

n 進表現を用いた RSA 暗号の拡張[†]

1 J-3

高木 剛 内藤 昭三[‡]Ⓢ NTT ソフトウェア研究所[§]

概要

公開鍵 n を用い、平文空間を n 進表現することにより、多次元の RSA 型の暗号を提案する。提案暗号は 2 個以上のブロックを平文空間として持ち、復号化が従来の多次元の RSA 型暗号より高速である。安全性は従来の RSA 暗号の安全性と等価である。また、この暗号は特別の場合としてオリジナルの RSA 暗号を包含している。

1 はじめに

現在広く使われている公開鍵暗号に、Rivest, Shamir, Adleman の 3 人により考案された RSA 暗号がある [5]。

多次元型 RSA 暗号とは公開鍵のビット長を 1 ブロックとし、複数のブロックを平文空間に持つ暗号である。そのブロックの数をその暗号の次元と呼ぶ。具体例として、楕円曲線を用いる 2 次元タイプ [1] [3], 2 次元を用いる 2 次元タイプ [2], 代数体を用いる多次元タイプ [6] などが提案されている。これらの多次元型 RSA 暗号 (1 次元とする) のアルゴリズムの速さは、オリジナルの RSA 暗号を 1 個同時に利用した以上の時間が必要であった。

また、小山により特異な三次曲線を用いる 2 次元タイプの RSA 暗号が考案された [4]。この暗号は復号化の際、2 ブロックの冪乗計算が 1 ブロックのみで計算され、RSA 暗号を 2 ブロック同時に利用した場合と比較して 2 倍高速になる。

本稿では n 進表現を用いた RSA 型多次元暗号を提案する。提案暗号は 2 個以上のブロックを平文領域に取れる。アルゴリズムの速度面では、復号化において始めのブロック以外は一次合同式を解くだけで良く、従来の多次元型 RSA 暗号より高速である。安全性の面では、従来の RSA 暗号と等価であることを示す。

2 アルゴリズム

- 鍵生成: 2 個の素数 p, q を生成し、その積 $n = pq$ を決定する。次に素数 p, q から、

$$L = \text{lcm}(p-1, q-1)$$

を計算し、 $ed \equiv 1 \pmod{L}$ をみたす e と、 d を生成する。 e, n を公開鍵、 d を秘密鍵とする。

- 暗号化: $0 \leq M_0, M_1, \dots, M_{k-1} < n$ をみたす組 $(M_0, M_1, \dots, M_{k-1})$ を平文とする。受け手の公開鍵 2 である e を用い、式

$$C \equiv (M_0 + nM_1 + \dots + n^{k-1}M_{k-1})^e \pmod{n^k}$$

によって暗号化を行う。

- 復号化: 秘密鍵 d を用い、送られてきた暗号文 C に対して、式

$$M_0 \equiv C^d \pmod{n}$$

を計算し、 M_0 を復号化する。次に、 $M_1, M_2, \dots, M_{k-1}$ に対しては、 n を法とする。一次合同式を解くことにより復号化する。

3 復号化の詳細

M_0 が復号化されたとする。 $M_1, M_2, \dots, M_{k-1}$ を求める方法を以下に記述する。

$$C \equiv (M_0 + nM_1 + \dots + n^{k-1}M_{k-1})^e \pmod{n^k}$$

の展開式から、一次合同式を解くことにより帰納的に求めることができる。ここで、 C の展開式の n^i ($1 \leq i \leq k-1$) の係数を K_i とする。すなわち、

$$C \equiv K_0 + nK_1 + \dots + n^{k-1}K_{k-1} \pmod{n^k}$$

とする。 K_i は $M_0, M_1, \dots, M_{i-1}$ で決まる。また、 K'_i を K_i から M_i を含む 1 個の項を取り除いたものとする。例えば、 $M_1, M_2, \dots, M_{k-1}$ は以下のように計算できる。 K_i の計算は次節に記述する。

M_1 については、 K_0, K'_1 が M_0 で決まることから、

$$b_1 \equiv \frac{C - C_1}{n} \pmod{n}$$

$$C_1 \equiv K_0 + nK'_1 \pmod{n^2}$$

とするとき、合同式

$$eM_0^{e-1}x \equiv b_1 \pmod{n}$$

をみたす x を求めることにより復号化できる。以下、同様に $M_2, M_3, \dots$ を帰納的に計算する。

M_{k-1} については、 $K_0, K_1, \dots, K_{k-2}, K'_{k-1}$ が $M_0, M_1, \dots, M_{k-2}$ で決まることから、

$$b_{k-1} \equiv \frac{C - C_{k-1}}{n^{k-1}} \pmod{n}$$

$$C_{k-1} \equiv M_0 + nM_1 + \dots + n^{k-2}M_{k-2} + n^{k-1}K'_{k-1} \pmod{n^k}$$

とするとき、合同式

$$eM_0^{e-1}x \equiv b_k \pmod{n}$$

をみたす x を求めることにより復号化できる。

3.1 C の展開式

C の展開式に於ける n^i の係数 K_i ($i = 0, 1, \dots, k-1$) の求め方を以下に記述する。多項定理より、

$$C = \sum_{\substack{s_0, s_1, \dots, s_{k-1}=1 \\ s_0+s_1+\dots+s_{k-1}=e}}^e f(M_0, M_1, \dots, M_{k-1})$$

[†]Extension of RSA cryptoscheme using n -adic expansion

[‡]Tsuyoshi Takagi Shozo Naito

[§]NTT Software Laboratories

と展開される。ただし,

$$f(x_0, x_1, \dots, x_{k-1}) = \frac{e!}{s_0!s_1!\dots s_{k-1}!} x_0^{s_0} (nx_1)^{s_1} \dots (n^{k-1}x_{k-1})^{s_{k-1}}$$

と定義する。 n^i , ($i = 1, 2, \dots, k-1$) の係数は,

$$\{s_0, s_1, \dots, s_{k-1} | s_1 + 2s_2 + \dots + (k-1)s_{k-1} = i, \\ s_0 + s_1 + \dots + s_{k-1} = e, 0 \leq s_1, s_2, \dots, s_k \leq e\}$$

全体の集合 Γ_i ($1 \leq i \leq e$) を求め,

$$\sum_{(s_0, s_1, \dots, s_{k-1}) \in \Gamma_i} \frac{e!}{s_0!s_1!\dots s_{k-1}!} M_0^{s_0} M_1^{s_1} \dots M_{k-1}^{s_{k-1}}$$

を計算することにより求まる。実際に, i が小さい場合を記述する。

$$\begin{aligned} K_0 &= M_0^e \\ K_1 &= eM_0^{e-1}M_1 \\ K_2 &= eC_2M_0^{e-2}M_1^2 + eM_0^{e-1}M_2 \\ K_3 &= eC_3M_0^{e-3}M_1^3 + 2eC_2M_0^{e-1}M_1M_2 + eM_0^{e-1}M_3 \\ K_4 &= eC_4M_0^{e-4}M_1^4 + 3eC_4M_0^{e-3}M_1^2M_2 \\ &\quad + eC_2M_0^{e-2}M_2^2 + eM_0^{e-1}M_4 \\ K_5 &= eC_5M_0^{e-5}M_1^5 + 3eC_4M_0^{e-4}M_1^3M_2 \\ &\quad + 3eC_3M_0^{e-3}M_1M_2^2 + 2eC_2M_0^{e-2}M_2M_3 \\ &\quad + 2eC_3M_0^{e-2}M_1M_4 + eM_0^{e-1}M_5 \\ K_6 &= eC_6M_0^{e-6}M_1^6 + 5eC_5M_0^{e-5}M_1^4M_2 \\ &\quad + 4eC_4M_0^{e-4}M_1^3M_3 + 3eC_3M_0^{e-3}M_1^2M_4 \\ &\quad + eC_3M_0^{e-3}M_2^3 + eC_2M_0^{e-2}M_3^2 \\ &\quad + 2eC_2M_0^{e-2}M_2M_4 + 2eC_2M_0^{e-2}M_1M_5 + eM_0^{e-1}M_6 \\ K_7 &= eC_7M_0^{e-7}M_1^7 + 6eC_6M_0^{e-6}M_1^5M_2 \\ &\quad + 5eC_5M_0^{e-5}M_1^4M_3 + 5C_2eC_5M_0^{e-5}M_1^3M_2^2 \\ &\quad + eC_4M_0^{e-4}M_1^3M_4 + 2eC_2eC_4M_0^{e-4}M_1^2M_2M_3 \\ &\quad + 4eC_4M_0^{e-4}M_1M_2^3 + 3eC_3M_0^{e-3}M_1^2M_5 \\ &\quad + 3eC_3M_0^{e-3}M_1M_3^2 + 3eC_3M_0^{e-3}M_2^2M_3 \\ &\quad + 2eC_2M_0^{e-2}M_1M_6 + 2eC_2M_0^{e-2}M_2M_5 \\ &\quad + 2eC_2M_0^{e-2}M_3M_4 + eM_0^{e-1}M_7 \\ &\dots \\ K_{k-1} &= \{M_0, M_1, \dots, M_{k-1} \text{の多項式}\} \end{aligned}$$

4 安全性

この節では提案暗号が, 従来の RSA 暗号と同等の安全性があることを証明する。

補題 1 n を大きな 2 個の素数の積, e を 3 以上の自然数, C, C' を暗号文とする。次の 2 つの計算量は多項式時間の違いで等価である。

- (1) $x^e \equiv C \pmod{n}$ の解を求める。
- (2) $x^e \equiv C' \pmod{n^k}$ の解を求める。

ただし, k は 2 以上の自然数とする。

証明: アルゴリズム (2) により得られた解を, n を法として剰余をとれば (1) の解となる。(1) $\Rightarrow$ (2) は 3 節の復号化のアルゴリズムにより多項式時間で計算可能である。 Q.E.D

この補題の (1) は RSA 暗号の完全解読アルゴリズムであり, (2) は本稿の提案暗号の完全解読アルゴリズムである。これより, 提案暗号は RSA 暗号と同等の安全性をもつことがわかる。

5 具体例

1. 鍵生成: 2 個の素数 $p = 863, q = 733$ を生成し, その積 $n = 632579$ を決定する。次に素数 p, q から $L = 315492$ を計算し, $e = 125$ と, $d = 118625$ を生成する。平文 (M_0, M_1) を (12345, 67890) とする。

2. 暗号化: 公開鍵 $e = 125$ を用い, 式

$$C \equiv (12345 + 632579 \times 67890)^{125} \\ \equiv 91837206038 \pmod{632579^2}$$

によって暗号化を行ない, 受け手に送る。

3. 復号化: 秘密鍵 $d = 118625$ を用い, 式

$$M_0 \equiv 91837206038^{118625} \\ \equiv 67890 \pmod{632579}$$

により M_0 を復号化し, 632579 を法とする一次合同式

$$53744x \equiv 59744 \pmod{632579}$$

を解くことにより, $M_1 = 67890$ を得る。

6 まとめ

n 進表現を用いた公開鍵暗号を提案した。平文空間として 2 個以上のブロックがとれ, 従来提案されていた多次元型 RSA 暗号より復号化が高速である。安全性は従来の RSA 暗号と等価である。今後は部分解読に対する安全性や高機能認証への応用可能性を考察する。

参考文献

- [1] N. Demytko; "A new elliptic curves based analogue of RSA," Proc. of EUROCRYPT '93, LNCS 765, pp.40-49 (1992)
- [2] J. H. Loxton, D. S. P. Khoo, G. J. Bird, J. Seberry; "A cubic RSA code equivalent to factorization," J. Cryptology, 5, pp.139-150 (1992)
- [3] K. Koyama, U. M. Maurer, T. Okamoto and S. A. Vanstone; "New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$," Proc. of CRYPTO '91, LNCS 576, pp.252-266 (1990)
- [4] K. Koyama; "Fast RSA-type schemes based on singular cubic curves," Proc. of EUROCRYPT '95, LNCS 921, pp.329-340 (1995)
- [5] R. Rivest, A. Shamir, L. M. Adleman; "A method for obtaining digital signatures and public-key cryptosystems," Com. of the ACM, 21, 2, pp.120-126 (1978)
- [6] 高木 剛, 内藤 昭三; "RSA 暗号の代数体への拡張と通報通信攻撃," to appear in ISEC '96