GNU MP を用いた公開鍵暗号系の実装と実行速度比較

小中佳子　(指導教官: 金子 晃)

1　はじめに

近年ますます, セキュリティの重要性が高くなってきている. セキュリティ技術の基礎を成すのは, 代数学に基づく暗号理論である.

まず, GNU MP が提供する多倍長演算ライブラリを使用し, RSA 暗号と楕円曲線暗号の実装をした. 本研究では, これらの暗号との実行速度を行った. 更に, RSA 暗号の秘密鍵 d を二つに分ける方法の実行速度の向上率を検討した.

2　GNU MP

GNU MP(通称 GMP) は, 整数と有理数と浮動小数点数に対して, 任意精度演算を可能にする, C 言語用のポータブルライブラリである. これは, C 言語で普通に扱えるものより高い精度を必要とするすべてのアプリケーションのために, できるだけ速い演算ライブラリを提供することを目指している. 最初の GMP リリースは, 1991 年になされ, 以後年に一度程度で新しいリリースがされてきた. ほとんどのアプリケーションは, 数百ビット程度の精度で十分だが, 一部のアプリケーションは数千または数百万ものビットを必要とし得る. GMP は, オペランド (演算数) のサイズに依存してアルゴリズムを選ぶことにより, また, オーバーヘッドを最小にすることによって, 両方に対して良い実装を与えるように設計されている.

GMP の速度は, 演算の基本ユニットとしてフルワードを使うこと, 高度なアルゴリズムを用いることにより, 多くの CPU に対して最も普遍的な内部ループに対して最適化されるよう慎重に調整されたアセンブラコードを用いることにより, また, コードの美しさを犠牲にした速さの強調によって, 達成されている.

ここでは, 整数型のみを使用する. GMP の整数は, サイズ及び符号を表す `_mp_size`, 可変長データへのポインタ `_mp_d`, 及び臨時のサイズを表す `_mp_alloc` よりなる構造体である.

3　公開鍵暗号

暗号化鍵と復号鍵が等しい秘密鍵暗号方式は, 何らかの方法で送信者 (暗号化する人) と受信者 (復号する人) の間で鍵を共有する必要がある (鍵配送の必要性). この鍵配送の問題を見事に解決したのが公開鍵暗号方式である. 公開鍵暗号では, 暗号化するための鍵と復号するための鍵が異なり, 暗号化のための鍵を公開し, 復号のための鍵を秘密にしておく. その実仕様である公開鍵基盤原理は以下の通りである.

鍵生成・登録 利用者 A は, 自分で秘密に管理する秘密鍵 S_{A} と公開する公開鍵 P_{A} の対をある決められた方法で生成する. A は, P_{A} を公開鍵簿に登録する. 公開鍵簿は, 電話帳のようなもので, A の名前に対して電話番号のかわりに公開鍵 P_{A} が掲載される.

暗号化 別の利用者 B が A に暗号化して送信する場合を考える. B は, 公開鍵簿を使って, A の公開鍵 P_{A} を検索する. 次に, 通話内容 M を P_{A} を使って, 暗号化する. ここで, その暗号文 C を $E_{P_{\mathrm{A}}}(M)$ と記す.

復号 暗号文 C を受け取った A は, A だけが知っている秘密鍵 S_{A} を用いて, C から $M = D_{S_{\mathrm{A}}}(C)$ を復号する.

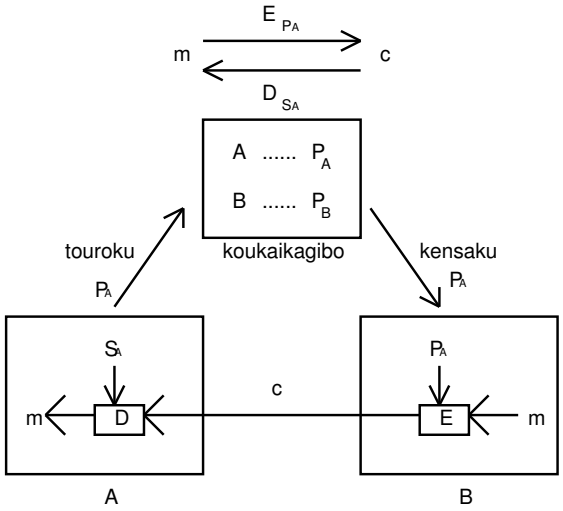

図 3.1: 公開鍵基盤の原理

4　RSA 暗号

1977 年に当時 MIT にいた 3 人の研究者 Rivest, Shamir, Adleman によって最初の公開鍵暗号が発見された. これを発見者の頭文字をとって RSA 暗号と呼ぶ. 素因数分解の困難さを安全性の根拠とする. RSA 暗号のブロック長は現在のところ, 1024 ビットが推奨されている.

鍵生成 二つの異なる大きな素数 p, q を生成し, $n = pq$ を計算する. $\lambda(n) = \mathrm{lcm}(p-1, q-1)$ とする. 適当な $e \in Z_{\lambda(\mathrm{n})}(\gcd(e, \lambda(n)) = 1)$ を定める. $d = 1/e \mod \lambda(n)$ を満たす d を定める.

秘密鍵 d, p, q
公開鍵 e, n

暗号化 $C = M^e \mod n$

復号 $M = C^d \mod n$

ここで M は, 暗号化の対象となるディジタル化された文書 (平文) であり, 同時にその 2 進数表現としての整数値を意味する. $M = M \in Z_{\mathrm{n}}$ とする.

これに対し, d は最悪 $\mathrm{lcm}(p-1, q-1)$ のビット長 1023 に近くなり得るので, 復号計算がはるかに重い. これを軽くする試みとして, 復号鍵 d を二つに分け, $d_{\mathrm{p}} = d \mod p-1, d_{\mathrm{q}} = d \mod q-1$ として記録し, これらを個別に用いることが J. J. Quisquater と C. Couvreur により提案された. この仕組みによる復号計算は以下のようになる.

(1) $M_p = C^{d_p} \mod p$, $M_q = C^{d_q} \mod q$ を別々に計算する.

(2) 中国人剰余定理により連立合同式

$$M = M_p \mod p, \quad M = M_q \mod q$$

の解を求める.

この M は Fermat の小定理により

$$M = M_p = C^{d_p} = C^{d+k(p-1)} = C^d \mod p,$$
$$M = M_q = C^{d_q} = C^{d+l(q-1)} = C^d \mod q$$

を満たし，従って $M = C^d \mod pq$ となるので，復号は正当化される．

(2) の連立合同式を解くには，$qa = 1 \mod p$, $pb = 1 \mod q$ なる a, b を用意して，

$$M = aqM_p + bpM_q \mod n$$

とすればよい．

5 楕円曲線

体 F 上の楕円曲線 E は, 次の形の方程式で与えられる曲線である．$a_{\mathrm{i}} \in F$ とし

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \quad (5.1)$$

式 (5.1) の a の添字は, 方程式が斉次, すなわち, 各項が全次数 6 をもつために, 係数に与えられるべき次数を示す．

$E(F)$ でこの方程式を満たす点 $(x, y) \in F^2$ と, $\mathcal{O}$ と表記する “無限遠点” の集合を表す．より一般に F の拡大体 K に対し, $E(K)$ で式 (5.1) を満たす $(x, y) \in K^2$ と $\mathcal{O}$ の集合を表す．(5.1) が楕円曲線であるためには, 滑らかでなければならない．これは両方の偏導関数が 0 になるような $E(\bar{F})$ の点がないことを意味する ($\bar{F}$ は F の代数的閉包を表す)．言い換えれば,

$$a_1Y = 3X^2 + 2a_2X + a_4, 2Y + a_1X + a_3 = 0 \quad (5.2)$$

と (5.1) は, F^2 において, 同時に満たされることがない．

F の標数が 2 でないなら, 一般性を失うことなく, $a_1 = a_3 = 0$ としてよい．標数 2 の場合は重要であり, 式 (5.1) の左辺が $Y^2 + a_3Y$ であるいわゆる “超特異” の場合と, 左辺が $Y^2 + a_1XY$ である “非超特異” の場合がある．後の場合, 一般性を失うことなく, $a_1 = 1$ とできる．(標数 2 のときには更に, 超特異の場合 $a_2 = 0$, 非超特異の場合 $a_4 = 0$ とできる．)

F の係数が 2 でも 3 でもないなら, 式 (5.1) の左辺を簡単化したあとで, 変数の 1 次変換, $X \to X - 1/3a_2$ により, 項 X^2 をも除去でき, 一般性を失うことなく, 楕円曲線は次の形の方程式で与えられるとしてよい．

$$Y^2 = X^3 + aX + b, \quad a, b \in F, \quad \mathrm{char}F \neq 2, 3. \quad (5.3)$$

この場合, 曲線が滑らかであるという条件は, 右辺の 3 次式が重根をもたないことを要請することと同値である．これは $Y^2 = X^3 + aX + b$ の判別式 $-(4a^3 + 27b^2)$ が非零のとき, かつそのときに限り成り立つ．

6 楕円曲線暗号

楕円曲線暗号系は, 1985 年 V.Miller と N.Koblitz によって独立に提案された．二つの利点がわかっている．(1) 群を選択するときの柔軟性が大きい (すなわち, 各素数べき q に対して, 乗法群 F_q^* はただひとつしかないが, 楕円曲線の群 E/F_q は沢山ある)．特に, (2)E を適当に選ぶなら, 暗号系を破る準指数時間アルゴリズムは知られていない．

7 RSA の計算量見積りと実行速度結果

RSA の秘密鍵 d を $\mathrm{mod}\ p$, $\mathrm{mod}\ q$ の二つに分けた暗号系を以下, dpqRSA と呼ぶことにする．本研究では, ブロック長 1024 ビットの通常の RSA, 同 dpqRSA, 及びこれと安全性が同等とされるブロック長 160 ビットの楕円曲線暗号 (Menezes-Vanstone 暗号) の速度比較を試みた．

dpqRSA の節約される計算量の見積りを考えてみる．d_{p}, d_{q} のビット長は高々512 程度である．個々の多倍長数の計算量はビット長が半分になれば, 少なくとも半分になる．特に積を原始的に実装している場合は, 1 回当たりビット長の 2 乗の計算量が必要なので，節約の効果は $\frac{1}{4}$ と劇的になる．次に復号の際の冪乗の回数であるが，C^d の計算はバイナリ法で最悪 1023×2 回必要なものが，C^{d_p} の計算は最悪 512×2 回で済む．しかし，C^{d_q} の分も有るので，加えると乗算回数は減っていない．最後の中国人剰余定理のところで 4 回の積と 1 回の和が余分に追加されるが，これらは 512 に比して無視できるので，全体として少なくとも $\frac{1}{2}$乃至$\frac{1}{4}$ くらいの節約が期待できる．

下の表の数値の単位は秒とする．システムパラメータと鍵の準備の部分は, それぞれ RSA と dpqRSA に対してはブロック長 1024 ビット, 楕円曲線暗号に対してはブロック長 160 ビットでの計算について計測した．暗号化と復号はすべて平文 128 ビットに対する所要時間に統一した．

	乱数生成	鍵生成	暗号化	復号化
RSA	0.062340	0.000091	0.000023	0.003346
dpqRSA	0.063842	0.000095	0.000022	0.001165
楕円曲線	0.005441	0.002743	0.018790	0.011022

実行速度結果の表

この結果から, dpqRSA は RSA と比較すると, 復号化にかかる実行時間が約 $\frac{1}{3}$ になっていることがわかる．これは, GMP の多倍長乗算がビット長 n の $O(n^{3/2})$ の計算量となる Karatsuba の算法を使っているためと思われる．楕円曲線は, RSA と dpqRSA と比較して総合的な時間が短いというよく知られた結果を得た．

8 今後の課題

今後, GMP を用いた超楕円曲線暗号の実装と高速化を行う．更に, 超楕円曲線暗号を一般化した代数幾何暗号の実装を行い, 安全な曲線の探求, 及びペアリングの実装などを行う予定である．

参考文献

[1] Neal Koblitz: “A Course in Number Theory and Cryptography, 2nd edition(Graduate Texts in Mathematics 114)”, Springer-Verlag New York 1994.

[2] Neal Koblitz: “Algebraic Aspects of Cryptography”, Springer-Verlag New York 1999.

[3] J. J. Quisquater and C. Couvreur:“Fast decipherment algorithm for RSA public key cryptosystem”, Electronic Letters, vol. 18, pp.905-907, 1982.

[4] 岡本龍明, 山本博資: “現代暗号”, 産業図書, 1997.

[5] 黒澤馨, 尾形わかは: “現代暗号の基礎数理”, コロナ社, 2004.