余乗算は，$A \times B \bmod N$ （Ａ，Ｂ，Ｎはｎ桁の正の整数，Ａ，ＢはＮ未満）で表現され，基本的には図１(a)に示されるように，部分積を加算して２ｎ桁の積を求めた後，除数Ｎの減算が繰り返されることにより行われる．この場合データ待避処理などが必要となるが，その簡略化のため部分積の間に除数を埋込み，加算と減算とを組にして繰り返すBakerの算法(図１(b)参照)が提案されている．しかし，この方法は図１(a) と同様に最大２ｎ回の加減算を必要とする．

ここで提案する算法は,図１(c)に示すように，２桁ずつシフトする基数４の乗算と除算を用いて加減算の回数を約半分に削減する方法であり，コンパクトなｎ桁幅の演算で実行できる．

乗除算とも基数４で動作可能とするため，本算法では以下の方策をとった．

i)除算用減算の途中結果（剰余）を一定範囲に抑えるため，次に加算される部分積を使って減算量を決定する．

ii)部分積を１桁削減するため,被乗数Ａの絶対値をＮ未満の範囲からＮ／２未満の範囲に予め変形する．但し,部分積はBoothの乗算法[4]で生成する．

２．２ 計算アルゴリズム

本算法の手順を図２に示す．主要な計算過程であるステップ３は,図３のRobertson図により説明される．横軸は現在の剰余４Ｒｋとｂ(k)Ａを加算した値に，縦軸は次の剰余Ｒk-1に対応し，グラフはＲk-1＝４Ｒｋ＋ｂ(k)Ａ＋ｃＮの関係を表わしている．ステップ３の繰り返し過程では，４Ｒｋ＋ｂ(k)Ａを横座標とするグラフから係数ｃを決め（図２の関数ｆｃに対応）,次の剰余Ｒk-1 を算出する．なお，図３では,一般的なRobertson図[4]と異なり,グラフの１価関数と２価関数との境界(減算量はこれにより決定される)

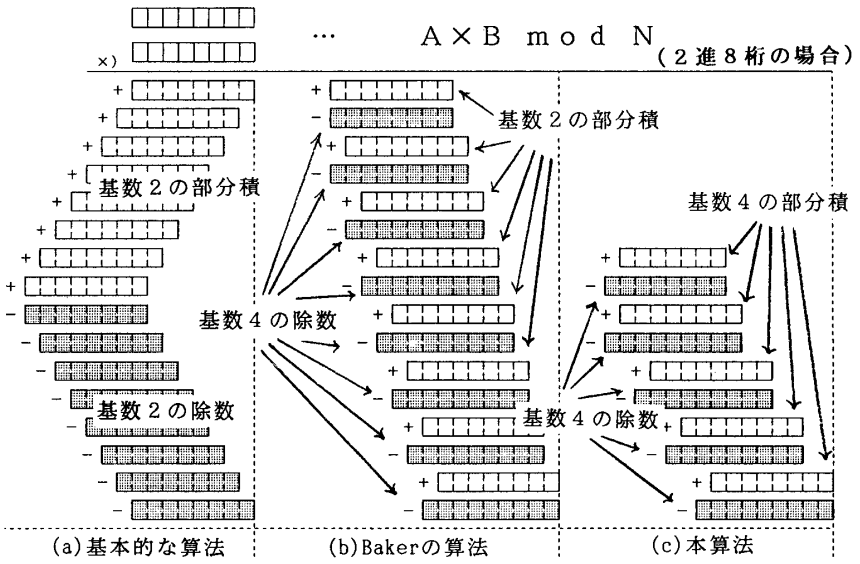

図１　従来法と本算法との原理比較

Fast Modular Multiplication Algorithm for RSA Cryptosystem
Hikaru MORITA
NTT Communications and Information Processing Laboratories

を示す指標 l_1, l_{-1}の値が変動する.

2．3　特徴

加減算回数の削減による高速性（表１参照）と，ｎ桁幅の演算で実行できるコンパクト性の他に，ハード実現上，以下の特徴を有する.

i)ハード量が小；ＮとＲの部分比較回路(Ｎの上位６桁Ｎｓ とＲの上位８桁Ｒｓとの比較)で係数ｃを生成可能．また，係数ｂとｃが－２～２間の整数のため，１桁シフトと反転用回路だけでｂＡ，ｃＮを生成可能.

ii)高速化が容易；ステップ３に於ける加減算は同時処理できるため，２段分の加減算を１クロックで実行可能．また，キャリーセーブ法が加減算に適用でき，かつ最終段の桁上がり伝搬加算をデータの出力速度にあわせることで，その遅延時間を見かけ上削減可能.

iii)桁数の拡張が容易；演算は全て隣接桁間のみで行われるため，ビットスライス構成が可能.

3．性能評価

本算法を実行する演算器は，レジスタ４個，全加算器２個を主たる構成要素とするセル(１００Ｇ；Bakerの算法より１～２割程度増）を，１次元アレイ状に配列して実現される．このセルの遅延時間は，加算器２段分とレジスタへのデータ書き込み時間が主であり，現在のＣＭＯＳ技術では約２０～３０ｎＳ程度となる．従って，５１２桁の演算器は約５０ＫＧで実現でき，その演算時間は約８μＳ（３０ＭＨｚクロック時）程度となる．この剰余乗算器をＲＳＡ暗号に適用した場合，その暗号化処理時間は約７ｍＳとなる.

高速剰余乗算法算出手順

ステップ１［Ｎの正規化］
・ＮのＭＳＢが１となるまで，ＮとＡを左シフト
ステップ２［初期化］
・Ｒ＝０，Ｎ＜２ＡならＡ＝Ａ－Ｎ
ステップ３［繰り返し処理］
（ｋ＝ｎ／２＋１から１迄逐次減算）
・ｃ＝ｆｃ（Ｒ＝４Ｒ＋ｂ(k)Ａ，ｂ(k-1)，Ａ）
・Ｒ＝Ｒ＋ｃＮ
ステップ４［計算結果Ａを元の０～Ｎ－１の範囲に変形］
・Ｒ＜０なら，Ｒ＝Ｒ＋Ｎ
・Ａ＝Ｒ，ステップ１のシフト量だけ右シフト

関数ｆｃ（Ｒ，ｂ，ａ）算出手順

・ｆｃ＝０
・ｄ＝Ｒ／|Ｒ|　（Ｒが正のとき１，負のとき－１）
・Ｒｓ＝|Ｒｓ|
・Ｒｓ＞Ｎｓなら，Ｒｓ＝Ｒｓ－Ｎｓ，ｆｃ＝１
・Ｒｓ＞|ｌｄ|Ｎｓなら，ｆｃ＝ｆｃ＋１（ｌｄは下表参照）
・ｆｃ＝－ｄｆｃ

場合分け		境界の指標ｌｄの値 $8l_1$	$-8l_{-1}$
ｂ＝０		4	4
|ｂ|＝１	ａｂ≧０	3	5
	ａｂ＜０	5	3
|ｂ|＝２	ａｂ≧０	2	6
	ａｂ＜０	6	2

注１：Ａ，Ｂ，Ｎはｎ桁のレジスタを示し，Ｒはｎ＋２桁のＲsumとＲcarryのレジスタで表される．Ａ，Ｒsum，Ｒcarryは負整数も表現するので，他に符号桁を持つ.
又，Ｂ[i]は，ＢレジスタのＬ ＳＢからｉ桁目の値を示す.
注２：ｂ(k)＝－２Ｂ[2k]＋Ｂ[2k-1]＋Ｂ[2k-2]
但し，ｂ(n/2+1)＝Ｂ[n]，ｂ(0)＝０，Ｂ[0]＝０

図２　高速剰余乗算法

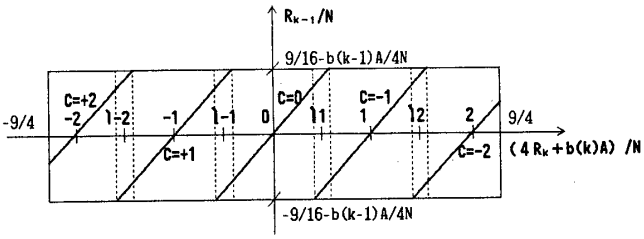

図３　高速剰余乗算法対応 Robertson 図

表１　剰余乗算法の速度比較

条件	加減算の回数 本算法	加減算の回数 Bakerの算法	速度比
平均	３ｎ／４ 乗算3n/8 除算3n/8	５ｎ／４ 乗算n/2 除算3n/4	１．７
最悪	ｎ 乗算n/2 除算n/2	２ｎ 乗算n 除算n	２

4．むすび

基数４の乗算と除算を組合せ，一定桁幅の処理で演算を完結する新たな剰余乗算法を提案した．本算法は従来法に対し約２倍高速であり，かつ５１２桁の剰余乗算器は５０ＫＧ規模のＬＳＩで実現可能である．これをＲＳＡ暗号に適用した場合の処理性能は約７０Ｋｂ／Ｓ（３０ＭＨｚクロック時）となる.

参考文献

[1]P.W.Baker:"Fast Computation of A * B Modulo N", Electron.Lett., 23-15, pp.794-795(1987).

[2]G.R.Blakley:"A Computer Algorithm for Calculating the Product AB Modulo M", IEEE Trans.Comput.,vol. C-32, pp.497-500(1983).

[3]D.E.Knuth：”準数値算法／算術演算”,the Art of Computer Programming, サイエンス社訳版(1986).

[4]K.Hwang："コンピュータの高速演算方式”，近代科学社訳版(1980).