修士論文 要旨

鍵の部分情報の漏洩に対する RSA 暗号の安全性解析

複雑理工学専攻 47176112　鈴木海地
指導教員　國廣昇

1　はじめに

RSA 暗号は 1978 年に Rivest らによって考案された公開鍵暗号方式である [1]．RSA 暗号の安全性解析として，秘密鍵の上位ビットもしくは下位ビットが得られたときに鍵全体を復元するアルゴリズムが，これまで活発に研究されてきた．一連の研究は，より少ない部分情報で RSA 暗号を破る多項式時間攻撃アルゴリズムを構成することを目標としてきた．現在知られている中で，Ernst らの攻撃 [2] と Takaysu と Kunihiro の攻撃 [3] が，最も少ない部分情報で秘密鍵を復元できる．Takayasu と Kunihiro の攻撃は，秘密鍵の上位ビットまたは下位ビットから全体を復元するものでは，Ernst らの攻撃より少ない部分情報で秘密鍵を復元できる．

ただし Ernst らは，秘密鍵の上位ビットと下位ビット両方の部分情報が得られたときに，鍵を復元する攻撃をも提案した．これに対して Takayasu と Kunihiro は，この設定での攻撃は提案していない．提案攻撃は，Takayasu と Kunihiro の攻撃を適切に拡張することで，上位と下位両方から復元する Ernst らの攻撃を改良したものである．

2　準備

2.1　RSA 暗号

RSA 暗号の鍵生成，暗号化，復号を簡単に説明する．

2 つの異なる素数 p, q に対して，$N = pq$ とする．自然数 e, d を，ある自然数 ℓ が存在して，$ed = 1 + \ell(p-1)(q-1)$ となるようにとる．(N, e) を公開鍵，d を秘密鍵とする．暗号化は $c = m^e \mod N$，復号は $m = c^d \mod N$ により行われる．

本論文では，p と q が $\log N/2$ ビット，e が $\log N$ ビットであるような状況を考える．

2.2　攻撃設定の定式化

全体で $\beta \log N$ ビットの秘密鍵 $d \approx N^\beta$ のうち，上位 $\delta_1 \log N$ ビットの値を $d_1 \approx N^{\delta_1}$，下位 $\delta_2 \log N$ ビットの値を $d_2 \approx N^{\delta_2}$ とする．このとき，

$$M_1 := 2^{(\beta-\delta_1)\log N}, \quad M_2 := 2^{\delta_2 \log N}$$

とすると，秘密鍵 d は

$$d = d_1 M_1 + d' M_2 + d_2$$

と表すことができる．いま，d_1, d_2 の値が与えられていて，d' の値が未知であるような状況を考える．このとき，ℓ の近似を $\ell_0 := \lfloor (ed_1M_1 - 1)/N \rfloor$ とすると，ℓ の真の値との近似誤差は $|\ell - \ell_0| \le N^{\beta-\delta_1} + N^{\beta-\frac{1}{2}} + 1$ となる．ここで，提案攻撃は $\delta_1 < 1/2$ のときにのみ Ernst らの攻撃を改良するため，本論文では，特に断らない限りこの場合のみを扱う．$\delta_1 < 1/2$ のとき，近似誤差 $|\ell - \ell_0|$ は高々 $N^{\beta-\delta_1}$ の定数倍となる．

多項式 $f_{eM_2}(x,y), f_e(x,y)$ を，

$$f_{eM_2}(x,y) := 1 - ed_2 + (\ell_0 + x)(N + y) \pmod{eM_2},$$
$$f_e(x,y) := 1 + (\ell_0 + x)(N + y) \pmod{e}$$

とおくと，$(\tilde{x}, \tilde{y}) := (\ell - \ell_0, -p - q + 1)$ は $f_{eM_2}(x,y)$, $f_e(x,y)$ の根となる．このような多項式の根 $(\tilde{x}, \tilde{y})$ の値を求めることができれば，N の素因数分解ができる．

3　RSA 暗号に対する既存攻撃の適用条件

3.1　Ernst らの攻撃

Ernst らは，上位ビットと下位ビット両方が得られた状況における RSA 暗号に対する攻撃を提案した [2]．彼らの手法を用いると，前章で定式化した $\beta, \delta_1, \delta_2$ が以下の条件を満たすとき，攻撃が成功する．

(a) $\delta_1 + \delta_2 > \beta - \frac{5}{6} + \frac{\sqrt{6\beta+1}}{3}$

(b) $\delta_1 \le \frac{1}{2}$ かつ $\delta_1 > \beta - \frac{3(1+2\delta_2)^2}{16(1+\delta_2)}$

(c) $\delta_1 > \frac{1}{2}$ かつ $\delta_1 + \delta_2 > \frac{1}{3}\left(2\beta - 1 + \sqrt{4\beta^2 + 2\beta - 2}\right)$

3.2　Takayasu と Kunihiro の攻撃

Takayasu と Kunihiro は，上位ビットのみまたは下位ビットのみが得られた 2 つの状況に限定して，Ernst らの攻撃を改良した [3]．まず上位ビットから復元する攻撃において，彼らは，多項式 $f^{MSBs}(x,y)$ を，

$$f^{MSBs}(x,y) := 1 + (\ell_0 + x)(N + y) \pmod{e}$$

とおき，この多項式の根を求める手法をとった．彼らの手法を用いると，2.2 章の攻撃設定において上位ビットのみが与えられたとき，すなわち $\delta_2 = 0, d_2 = 0$ であるような状況で，適用条件を以下のように改良できる．

(A) $\beta \le \frac{1}{2}$ のとき，

$$\delta_1 > \frac{1}{2}\left(-(1-\beta) + \sqrt{-3(1-\beta)^2 + 2}\right)$$

(B) $\frac{1}{2} < \beta \le \frac{9}{16}$ のとき，

$$6(\beta - \delta_1)\sigma - 3\sigma^2 + 2\sigma^3 < \frac{(\sigma - 2\delta_1)^3}{2 - 2\beta - 2\delta_1},$$
$$\sigma = 1 - \frac{2\beta - 1}{1 - 2\sqrt{1 - \beta - \delta_1}}$$

また下位ビットから復元する攻撃において，彼らは，多項式 $f^{LSBs}_{eM_2}(w,y), f^{LSBs}_e(w,y)$ を，

$$f^{LSBs}_{eM_2}(w,y) := 1 - ed_2 + w(N + y) \pmod{eM_2},$$
$$f^{LSBs}_e(w,y) := 1 + w(N + y) \pmod{e}$$

とおき，この多項式の根を求める手法をとった．この手法を用いると，$\delta_1 = 0, d_1 = 0$ であるような状況において攻撃の適用条件を以下のように改良できる．

(C) $\beta < \dfrac{9-\sqrt{21}}{12}$ のとき，

$$\delta_2 > \frac{1}{2}\left(-(1-\beta) + \sqrt{-3(1-\beta)^2+2}\right)$$

4 提案攻撃

4.1 提案攻撃の概要

本研究では，上位と下位両方から復元する攻撃として，2.2 章の攻撃設定で定めた多項式 $f_{eM_2}(x,y), f_e(x,y)$ の根を求める手法をとった．我々は Ernst らの攻撃の適用条件を以下のように改良することに成功した．

(1) $\beta \leq \dfrac{9-\sqrt{21}}{12}$ のとき，

$$\delta_1 + \delta_2 > \frac{1}{2}\left(-(1-\beta) + \sqrt{-3(1-\beta)^2+2}\right)$$

(2) $\dfrac{1}{2} - \delta_1 + \delta_2 \leq \beta \leq \dfrac{1}{2} + \delta_2$ のとき，

$$\delta_1 > \frac{1}{2}\left(-(1-\beta+\delta_2) + \sqrt{-3(1-\beta+\delta_2)^2 + 2(1+\delta_2)}\right)$$

(3) $\dfrac{1}{2} + \delta_2 \leq \beta \leq \delta_1(4(1+\delta_2)(1-\delta_1)-1)$ のとき，

$$6(\beta-\delta_1)\sigma - 3(1+2\delta_2)\sigma^2 + 2(1+\delta_2)\sigma^3 < \frac{(\sigma-2\delta_1)^3}{2-2\beta-2\delta_1+2\delta_2},$$

$$\sigma = 1 - \frac{2\beta - 2\delta_2 - 1}{1 - 2\sqrt{(1+\delta_2)(1-\beta-\delta_1+\delta_2)}}$$

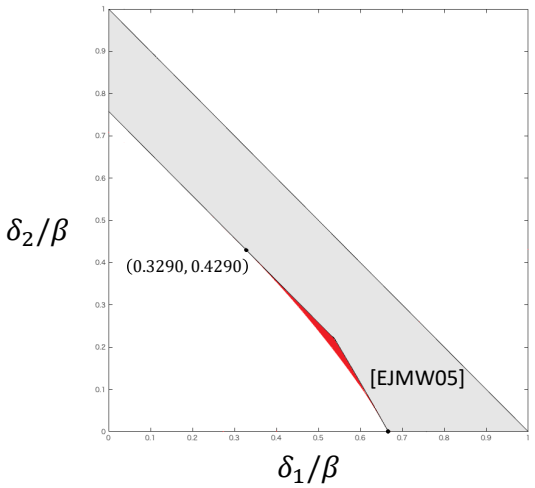

図 1. $d = N^{0.5625}$ のときの既存攻撃と提案攻撃の適用範囲の比較

提案攻撃は，Takayasu と Kunihiro の攻撃の拡張となっている．これらの適用条件は，$\delta_1 = 0$ としたとき，上位ビットのみが得られたときの適用条件 (A) および (B) を含みかつ部分的に一致する．また，$\delta_2 = 0$ としたとき，下位ビットのみが得られたときの適用条件 (C) を含む．提案攻撃は，$d < N$ のすべての秘密鍵の大きさの範囲において，Ernst らの攻撃に対して改良範囲をもつ．この一例として，$d = N^{0.5625}$ における既存攻撃と提案攻撃の適用範囲の比較を，図 1 に示した．

4.2 数値実験

本実験では，2048 ビットの合成数をもつ RSA 暗号のサンプルを 50 組ずつ生成し，それぞれに既存攻撃および提案攻撃を適用した．既存攻撃としては 3.1 節の (b) を，提案攻撃としては 4.1 節の (2) を実装した．各攻撃によってノルムの小さい多項式を生成できた場合を成功とし，50 組のサンプルのうち，それぞれの攻撃が成功したサンプルの数を数え，比較をした．

表 1. $\beta = 0.5625$ のときの既存攻撃 (b) の成功率

		$\delta_1 \log N$（ビット）					
		852	853	854	855	856	857
$\delta_2 \log N$（ビット）	253	0.00	0.00	0.04	0.08	0.28	0.86
	254	0.02	0.02	0.06	0.22	0.62	1.00
	255	0.02	0.06	0.16	0.38	0.92	1.00
	256	0.02	0.04	0.28	0.82	1.00	1.00
	257	0.04	0.26	0.66	1.00	1.00	1.00
	258	0.10	0.50	0.92	1.00	1.00	1.00

表 2. $\beta = 0.5625$ のときの提案攻撃 (2) の成功率

		$\delta_1 \log N$（ビット）					
		852	853	854	855	856	857
$\delta_2 \log N$（ビット）	253	0.00	0.00	0.04	0.08	0.60	1.00
	254	0.02	0.08	0.12	0.42	0.92	1.00
	255	0.04	0.08	0.36	0.70	1.00	1.00
	256	0.04	0.18	0.52	1.00	1.00	1.00
	257	0.08	0.26	0.92	1.00	1.00	1.00
	258	0.34	0.72	1.00	1.00	1.00	1.00

表 1，2 は，それぞれ既存攻撃と提案攻撃を比較したものである．1152 ビット ($\beta = 0.5625$) の秘密鍵のうち，852〜857 ビットの上位ビットおよび 253〜258 ビットの下位ビット ($\delta_1 \approx 0.4, \delta_2 \approx 0.125$) の部分情報が得られた状況を攻撃対象とした．これらの表から，提案攻撃は既存攻撃よりも少ない部分情報で，多項式の生成に成功することが分かる．

参考文献

[1] Rivest R., Shamir A., Adleman L. M. “A method for obtaining digital signatures and public-key cryptosystems.” Communications of the ACM, vol. 21(2), pp. 120–126. (1978)

[2] Ernst M., Jochemsz E., May A., de Weger B. “Partial key exposure attacks on RSA up to full size exponents.” EUROCRYPT 2005. LNCS, vol. 3494, pp. 371–386. (2005)

[3] Takayasu A., Kunihiro N. “Partial key exposure attacks on RSA: Achieving the Boneh-Durfee bound.” Selected Areas in Cryptogaphy 2014. LNCS, vol. 8781, pp. 345–362. (2014)