中国剰余定理におけるGaussのアルゴリズムに対する単純電力解析

小池正修[†,††] 松本勉[†]

中国剰余定理（CRT）は多くの公開鍵暗号を高速に実装するために用いられる．本論文ではCRTにおけるGaussのアルゴリズムに対する単純電力解析（SPA）を提案する．提案解析手法は，2次元の場合のGaussのアルゴリズムに対し，消費電力波形から入力値を推測する．この手法を，剰余演算系（RNS）上のモンゴメリ乗算を利用したRSA-CRTに対して適用し，秘密素数pに関する部分情報を求めることができることを示す．さらに二分探索を応用することによりpを高確率で求めるアルゴリズムも提案する．

A Simple Power Analysis on Gauss's Algorithm for Chinese Remainder Theorem

Masanobu Koike[†,††] and Tsutomu Matsumoto[†]

The Chinese Remainder Theorem (CRT) is used to optimize implementation of a lot of public-key cryptosystems. In this paper we propose a simple power analysis (SPA) on Gauss's algorithm for CRT. Our attack reveals input values of Gauss's algorithm in two-dimensional case using several power consumption traces. We apply this method to RSA-CRT implementation using Montgomery multiplication based on Residue Number Systems (RNS). Then we can deduce the partial information related to the secret prime p. Furthermore we show an algorithm to reveal p with high probability by modifying the binary search algorithm.

1. はじめに

サイドチャネル解析の出現により，ハードウェア上に暗号アルゴリズムをいかに安全に実装するかが大きな課題となっている．サイドチャネル解析は，装置が暗号処理を行う際の処理時間や消費電力を観測することで，装置内の秘密情報を推測する手法である．処理時間を利用するものをタイミング解析，消費電力を利用するものを電力解析と呼ぶ．

現在までにさまざまな暗号方式に対して，多くのサイドチャネル解析手法が提案されている．一般に，中国剰余定理（Chinese Remainder Theorem，以下CRTと略記）を用いたRSA[15]実装に対するサイドチャネル解析手法は，公開の法Nを$N=pq$と素因数分解することを目的としている．ここでNを素因数分解するには，文献6)により，pの部分情報が得られれば十分である場合もある．

同時にそれらへの対策も多く提案されている．しかし対策を施すことによってあまりにも非効率になるのは望ましくない．そのため，実装するアルゴリズムに対してどのような攻撃があるかを見極めたうえで安全性と効率の両面から適切な対策を選定することが必要である．したがって，多くの暗号アルゴリズムで用いられる基本的な演算の，サイドチャネル解析に対する脆弱性を調査することは重要であると考えられる．

本論文ではGaussのアルゴリズムへの電力解析手法を提案する．Gaussのアルゴリズムは CRTを利用した暗号アルゴリズムの実装時によく使われる基本的な演算であるが，筆者らが知る限り，この演算に対するサイドチャネル解析手法は提案されていない．本論文で提案する解析手法は2次元の場合に，消費電力波形からGaussのアルゴリズムへの入力値を推定する手法である．

この解析手法を剰余演算系（Residue Number Systems，以下RNSと略記）上のモンゴメリ乗算[10]を用いたRSA-CRT実装に適用した．RNSモンゴメリ

† 横浜国立大学大学院環境情報学府/研究院
Graduate School of Environment and Information Sciences, Yokohama National University
†† 東芝ソリューション株式会社SI技術開発センター
Systems Integration Technology Center, Toshiba Solutions Corporation

乗算が Gauss のアルゴリズムを利用しているとき，上記の解析手法と二分探索を応用することで，p を高確率で求めることができることを示す．

本論文の構成は以下のとおりである．2 章で CRT，Gauss のアルゴリズムおよび RNS について，3 章でサイドチャネル解析について復習する．4 章では Gauss のアルゴリズムに対する電力解析手法，5 章では 4 章の解析手法を RNS モンゴメリ乗算を用いた RSA-CRT 実装に適用して，秘密素数 p を求める手法を提案する．6 章ではこれらの解析手法の対策を述べる．7 章では，4 章，5 章で述べた解析手法に関するいくつかの定理の証明を与え，8 章でむすぶ．

2. Gauss のアルゴリズム

2.1 Chinese Remainder Theorem

集合 $\mathcal{A} = \{a_1, a_2, \ldots, a_n\}$ をどの 2 つも互いに素な整数の集合とし，このすべての要素の積を A とする．このとき CRT の主張は環として

$$\mathbb{Z}/A\mathbb{Z} \cong \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$$

が成立することである．同型写像としては次の 2 種類 $f_1, f_2 : \mathbb{Z}/A\mathbb{Z} \to \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$ がよく知られている．どちらも

$$f_j(x) = (x[a_1], \cdots, x[a_n]) \quad (j = 1, 2)$$

で定義される．ここで $x[a_i] = x \bmod a_i$ である．逆写像は異なっていて，一方は

$$f_1^{-1}(x_1, \cdots, x_n) = \sum_{i=1}^{n} \xi_i A_i \bmod A \qquad (1)$$

で与えられる．ここで $A_i = A/a_i$，$\xi_i = x_i A_i^{-1} \bmod a_i$ である．これを Gauss のアルゴリズムと呼ぶ．もう一方は $\theta_{i,j} = a_i^{-1} \bmod a_j$ として h_i を

$$\begin{aligned} h_1 &= x_1[a_1] \\ h_2 &= (x_2 - h_1)\theta_{1,2}[a_2] \\ &\vdots \\ h_n &= (\cdots(x_n - h_1)\theta_{1,n} - \cdots - h_{n-1})\theta_{n-1,n}[a_n] \end{aligned}$$

と定義したとき

$$\begin{aligned} &f_2^{-1}(x_1, \cdots, x_n) \\ &= h_1 + a_1(h_2 + a_2(h_3 + \cdots + a_{n-1}h_n)\cdots) \end{aligned}$$

で与えられる．これを Garner のアルゴリズムと呼ぶ．

2.2 RSA-CRT

暗号アルゴリズムへ CRT を適用した最も代表的な例は，Quisquater らによる RSA 復号アルゴリズム（RSA-CRT と呼ぶ）である[14]．暗号文 c に対する RSA 復号では，秘密指数 d と公開の法 N を用いて $c^d \bmod N$ を計算する．CRT を用いた実装では，まず

Input: $c, p, q, d_p, d_q, p^{-1} \bmod q$
Output: $m = c^d \bmod N$

1: $c_p = c \bmod p$
2: $m_p = c_p^{d_p} \bmod p$
3: $c_q = c \bmod q$
4: $m_q = c_q^{d_q} \bmod q$
5: $m = m_p + p((m_q - m_p)(p^{-1} \bmod q) \bmod q)$

図 1 RSA-CRT アルゴリズム
Fig. 1 RSA-CRT algorithm.

Input: $\langle x\rangle_{\mathcal{A}\cup\mathcal{B}}, \langle y\rangle_{\mathcal{A}\cup\mathcal{B}} (x, y < 2N)$
Output: $\langle w\rangle_{\mathcal{A}\cup\mathcal{B}} (w \equiv xyB^{-1} (\mathrm{mod} N), w < 2N)$

	Base $\mathcal{A}$ operation	Base $\mathcal{B}$ operation
1:	$\langle s\rangle_{\mathcal{A}} \leftarrow \langle x\rangle_{\mathcal{A}}\langle y\rangle_{\mathcal{A}}$	$\langle s\rangle_{\mathcal{B}} \leftarrow \langle x\rangle_{\mathcal{B}}\langle y\rangle_{\mathcal{B}}$
2:		$\langle t\rangle_{\mathcal{B}} \leftarrow \langle s\rangle_{\mathcal{B}}\langle(-N)^{-1}\rangle_{\mathcal{B}}$
3:		$\langle t\rangle_{\mathcal{A}\cup\mathcal{B}} \Longleftarrow \langle t\rangle_{\mathcal{B}}$
4:	$\langle u\rangle_{\mathcal{A}} \leftarrow \langle t\rangle_{\mathcal{A}}\langle N\rangle_{\mathcal{A}}$	
5:	$\langle v\rangle_{\mathcal{A}} \leftarrow \langle s\rangle_{\mathcal{A}} + \langle u\rangle_{\mathcal{A}}$	
6:	$\langle w\rangle_{\mathcal{A}} \leftarrow \langle v\rangle_{\mathcal{A}}\langle B^{-1}\rangle_{\mathcal{A}}$	
7:	$\langle w\rangle_{\mathcal{A}} \Longrightarrow \langle w\rangle_{\mathcal{A}\cup\mathcal{B}}$	

図 2 RNS モンゴメリ乗算アルゴリズム
Fig. 2 RNS Montgomery multiplication algorithm.

p と q を法としたベキ乗剰余算をそれぞれ行い，CRT によりその 2 つの結果を結合して N を法とした結果を得る．結合のアルゴリズムとしては通常 Garner のアルゴリズムが用いられる．**図 1** に RSA-CRT アルゴリズムを示す．

2.3 Residue Number Systems

整数 x に対し $f_1(x)$ を x の RNS 表現と呼ぶ．集合 $\mathcal{A}$ を RNS 基底または単に基底，その元の個数 n を基底のサイズと呼ぶ．簡単のため，基底の元はすべて同じビット長 r であるとする．基底を明確にするために，$f_1(x)$ を $\langle x\rangle_{\mathcal{A}}$ と書くことにする．

RNS 表現は，加減乗算を各基底の下での剰余加減乗算で実現でき，かつ基底ごとに独立に行えるため，並列計算に適した手法である．本論文では，RNS 表現での演算は，n 個の演算器（各演算器は $\bmod a_i$ での積和演算を行う）で並列に処理するものとする．また，そのような装置を並列演算器と呼ぶことにする．

2.4 RNS モンゴメリ乗算

図 2 に示す RNS モンゴメリ乗算アルゴリズムは，サイズ n の 2 つの基底 $\mathcal{A}, \mathcal{B} = \{b_1, \cdots, b_n\}$ を用いる．これらは $A, B > 8N$，$\gcd(A, B) = 1$，$\gcd(B, N) = 1$ を満たすものとする．ここで $B = \prod_{i=1}^{n} b_i$ である．

入力 $x, y < 2N$ に対し，RNS モンゴメリ乗算は

$$w = \frac{xy + (xy(-N)^{-1} \bmod B)N}{B}$$
$$\equiv xyB^{-1} \pmod N$$

を計算する．この式から分かるように，モンゴメリ定数は B である．これを

$$w = MM(x, y, N, \mathcal{B}, \mathcal{A})$$

と書くことにする．

図 2 のステップ 3 と 7 の操作を基底拡張と呼ぶ．基底拡張 $\langle x\rangle_{\mathcal{A}} \Rightarrow \langle x\rangle_{\mathcal{A}\cup\mathcal{B}}$ は，まず CRT により x を計算したのちに $x \bmod b_i$ を計算するというステップをとる．CRT の部分では，Gauss，Garner いずれのアルゴリズムでも実現可能であるが，Gauss のアルゴリズムはその計算式の対称性から，並列演算器の各演算器を同一の構成にできるという利点がある．そのため，Kawamura ら[7]，Bajard ら[2] は Gauss のアルゴリズムによる基底拡張手法を採用している．本論文ではこのような，CRT での結合に Gauss のアルゴリズムを利用して RNS 演算を行う並列演算器を考察の対象とする．

まず A での除算を回避するためにある整数 k を用いて式 (1) を式 (2) のように書き換える：

$$x = \sum_{i=1}^{n} \xi_i A_i \bmod A$$
$$= \sum_{i=1}^{n} \xi_i A_i - kA. \tag{2}$$

式 (2) の両辺を A で割ると $0 \le x/A < 1$ より

$$k = \left\lfloor \sum_{i=1}^{n} \frac{\xi_i}{a_i} \right\rfloor \tag{3}$$

が得られる．この式より $0 \le k < n$ であることがいえる．式 (3) は浮動小数点演算を含んでいるため，効率良く実装するアルゴリズムがいくつか提案されている[2),7]．ここでは Kawamura らの方法[7] を復習する．

式 (2) と (3) を組み合わせると，x は

$$x = \sum_{i=1}^{n} (\xi_i A_i - k_i A) \tag{4}$$

と計算できる．ここで

$$k_i = \left\lfloor \left(\sum_{j=1}^{i-1} \frac{\xi_j}{a_j} - \left\lfloor \sum_{j=1}^{i-1} \frac{\xi_j}{a_j} \right\rfloor \right) + \frac{\xi_i}{a_i} \right\rfloor \tag{5}$$

である．Kawamura らの方法では，k を

$$\widehat{k} = \left\lfloor \sum_{i=1}^{n} \frac{\mathrm{trunc}(\xi_i)}{2^r} + \alpha \right\rfloor \tag{6}$$

Input: $\langle x\rangle_{\mathcal{A}}, \alpha$
Output: $\langle z\rangle_{\mathcal{A}\cup\mathcal{B}} = (\langle x\rangle_{\mathcal{A}}, \langle y\rangle_{\mathcal{B}})$
Precomputation: $\langle A_i^{-1}\rangle_{\mathcal{A}}, \langle A_i\rangle_{\mathcal{B}}, \langle -A\rangle_{\mathcal{B}}$

1: $\xi_i = x[a_i]A_i^{-1} \bmod a_i$
2: $\sigma_0 = \alpha, y_{i,0} = 0$
3: for ($j = 1$ to n) {
4: $\sigma_j = \sigma_{j-1} + \mathrm{trunc}(\xi_j)/2^r$
5: $\widehat{k}_j = \lfloor \sigma_j \rfloor$
6: $\sigma_j = \sigma_j - \widehat{k}_j$
7: $y_{i,j} = y_{i,j-1} + \xi_j A_j[b_i] + \widehat{k}_j(-A)[b_i]$
8: }
9: $y[b_i] = y_{i,n} \bmod b_i$

図 3 Kawamura らの基底拡張アルゴリズム
Fig. 3 Base extension algorithm proposed by Kawamura.

Input: $c, N, d = \sum_{i=0}^{\nu-1} d_\nu 2^\nu$ $(d_\nu \in \{0,1\})$
Output: $m = c^d \bmod N$
Precomputation: $B_N^2 = B^2 \bmod N$

1: Compute $\langle(-N)^{-1}\rangle_{\mathcal{B}}$
2: Radix-RNS conversion: N, B_N^2, c
3: $c' = MM(c, B_N^2, N, \mathcal{B}, \mathcal{A})$
4: $m' = MM(1, B_N^2, N, \mathcal{B}, \mathcal{A})$
5: for ($i = \nu - 1$ down to 0) {
6: $m' = MM(m', m', N, \mathcal{B}, \mathcal{A})$
7: if ($d_i = 1$)
8: $m' = MM(m', c', N, \mathcal{B}, \mathcal{A})$
9: }
10: $m = MM(m', 1, N, \mathcal{B}, \mathcal{A})$
11: RNS-Radix conversion: m
12: If $m > N$ then $m \leftarrow m - N$

図 4 RNS モンゴメリ乗算を用いたベキ乗剰余算アルゴリズム
Fig. 4 RNS modular exponentiation algorithm.

で近似計算する．ここで $\mathrm{trunc}(\xi_i)$ は ξ_i の下位 $(r-g)$ ビット（g は r 未満の正整数）を 0 にマスクする処理で，α は誤差補正項である．式 (6) の $\widehat{k}$ は**図 3** のステップ 4 から 6 のように，$\widehat{k}_j$ を 1 ビットずつ計算することにより求められる．ここで $\widehat{k} = \sum_{j=1}^{n} \widehat{k}_j$ かつ $\widehat{k}_j \in \{0,1\}$ である．よって $\widehat{k}_j$ の値に応じて式 (4) における A での減算が，図 3 のステップ 7 で $(-A)[b_i]$ を加えることで実行される．

2.5 ベキ乗剰余算

RNS モンゴメリ乗算を用いたバイナリ法によるベキ乗剰余算アルゴリズムを**図 4** に示す．まずパラメータを RNS 表現に変換し（ステップ 2），次に入力値 c

をモンゴメリ系での表現 $c' = cB \bmod N$ に変換する（ステップ 3）．その後 2 乗算と乗算のループによりベキ乗処理を行い，最後に m' を基数表現の m に戻す．

Bajard らは入出力も RNS 表現で行うことで，基数表現と RNS 表現との変換が不要な RNS モンゴメリ乗算方法を提案している（full RNS implementation と呼ぶ）[3]．ただしこの手法では通信二者間で RNS 基底を共有している必要がある．

図 1 と図 4 を組み合わせたアルゴリズムは容易に構成できる．図 1 のステップ 2 と 4 のベキ乗剰余算を図 4 のアルゴリズムで行えばよい．

RNS のパラメータ n，r は冗長度が最小になるように選ぶのが望ましい．ただし r は現在の演算器ビット幅の主流が 32 であるため，$r = 32$ と選ぶものとする．そのうえで Kawamura ら，Bajard らは N が 1,024 ビット，p が 512 ビットでの RSA-CRT 実装のときにはそれぞれ $n = 17$，$n = 18$ を選択している．

3. サイドチャネル解析

タイミング解析は，装置が暗号処理に必要な処理時間を解析することで，装置内の秘密情報を推測する解析手法である．RSA-CRT に対するタイミング解析として，Kocher の手法が知られている[8]．それは図 1 のステップ 1 に注目し，$c \geq p$ のときと $c < p$ のときの処理時間の違いから，$c = p$ なる暗号文を二分探索で見つける手法である．

一方電力解析は，暗号処理中の消費電力波形を解析することで，装置内の秘密情報を推測する解析手法である．CRT に対する電力解析として，Novak [11]，Okeya ら[13] の手法が知られている．これらはともに Garner のアルゴリズムに対する単純電力解析（Simple Power Analysis，以下 SPA と略記）である．Novak は RSA-CRT に対する解析手法を提案し，Okeya らはそれを Multi-prime RSA 等に拡張した．

Novak は Garner のアルゴリズムでの演算 $(m_q - m_p) \bmod q$ に注目した．この演算が

$$(m_q - m_p) \bmod q = \begin{cases} m_q - m_p & \text{if } m_q \geq m_p \\ (m_q - m_p) + q & \text{if } m_q < m_p \end{cases}$$

と実装されており，これらの演算列の違いを消費電力波形から区別できることを前提としている．Novak は $m_q - m_p$ の符号が，m が q の倍数のときに正から負に変化することに注目し，二分探索により q の倍数である平文 m を見つけるアルゴリズムを提案している．

本論文では Novak らのような RSA-CRT における CRT ではなく，RNS モンゴメリ乗算での基底拡張における CRT を念頭に Gauss のアルゴリズムを考察の対象とする．またその応用として，文献 12) で提案されている，Gauss のアルゴリズムを利用した RNS モンゴメリ乗算実装に対する解析手法を提案する．

4. Gauss のアルゴリズムに対する電力解析

本章では $n = 2$ の場合の Gauss のアルゴリズムに対する SPA 手法を提案する．

式 (4) と (5) より，$(x_1, x_2) \in \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z}$ としたときの $x = f_1^{-1}(x_1, x_2)$ は

$$x = \xi_1 A_1 + \xi_2 A_2 - kA \tag{7}$$

で計算される．ここで $k \in \{0, 1\}$ は $x < A$ とするためのパラメータである．別の表現で表すと，k は不等式

$$0 \leq \frac{\xi_1}{a_1} + \frac{\xi_2}{a_2} - k < 1$$

を満たす整数として定義される．よって k の値により式 (7) の x は異なる演算列で求められる．すなわち $k = 1$ のときは減算 $-A$ が行われるが，$k = 0$ のときは行われない．この演算列の差は，Novak の SPA 手法と同様に，消費電力波形から観測可能であるとする．このとき $k = 0$ か 1 かの情報を利用することで ξ_1，ξ_2（したがって Gauss のアルゴリズムへの入力値 x_1，x_2）を推測可能である．定理 1 がその具体的な提案解析手法である．定理 1 の証明は 7 章を参照のこと．

定理 1 2 つの整数 a_1，a_2 を互いに素な r ビットの整数とし，ξ_1，ξ_2 を $0 < \xi_1 < a_1$，$0 < \xi_2 < a_2$ を満たす整数とする．さらに不等式

$$0 \leq \frac{2^\lambda \xi_1 \bmod a_1}{a_1} + \frac{2^\mu \xi_2 \bmod a_2}{a_2} - k_{\lambda,\mu} < 1$$

を満たす整数として $k_{\lambda,\mu} \in \{0, 1\}$ を定義する（$\lambda, \mu = 0, 1, \cdots, r+1$）．もし a_1，a_2 およびすべての $k_{\lambda,\mu}$ の値が分かれば，ξ_1 と ξ_2 の値を決定できる．

注意 1 上の定理から $\xi_1 = 0$ または $\xi_2 = 0$ の場合は除外してある．たとえば $\xi_1 = 0$ のときは ξ_2 の値にかかわらず $k_{\lambda,\mu} = 0$ であるので ξ_2 の値を決定できない．

注意 2 式 (7) の k を式 (5) ではなく，式 (6) に基づいた $\widehat{k}$ に置き換えた場合，すなわち $\widehat{k}_{\lambda,\mu}$ を

$$0 \leq \frac{\mathrm{trunc}(2^\lambda \xi_1 \bmod a_1)}{2^r} + \frac{\mathrm{trunc}(2^\mu \xi_2 \bmod a_2)}{2^r} - \widehat{k}_{\lambda,\mu} < 1$$

で定義した場合も，定理 1 と同様な定理が成り立つ．ただし $\alpha = 0$ とする．

5. RNS モンゴメリ乗算への適用

本章では RNS モンゴメリ乗算を利用した RSA-CRT に対する電力解析手法を提案する．ここでは図 1 から図 4 を組み合わせたアルゴリズムで並列演算器上に実装されていることを想定している．ただし記述を簡単にするため，以下では基底拡張の式を式 (4) で代用する場合もあるが，実装上は図 3 のアルゴリズムを用いていることに注意されたい．

本手法は前章で述べた Gauss のアルゴリズムに対する解析手法と二分探索アルゴリズムに基づいている．また Coppersmith の素因数分解手法[6] を利用すれば，必要とする消費電力波形数を減らすこともできる．ここで Coppersmith の素因数分解手法は，p の上位 $(\log_2 N)/4$ ビットが既知のとき，格子基底縮小アルゴリズム[9] を利用して $\log_2 N$ の多項式時間で N を素因数分解する手法である．

5.1 前提条件

提案解析手法の前提条件は次のとおりである．

(A1) 基底拡張に Gauss のアルゴリズムを利用している．

(A2) 図 3 のステップ 7 での加算 $+\widehat{k}_j(-A)[b_i]$ の有無が観測可能．

(A3) 任意の $1 \le i,\ j \le n$ に対し $b_i b_j < N^{1/4} < p, q$.

(A4) 攻撃者はすべての基底要素を知っている．

図 3 のステップ 7 での加算 $+\widehat{k}_j(-A)[b_i]$ は，ステップ 4〜6 で決めた $\widehat{k}_j$ の値が 1 の場合に $(-A)[b_i]$ を加算し，$\widehat{k}_j = 0$ の場合は加算しないことで実現される．したがって $\widehat{k}_j$ の値によりステップ 7 の演算列が異なるため，前提条件（A2）は妥当な仮定といえる．前提条件（A3）は $B = \prod b_i > p$，$q \approx N^{1/2}$ と各 b_i のビット数が同じ r であることからおおよそ $n \ge 5$ と言い換えられる．前提条件（A4）はたとえば full RNS implementation[3] の状況で成立する．

5.2 節では，議論の単純化のためさらに次の 2 つを仮定する．5.3 節でこれら仮定を外した場合の考察を行う．

(A5) 式 (4) 内で $\xi_i = 0$ であることを消費電力波形から判別可能．

(A6) ある $i_1 < i_2$ に対して $\xi_{i_1} \neq 0$ かつ $\xi_{i_2} \neq 0$.

5.2 提案解析手法

提案解析手法は次の 2 つのフェーズからなる：

(I) RSA-CRT への入力値が $c = 1$ の場合に，図 4 のステップ 3 での RNS モンゴメリ乗算における基底拡張に，前節の解析手法を適用して $\lfloor B^2/p \rfloor$ の部分情報を得る．

(II) 得られた部分情報を利用し，RSA-CRT への入力値 c が $c \ge p$ か否かを判別し，二分探索により p を推測する．

5.2.1 解析手法のアイディア

フェーズ（I），(II）ともに図 4 のステップ 3

$$c'_p = MM(c_p, B_p^2, N, \mathcal{B}, \mathcal{A}) \tag{8}$$

での最初の基底拡張に注目する．RSA-CRT 実装なので法は p であることに注意しておく．ここで c は RSA-CRT への入力値，$c_p = c \bmod p$，$B_p^2 = B^2 \bmod p$ である．RNS モンゴメリ乗算 (8) は図 2 のアルゴリズムで実行される．最初の基底拡張（図 2 のステップ 3）における値 t は

$$t = c_p \times B_p^2 \times (-p^{-1} \bmod B) \bmod B \tag{9}$$

となる．ここで B^2 を p で割ったときの商を Q，余りを $R < p$ とすると

$$\begin{aligned} &B_p^2 \times (-p^{-1} \bmod B) \bmod B \\ &= (B^2 - Qp) \times (-p^{-1} \bmod B) \bmod B \\ &= Q \bmod B \end{aligned}$$

であるので式 (9) を

$$t = c_p \times (Q \bmod B) \bmod B \tag{10}$$

と書き換えることができる．

最初の基底拡張 $\langle t \rangle_{\mathcal{B}} \Rightarrow \langle t \rangle_{\mathcal{A}\cup\mathcal{B}}$ においては

$$\begin{aligned} t &= \sum_{i=1}^{n} (\xi_i B_i - k_i B) \\ &= (\cdots((\xi_1 B_1 + \xi_2 B_2 - k_2 B) + \xi_3 B_3 - k_3 B) \\ &\quad + \cdots - k_{n-1} B) + \xi_n B_n - k_n B \end{aligned} \tag{11}$$

が計算される．ここで $\xi_i = t[b_i] B_i[b_i] \bmod b_i$ である．式 (10) と合わせると，c_p が既知であれば ξ_i から $Q \bmod b_i$ の値が決定できる．逆に $c_p Q \bmod b_i$ から ξ_i の値が決定できる．

そこで式 (11) の加算のうち，最初の 2 回に注目する．この演算は $k_1 = 0$ より $\xi_1 B_1 + \xi_2 B_2 - k_2 B$ である．

フェーズ（I）は $c = 1$ の場合に，定理 1 を利用して ξ_1，ξ_2，したがって $Q \bmod b_1$，$Q \bmod b_2$ を求めるステップである．

フェーズ（II）は c を入力したときに，$c \ge p$ であるか否かを k_2 の値を利用して判定する方法を与え，二分探索により $c = p$ なる c を探すステップである．

5.2.2 フェーズ（I）

前提条件（A2），（A4）より，$0 \le (2^\lambda \xi_1 \bmod b_1)/b_1 + (2^\mu \xi_2 \bmod b_2)/b_2 - k_{\lambda,\mu} < 1$ で定義された $k_{\lambda,\mu} \in \{0,1\}$ の値がすべての $0 \le \lambda,\ \mu \le r+1$ に対して決定できる．よって定理 1 より ξ_1，ξ_2 の値を求めることができる．注目している基底拡張で $2^\lambda \xi_1 \bmod b_1$，$2^\mu \xi_2 \bmod b_2$ を計算させるためには，$c_{\lambda,\mu} \equiv 2^\lambda \bmod b_1$ と $c_{\lambda,\mu} \equiv 2^\mu \bmod b_2$ を満たすような整数 $0 \le c_{\lambda,\mu} < b_1 b_2$ を定め，RSA-CRT への入力値を $c \cdot c_{\lambda,\mu} = c_{\lambda,\mu}$ で定めればよい．前提条件（A3）より $c_{\lambda,\mu} < p$ なので $c_p = c_{\lambda,\mu}$ となる．

ただし定理 1 から ξ_1，ξ_2 を得るためには $\xi_1 \neq 0$ かつ $\xi_2 \neq 0$ でなければならない．しかし仮に $\xi_1 = 0$ とすると $\xi_1 B_1 = 0$ で $k_2 = 0$ となるので，代わりに加算 $\xi_2 B_2 + \xi_3 B_3 - k_3 B$ に，一般に $\xi_{i_1} \neq 0$ かつ $\xi_{i_2} \neq 0$ となるような最初の 2 つの ξ_{i_1}，ξ_{i_2} の加算に注目すればよい．仮定（A6）よりこのようなものが存在し，かつ仮定（A5）によりこのような i_1，i_2 を見つけることができる．また今の場合 $\xi_i = 0$ となるのは $Q \bmod b_i = 0$ のときで，かつそのときに限ることに注意しておく．

以上より攻撃者は $Q \bmod b_{i_1}$ と $Q \bmod b_{i_2}$ の値を決定できる．

5.2.3 フェーズ（II）

フェーズ（I）の結果を利用し，二分探索の応用により高確率で $c = p$ なる c を見つけるアルゴリズムを述べる．ここでは p のビット数 ℓ は既知とする．通常 ℓ は N のビット数の 1/2 であるため，この仮定は妥当である．

フェーズ（I）の結果より，攻撃者は任意の整数 c に対して $cQ \bmod b_1$，$cQ \bmod b_2$，すなわち ξ_1，ξ_2 を計算できる．よって RSA-CRT への入力値が c の場合の k_2 を計算することができる．この操作をシミュレーションと呼び，求めた k_2 を $K(c)$ と書くことにする．一方，RSA-CRT への入力値が c で消費電力波形から観測される k_2 を $k(c)$ と書くことにする．

まず $c < p$ の場合を考えると $c_p = c$ より $K(c) = k(c)$ となる．逆に $c > p$ の場合は，式 (10) の t の値を，シミュレーションでは

$$t = c \times (Q \bmod B) \bmod B,$$

消費電力波形からの観測結果では

$$t = (c \bmod p) \times (Q \bmod B) \bmod B$$

と異なる値を計算する．したがって，$K(c) = k(c)$ となる確率，$K(c) \neq k(c)$ となる確率はともに 1/2 と考えられる．

上記の考察をもとに，**図 5** にフェーズ（II）における二分探索アルゴリズムを示す．これは上限を $U = 2^\ell - 1$，下限を $L = 2^{\ell-1}$ と初期設定して $c = p$ なる c を求めるアルゴリズムである．まず上限 U と下限 L の中間値 $(U+L)/2$ を c として RSA-CRT に入力し，$K(c)$ と $k(c)$ を比較する（ステップ 3 ～ 5）．これらの値が異なっていた場合，$c > p$ と判断できるので，$U \leftarrow c$ で上限 U を更新して二分探索を継続する（ステップ 7）．

一方 $K(c) = k(c)$ の場合，c と p の大小は決定できない．仮に実際は $c > p$ だったとすると，ω を任意に選んだ正整数としたとき，$c+1, c+2, \ldots, c+\omega > p$ となる．よって $c+1$ から順に RSA-CRT に入力していくと，確率 1/2 で $K(c+j) \neq k(c+j)$ となり，このとき $c > p$ であったと判定できる（ステップ 17）．またすべての j に対して $K(c+j) = k(c+j)$ となる確率は $(1/2)^\omega$ と見積もってよい．逆に実際は $c < p$ だったとすると，$c + \omega < p$ であれば上のすべての j に対して $K(c+j) = k(c+j)$ である．したがって ω を適切に大

```
Input: ℓ, Q mod b_{i_1}, Q mod b_{i_2}
Output: p
 1:  U = 2^ℓ − 1, L = 2^{ℓ−1}
 2:  while (U ≠ L) {
 3:    c = (U + L)/2
 4:    compute K(c) by simulation
 5:    deduce k(c) using SPA
 6:    if (K(c) ≠ k(c)) {
 7:      set U = c
 8:    } else {
 9:      for (j = 1 to ω) {
10:        compute gcd(c + j, N)
11:        if (gcd(c + j, N) = p) {
12:          set U = V = p and go to step 2
13:        } else {
14:          compute K(c + j) by simulation
15:          deduce k(c + j) using SPA
16:          if (K(c + j) ≠ k(c + j))
17:            set U = c and go to step 2
18:        }
19:      }
20:      set L = c
21:    }
22:  }
23:  return U
```

図 5 二分探索による p の導出アルゴリズム
Fig. 5 Algorithm for finding p by binary search.

きくとれば，すべての j に対して $K(c+j)=k(c+j)$ のときは $c<p$ と判断してよい（ステップ 20）．ここで $c<p$ のとき $c+\omega<p$ であることを仮定したが，これは各 $c+j$ について $\gcd(c+j,N)$ を計算することで検査できる．もし $c+\omega>p$ であれば，ある j で $c+j=p$ であるので，上の最大公約数計算により N の素因子 p を求めることができる（ステップ 10〜12）．

以上を $U=L$ となるまで繰り返すと，ループ終了時に $U=L=p$ が得られる．

5.3 仮定（A5），（A6）について

前節では（A5），（A6）を仮定していたが，本節ではこれらの仮定がなくても，前節の提案解析手法が高確率で成功することを示す．ここで確率は，p が ℓ ビットの素数を動いた場合のものである．したがってほとんどの RSA の鍵に対して提案解析手法が機能するといってよい．

以下では，（A6）を仮定しない場合，および（A5），（A6）をともに仮定しない場合を考察する．前者は仮定（A5）が妥当である場合の，後者はそうでない場合の考察である．また仮定（A6）は仮定（A5）の下で意味を持つ仮定であるため，（A5）を仮定せずに（A6）を仮定する，という場合は考察しない．以下の考察における定理の証明は 7 章を参照のこと．

まず（A6）を仮定しない場合に提案解析手法が成功する確率を考察する．次の定理は成功確率の下限を与える．

定理 2 前提条件（A1）から（A5）のもとで，前節の解析手法が失敗する確率はたかだか $4n^2\cdot 2^{-2(n-1)(r-1)}$ である．

この確率の具体的な例として Kawamura らのパラメータ設定である $\log_2 p=512$，$r=32$，$n=17$ の場合を考えると

$$4\times 17^2\times 2^{-2\times 16\times 31}<2^{-980}$$

となる．したがってこの場合，提案解析手法はほぼ確率 1 で成功することが分かる．

次に（A5），（A6）ともに仮定しない場合を考察する．仮定（A5）がないと，攻撃者は $\xi_1\neq 0$ かつ $\xi_2\neq 0$ と想定して提案解析手法を適用することになる．したがって $\xi_1\neq 0$ かつ $\xi_2\neq 0$ であれば仮定（A5）がなくても提案解析手法による攻撃は成功するが，$\xi_1=0$ または $\xi_2=0$ の場合は定理 1 が使えないため，提案解析手法は機能しなくなる．次の定理は提案解析手法の成功確率の下限を与える．

定理 3 前提条件（A1）から（A4）のもとで，前節の解析手法が失敗する確率はたかだか $2^{-2(r-2)}$ である．

この確率の具体的な例として再び $\log_2 p=512$，$r=32$，$n=17$ の場合を考えると 2^{-60} となる．したがって高い確率で成功することが分かる．

以上より，前提条件（A1）から（A4）のみで，実用上は提案解析手法が機能するといえる．

5.4 必要な消費電力波形数

前提条件（A1）から（A4）のもとで，提案解析手法に必要な消費電力波形数を考察する．ここでは p のビット長は ℓ は既知とする．まず 5.2 節のフェーズ（I）では最大 $(r+2)^2$ 個の消費電力波形が必要である．

次にフェーズ（II）を見積もる．ここで c と p の大小比較が正しくできると仮定した場合の上限 U と下限 L の更新 $U\leftarrow c$ および $L\leftarrow c$ が起こる確率をそれぞれ 1/2 とする．すると図 5 のステップ 7 により上限 U が更新される確率は 1/4 であり，その while ループ内で必要な消費電力波形は 1 個である．ステップ 7 で更新されない確率は 3/4 であり，この場合はさらに最大 ω 個の消費電力波形が必要となる．したがってフェーズ（II）では平均的に

$$1\times\ell+\omega\times\frac{3\ell}{4}=\frac{\ell(3\omega+4)}{4}$$

個の消費電力波形が必要となる．

以上より，必要な消費電力波形の個数は $(r+2)^2+\ell(3\omega+4)/4$ と見積もることができる．

この値を $\log_2 N=1024$，$\log_2 p=512$，$r=32$，$n=17$ の場合で考えると $(r+2)^2+\ell(3\omega+4)/4=384\omega+1668$ である．たとえば $\omega=10$ とすると 5,508 個，$\omega=20$ とすると 9,348 個である．この個数は十分攻撃可能な数と考える．さらに Coppersmith の素因数分解手法[6] を利用すれば，p の上位 256 ビットだけ決定できればよいので，$192\omega+1{,}412$ 個まで減らすことができる．

6. 対　　策

提案解析手法への対策としては 2 種類が考えられる．

まず演算中の値をランダム化することがあげられる．ランダム化手法としては，メッセージ，ベキ指数，ベキ乗剰余算のアルゴリズムに対するものが知られている．提案解析手法は選択平文攻撃であるため，メッセージのランダム化[8] により防御可能である．その一方で，提案解析手法はベキ乗剰余算本体に着目していないため，ベキ指数やベキ乗剰余算アルゴリズムのランダム化では防御できない．

もう 1 つは条件分岐のない基底拡張アルゴリズムを利用することである．Gauss のアルゴリズムを用い

たものとしては，Bajard らの方法[3] が知られている．また Garner のアルゴリズムを用いたものも提案されている[4]．Garner のアルゴリズムは出力が CRT での法以下であることが保証されているため，今回解析の対象となった加算は行われない．

また基底をランダムに選択することにより，RNS モンゴメリ乗算にサイドチャネル解析への耐性を持たせる手法が提案されている[4),5]．これらは条件分岐のない基底拡張アルゴリズムを利用しているため，提案解析手法をそのまま適用することはできない．仮に Kawamura らの手法に基底のランダム選択手法を採用した場合には，図 4 のステップ 3 の RNS モンゴメリ乗算を行う際に基底をランダムに選択していないと，提案解析手法を防御できないことに注意が必要である．

最後に，提案解析手法は Kocher のタイミング解析手法と同様，入力値 c と p の大小関係に注目した手法である．ただし着目している演算が異なるため，図 1 ステップ 1 の演算に Kocher の解析手法への対策を講じるだけでなく，図 4 ステップ 3 の演算にも対策が必須であることを指摘している．

7. 定理の証明

7.1 定理 1 の証明

まず次の記号を導入する：

$$\sigma_\lambda = \frac{2^\lambda \xi_1 \bmod a_1}{a_1}, \tau_\mu = \frac{2^\mu \xi_2 \bmod a_2}{a_2}.$$

さらに ξ_1/a_1 と ξ_2/a_2 の 2 進展開をそれぞれ

$$\frac{\xi_1}{a_1} = \sum_{i=1}^{\infty} \alpha_i 2^{-i}, \quad \frac{\xi_2}{a_2} = \sum_{i=1}^{\infty} \beta_i 2^{-i}$$

とする．

以下では主に α_i，a_1，λ について記述するが，β_i，a_2，μ についても同様の議論が成り立つ．

補題 1 上の記号のもと，$\lambda = 0, 1, 2, \cdots$ に対し

$$\sigma_\lambda = \sum_{i=1}^{\infty} \alpha_{\lambda+i} 2^{-i}$$

である．さらに

$$\sigma_{\lambda+1} = 2\sigma_\lambda - \alpha_{\lambda+1}$$

が成り立つ．特に

$$\sigma_{\lambda+1} \geq \sigma_\lambda \Leftrightarrow \alpha_{\lambda+1} = 0$$
$$\sigma_{\lambda+1} < \sigma_\lambda \Leftrightarrow \alpha_{\lambda+1} = 1$$

である．

補題 1 の証明： 最初の主張は σ_λ が

$$2^\lambda \times \frac{\xi_1}{a_1} = \sum_{i=1}^{\lambda} \alpha_i 2^{\lambda-i} + \sum_{i=1}^{\infty} \alpha_{\lambda+i} 2^{-i}$$

の小数部分であることから従う．よって

$$\begin{aligned} 2\sigma_\lambda &= \sum_{i=1}^{\infty} \alpha_{\lambda+i} 2^{-i+1} \\ &= \alpha_{\lambda+1} + \sum_{i=1}^{\infty} \alpha_{\lambda+1+i} 2^{-i} \\ &= \alpha_{\lambda+1} + \sigma_{\lambda+1} \end{aligned}$$

であるので，2 つ目の主張も成り立つ．3 つ目の主張は 2 つ目の主張と $\sigma_\lambda < 1$ より成り立つ． □

補題 2 すべての α_i $(1 \leq i \leq r)$ より ξ_i の値を決定できる．

補題 2 の証明： まず $\gamma = \sum_{i=r+1}^{\infty} \alpha_i 2^{-i}$ とおくと $a_1\gamma < a_1 \times 2^{-r} < 1$ である．よって ξ_1 が整数であることを考慮すると

$$\begin{aligned} \xi_1 &= a_1 \sum_{i=1}^{\infty} \alpha_i 2^{-i} \\ &= a_1 \left(\sum_{i=1}^{r} \alpha_i 2^{-i} + \gamma \right) \\ &= \frac{a_1 (\sum_{i=1}^{r} \alpha_i 2^{r-i})}{2^r} + a_1\gamma \\ &= \left\lceil \frac{a_1 (\sum_{i=1}^{r} \alpha_i 2^{r-i})}{2^r} \right\rceil \end{aligned} \tag{12}$$

であるので，題意が成り立つ． □

式 (12) より補題 3 が示せる．

補題 3 すべての $1 \leq i \leq r$ に対し $\alpha_i = 0$ のとき $\xi_1 = 0$，$\alpha_i = 1$ のとき $\xi_1 = a_1$ である． □

補題 2 より定理 1 を証明するには $\lambda = 1, 2, \cdots, r$ に対して α_λ の値が分かればよい．以下 λ を 1 つ固定して，次の 2 つに場合を分けて考察する．

(i) ある μ について $k_{\lambda-1,\mu} \neq k_{\lambda,\mu}$.

(ii) すべての $0 \leq \mu \leq r+1$ について $k_{\lambda-1,\mu} = k_{\lambda,\mu}$.

(i) の場合は補題 4 より，(ii) の場合は補題 6 より α_λ の値を決定できることを示す．

まず (i) の場合を考える．

補題 4 $(k_{\lambda-1,\mu}, k_{\lambda,\mu}) = (0,1)$ のとき $\alpha_\lambda = 0$，$(k_{\lambda-1,\mu}, k_{\lambda,\mu}) = (1,0)$ のとき $\alpha_\lambda = 1$ である．

補題 4 の証明： 定義より $k_{\lambda-1,\mu}$ と $k_{\lambda,\mu}$ は次の不等式を満たす整数として定まる：

$$0 \leq \sigma_{\lambda-1} + \tau_\mu - k_{\lambda-1,\mu} < 1$$
$$0 \leq \sigma_\lambda + \tau_\mu - k_{\lambda,\mu} < 1.$$

よって $(k_{\lambda-1,\mu}, k_{\lambda,\mu}) = (0,1)$ のときは $\sigma_{\lambda-1} < \sigma_\lambda$ であり，補題 1 より $\alpha_\lambda = 0$ である．

逆に $(k_{\lambda-1,\mu}, k_{\lambda,\mu}) = (1,0)$ のときは $\sigma_{\lambda-1} > \sigma_\lambda$ なので，同様に補題 1 から $\alpha_\lambda = 1$ である． □

次に (ii) の場合を考える．まず準備として補題 5 を示し，その後に補題 6 を示す．

補題 5 すべての $0 \le \mu \le r-1$ に対し $k_{\lambda-1,\mu} = 0$ のとき $\alpha_\lambda = 0$，$k_{\lambda-1,\mu} = 1$ のとき $\alpha_\lambda = 1$ である．

補題 5 の証明： すべての $0 \le \mu \le r-1$ に対し $k_{\lambda-1,\mu} = 0$ かつ $\alpha_\lambda = 1$ と仮定する．さらにある $1 \le \mu \le r$ に対し $\beta_\mu = 1$ と仮定すると

$$\begin{aligned}&\sigma_{\lambda-1} + \tau_{\mu-1}\\ &= \sum_{i=1}^{\infty} \alpha_{\lambda-1+i} 2^{-i} + \sum_{i=1}^{\infty} \beta_{\mu-1+i} 2^{-i}\\ &\ge \frac{\alpha_\lambda}{2} + \frac{\beta_\mu}{2}\\ &= 1\end{aligned}$$

となる．したがって $k_{\lambda-1,\mu-1} = 1$ となるが，これは仮定に反する．よってすべての $1 \le \mu \le r$ に対し $\beta_\mu = 0$ である．すると補題 3 より $\xi_2 = 0$ となり定理 1 の仮定に矛盾．したがって $\alpha_\lambda = 0$ である．

逆にすべての $0 \le \mu \le r-1$ に対し $k_{\lambda-1,\mu} = 1$ かつ $\alpha_\lambda = 0$ と仮定する．ある $1 \le \mu \le r$ に対し $\beta_\mu = 0$ と仮定すると上と同様にして $k_{\lambda-1,\mu-1} = 0$ で矛盾，同様にしてさらに $\xi_2 = a_2$ が得られ矛盾．したがって $\alpha_\lambda = 1$ である． □

補題 6 すべての $1 \le \mu \le r+1$ に対し $k_{\lambda-1,\mu} = k_{\lambda,\mu}$ とする．このとき $\alpha_\lambda = k_{\lambda-1,1}$ である．

補題 6 の証明： まず $\alpha_\lambda = 0$ と仮定したとき，次の 3 通りしか起こりえないことを示す．

(a1) すべての $1 \le \mu \le r+1$ に対し $k_{\lambda-1,\mu} = k_{\lambda,\mu} = 0$.

(b1) すべての $1 \le \mu \le r+1$ に対し $k_{\lambda-1,\mu} = k_{\lambda,\mu} = 1$.

(c1) ある $1 \le \rho \le r$ が存在して，$1 \le \mu \le \rho$ に対しては $k_{\lambda-1,\mu} = k_{\lambda,\mu} = 0$ で，$\rho+1 \le \mu \le r+1$ に対しては $k_{\lambda-1,\mu} = k_{\lambda,\mu} = 1$.

補題 5 より (b1) は $\alpha_\lambda = 1$ を意味するため起こりえない．よって (a1)，(c1) どちらの場合でも $k_{\lambda-1,1} = 0 = \alpha_\lambda$ となる．

(a1) から (c1) の 3 通りであることを示すためには $k_{\lambda-1,\mu} = k_{\lambda,\mu} = 1$ のときは $k_{\lambda-1,\mu+1} = k_{\lambda,\mu+1} = 0$ とならないことを示せばよい．補題 1 より $\sigma_\lambda = 2\sigma_{\lambda-1}$ であり $\sigma_{\lambda-1} < 1/2$ となる．よって $k_{\lambda-1,\mu}$ と $k_{\lambda,\mu}$ は $1 \le \mu \le r$ に対し

$$0 \le \sigma_{\lambda-1} + \tau_\mu - k_{\lambda-1,\mu} < 1 \qquad (13)$$

$$0 \le 2\sigma_{\lambda-1} + \tau_\mu - k_{\lambda,\mu} < 1 \qquad (14)$$

で定まる．ここで $k_{\lambda-1,\mu} = k_{\lambda,\mu} = 1$ とすると不等式 (13) と $\sigma_{\lambda-1} < 1/2$ より $\tau_\mu \ge 1 - \sigma_{\lambda-1} > 1/2$ である．よって $\tau_{\mu+1} = 2\tau_\mu - 1 \ge 2(1-\sigma_{\lambda-1}) - 1 = 1 - 2\sigma_{\lambda-1}$ となる．さらに $k_{\lambda-1,\mu+1} = k_{\lambda,\mu+1} = 0$ と仮定すると $\mu+1$ の場合の不等式 (14) より $\tau_{\mu+1} < 1 - 2\sigma_{\lambda-1}$ となるがこれは矛盾である．

逆に $\alpha_\lambda = 1$ の場合も同様にして次の 3 通りしか起こりえないことを示せる．

(a2) すべての $1 \le \mu \le r+1$ に対し $k_{\lambda-1,\mu} = k_{\lambda,\mu} = 0$.

(b2) すべての $1 \le \mu \le r+1$ に対し $k_{\lambda-1,\mu} = k_{\lambda,\mu} = 1$.

(c2) ある $1 \le \rho \le r$ が存在して，$1 \le \mu \le \rho$ に対しては $k_{\lambda-1,\mu} = k_{\lambda,\mu} = 1$ で，$\rho+1 \le \mu \le r+1$ に対しては $k_{\lambda-1,\mu} = k_{\lambda,\mu} = 0$.

補題 5 より (a2) は $\alpha_\lambda = 0$ を意味するため起こりえないので (b2), (c2) どちらの場合でも $k_{\lambda-1,1} = 1 = \alpha_\lambda$ である． □

以上により定理 1 が証明できた． □

7.2 定理 2 の証明

提案解析手法は，仮定 (A6) が成立しないときに失敗する．仮定 (A6) が成立しないのは，たかだか 1 個の i を除いたすべての i について $\xi_i = 0$，すなわち $Q \bmod b_i = 0$ の場合である．

まずすべての i について $Q \bmod b_i = 0$ の場合を考える．CRT より $Q \bmod B = 0$ となる．すると定義より $R \bmod B = 0$ となるが，$R < p < B$ であるので $R = 0$ である．したがって B^2 が p の倍数となるが，これは RNS 基底のとり方から起こりえない．よってこの場合が起こる確率は 0 である．

次に $Q \bmod b_1 \ne 0$ かつ $Q \bmod b_i = 0$ $(i > 1)$ となる場合を考える．この確率は，Q が $b_2 \cdots b_n$ の倍数であることから，$1/b_2 \cdots b_n = b_1/B \le 2^r/2^{n(r-1)}$ でおさえられる．より正確には，Q が b_1 の倍数でなくかつ $\lfloor B^2/Q \rfloor$ が素数の場合，という条件を付加する必要があるためこの確率はもっと小さくなるが，ここでは $2^r/2^{n(r-1)}$ を確率の上限として採用する．したがって $Q \bmod b_2 \ne 0$ の場合，$Q \bmod b_3 \ne 0$ の場合，と順に考えていくことで，1 個の i を除いては $Q \bmod b_i = 0$ となる確率はたかだか $n \cdot 2^r/2^{n(r-1)}$ であることが分かる．

最後に，提案解析手法は，法が p での演算，法が q での演算でともにたかだか 1 個の i を除いて $Q \bmod b_i = 0$ のときに失敗する．したがって失敗する確率は

$$(n \cdot 2^r / 2^{n(r-1)})^2 = 4n^2 \cdot 2^{-2(n-1)(r-1)}$$

でおさえることができる．□

7.3 定理 3 の証明

提案解析手法が失敗する $\xi_1 = 0$ または $\xi_2 = 0$ となる確率を考える．まず $\xi_1 = 0$ すなわち $Q \bmod b_1 = 0$ となるのは Q が b_1 の倍数のときなので，その確率は $1/b_1 < 2^{-(r-1)}$ でおさえられる．

同様に $\xi_2 = 0$ となる確率も $2^{-(r-1)}$ でおさえられるので，$\xi_1 = 0$ または $\xi_2 = 0$ となる確率はたかだか $2^{-(r-1)} + 2^{-(r-1)} = 2^{-(r-2)}$ である．

定理 2 と同様に，法が p での演算，法が q での演算でともに $\xi_1 = 0$ または $\xi_2 = 0$ のときに失敗するので，その確率は

$$(2^{-(r-2)})^2 = 2^{-2(r-2)}$$

でおさえることができる．□

8. ま と め

本論文では，Gauss のアルゴリズムに対する電力解析手法を新たに提案した．この攻撃は 2 次元の場合に，法以下にするための条件付き減算に注目して，Gauss のアルゴリズムへの入力値を推測する手法である．

Gauss のアルゴリズムは暗号アルゴリズムを実装するうえでの 1 つの基本演算であるため，提案解析手法は重要である．実際に RNS モンゴメリ乗算を利用した RSA-CRT 実装に対し提案解析手法を適用し，秘密素数 p を高確率で暴くことができることを示した．

対策としては，メッセージのランダム化や条件付き減算を用いない基底拡張アルゴリズムを利用することがあげられる．つまり Gauss のアルゴリズムを用いるときはこのような対策が不可欠であることを示した．

参 考 文 献

1) Akishita, T. and Takagi, T.: Zero-Value Point Attacks on Elliptic Curve Cryptosystem, *ISC 2003*, LNCS 2851, pp.218–223 (2003).
2) Bajard, J.C., Didier, L.S. and Kornerup, P.: Modular Multiplication and Base Extension in Residue Number Systems, *Proc. 15th IEEE symposium on Computer Arithmetic*, pp.59–65 (2001).
3) Bajard, J.C. and Imbert, L.: A Full RNS Implementation of RSA, *IEEE Trans. Comput.*, Vol.53, No.6, pp.769–774 (2004).
4) Bajard, J.C., Imbert, L., Liardet, P.Y. and Teglia, Y.: Leak Resistant Arithmetic, *CHES 2004*, LNCS 3156, pp.62–75 (2004).
5) Ciet, M., Neve, M., Peerers, E. and Quisquater, J.J.: Parallel FPGA Implementation of RSA with Residue Number Systems — Can Side-Channel Threats be Avoided?, *46th IEEE International Midwest Symposium on Circuits and Systems* (2003).
6) Coppersmith, D.: Finding a Small Root of a Bivariate Integer Equation; Factoring with High Bits Known, *EUROCRYPT '96*, LNCS 1070, pp.178–189 (1996).
7) Kawamura, S., Koike, M., Sano, F. and Shimbo, A.: Cox-Rower Architecture for Fast Parallel Montgomery Multiplication, *EUROCRYPT 2000*, LNCS 1807, pp.523–538 (2000).
8) Kocher, P.: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems, *CRYPTO '96*, LNCS 1109, pp.104–113 (1996).
9) Lenstra, A.K., Lenstra, H.W. and Lovasz, L.: Factoring Polynomials with Rational Coefficients, *Mathematische Annalen*, Vol.261, No.4, pp.515–534 (1982).
10) Montgomery, P.L.: Modular Multiplication without Trial Division, *Math. Computation*, Vol.44, pp.519–521 (1985).
11) Novak, R.: SPA-Based Adaptive Chosen-Ciphertext Attack on RSA Implementation, *PKC 2002*, LNCS 2274, pp.252–261 (2002).
12) Nozaki, H., Motoyama, M., Shimbo, A. and Kawamura, S.: Implementation of RSA Algorithm Based on RNS Montgomery Multiplication, *CHES 2001*, LNCS 2162, pp.364–376 (2001).
13) Okeya, K. and Takagi, T.: Security Analysis of CRT-Based Cryptosystems, *ACNS 2004*, LNCS 3089, pp.383–397 (2004).
14) Quisquater, J.J. and Couvreur, C.: Fast Decipherment Algorithm for RSA Public-Key Cryptosystem, *Electronics Letters*, Vol.18, pp.905–907 (Oct. 1982).
15) Rivest, R.L., Shamir, A. and Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Comm. ACM*, Vol.21, pp.120–126 (1978).

(平成 16 年 11 月 29 日受付)
(平成 17 年 6 月 9 日採録)

小池　正修（正会員）

1974 年生．1996 年東京大学理学部数学科卒業．1998 年東京大学大学院数理科学研究科修士課程修了．同年株式会社東芝入社．2003 年東芝ソリューション株式会社に異動．入社以来，暗号と情報セキュリティの研究開発に従事．2005 年横浜国立大学大学院環境情報学府博士課程後期修了．博士（工学）．

松本　　勉（正会員）

1986 年東京大学大学院博士課程修了．工学博士．同年横浜国立大学工学部専任講師．同助教授，教授を経て，2001 年より同大学大学院環境情報研究院教授．1981 年より暗号や情報セキュリティの研究に従事．「明るい暗号研究会」創設メンバ．現在，情報セキュリティ，暗号アルゴリズム，認証プロトコル，ディジタル証拠性，情報ハイディング，バイオメトリクス，人工物メトリクス，耐タンパー技術等に広く関心を持つ．国際暗号学会 IACR 理事．暗号技術検討会構成員．CRYPTREC 暗号モジュール委員会委員長．INSTAC 耐タンパー性標準化調査研究委員会委員長．電子情報通信学会より「情報セキュリティの基礎理論」への貢献に関して業績賞を受賞．