SCIS 2008 The 2008 Symposium on Cryptography and Information Security
Miyazaki, Japan, Jan. 22-25, 2008
The Institute of Electronics, Information and Communication Engineers

多変数非線形方程式に基づく署名方式 $3IC$- の安全性解析

Security consideration on the signature scheme $3IC$-

宮澤 俊之* 星野 文学 * 小林 鉄太郎 *
Miyazawa Toshiyuki Hoshino Fumitaka Kobayashi Tetsutaro

あらまし 2007 年に Dubois らは NESSIE で採択されたデジタル署名方式 SFLASH (C^{*-}) の公開鍵の差分をとることにより C^* の公開鍵を復元する方式を示し，これによって C^{*-} の公開鍵が与えられれば署名を偽造できることを示した．C^{*-} のほかにも，多変数非線型方程式に基づくデジタル署名方式に対して，Dubois らの用いた差分による攻撃の有効性を評価することは重要である．本稿では，2007 年に Ding らによって提案されたデジタル署名方式 $3IC$- (Delta Invertible cycle) [1] に対して，差分を用いた攻撃の有効性を評価した．$3IC$- は，多変数 2 次多項式暗号 $3IC$ の公開鍵から (C^{*-} と同様に) 幾つかの 2 次式を削除することによって構成されるデジタル署名方式であるが，本稿では，$3IC$- の公開鍵の差分を取ることによって，$3IC$ の公開鍵を復元できることを示す．

キーワード 多変数非線型方程式，デジタル署名，差分，SFLASH

1 はじめに

現在利用されている公開鍵暗号は，素因数分解問題や (楕円) 離散対数問題の困難さに基づいている．しかし，素因数分解や離散対数問題は，量子計算機が実現されると Shor のアルゴリズム [10] によって全て多項式時間で解けるため，現在利用されている RSA 暗号や楕円曲線暗号は全て解読できる．量子計算機の実用化は，かなり先であると考えられるが，公開鍵暗号は情報社会の基盤を形成する技術の一つであるため，量子計算機の実現後のために，今からその対策を進めておくことは重要である．

量子計算機に対して安全な暗号の候補として，NP 困難な問題に基づく暗号が挙げられる．このような方式としては，部分和問題に基づく方式 [7, 6] や，格子の最短／最近ベクトル問題に基づく方式や，有限体上の多変数非線形方程式の求解問題に基づく方式などがある．(以下では有限体上の多変数非線形方程式の求解問題に基づく方式を 多変数非線型方程式に基づく暗号と呼ぶ.)

多変数非線型方程式に基づく暗号は，1986 年に松本-今井 [4] によって提案されて以降，安全性解析と改良を繰り返し，さまざまな方式が提案されている．その中で，特に標準化が進んでいた方式に SFLASH [9] がある．SFLASH は，松本-今井方式 (C^* 方式) の公開鍵から幾つかの 2 次式を削除したデジタル署名方式 C^{*-} に具体的なパラメータを与えた方式で，欧州連合による欧州推薦暗号 (NESSIE) に採択されている [5].

しかし，2007 年に Dubois らは C^{*-} の（NESSIE に採用されている SFLASH で与えられているパラメータを含む）ほとんどのパラメータ選択において，公開鍵が与えられれば署名の偽造が出来ることを示した [2, 3]．この攻撃は，C^{*-} の公開鍵の差分 (differential) をとることにより，C^* の公開鍵を復元し，Patarin の関係式 [8] を用いて署名を偽造する攻撃である．

C^{*-} のほかにも多変数非線型方程式に基づくデジタル署名方式は複数あるが，差分による攻撃の有効性を評価することは重要である．

本稿では，2007 年に Ding が提案したデジタル署名方式 $3IC$- (Delta Invertible cycle) [1] に対して，差分を用いた攻撃の有効性を評価した．$3IC$- は，多変数 2 次多項式暗号系 $3IC$ の公開鍵から (C^{*-} と同様に) 幾つかの 2 次式を削除することによって構成されるデジタル署名方式であるが，本稿では，$3IC$- の公開鍵の差分を取ることによって，$3IC$ の公開鍵を復元できることを示す．

本稿の構成は以下のとおりである．2 節では，C^* とその改良の C^{*-} の概略を示し，3 節で Dubois らによる差分を用いた攻撃の概略を示す．4 節では ℓIC と ℓIC- の概略と $3IC$- に対する差分を用いた解析を示す．

* 日本電信電話株式会社 NTT 情報流通プラットフォーム研究所 〒 180-8585 東京都武蔵野市緑町 3-9-11 {miyazawa.toshiyuki, hoshino.fumitaka, kobayashi.tetsutaro }@lab.ntt.co.jp

2 多変数非線型方程式に基づく署名方式とその攻撃

本節では，多変数非線型方程式に基づく暗号方式の概略と，C^* 方式とそれに対する Patarin の攻撃，および，Patarin の攻撃を回避する改良 C^{*-} 方式の概略を示す．

2.1 多変数非線型方程式に基づく方式の構成

$\mathbb{F}_q^n$ を位数 $q(=2^m)$ の有限体 $\mathbb{F}_q$ 上の n 次元ベクトル空間とする．関数

$$\begin{array}{rcl} F : {\mathbb{F}_q}^n & \longrightarrow & {\mathbb{F}_q}^{n'} \\ (x_1, ..., x_n) & \mapsto & (f_1(x_1, ..., x_n), ..., f_{n'}(x_1, ..., x_n)) \end{array}$$

において，すべての f_i $(i = 1, ..., n')$ の total degree が 2 である，つまり，f_i が

$$f_i(x_1, ..., x_n) = \sum_j \sum_k \alpha_{jk} x_j x_k + \sum_j \beta_j x_j + \gamma_0 \qquad (\alpha_{ij}, \beta_i, \gamma_0 \in \mathbb{F}_q)$$

で表されるとき，quadratic function と呼ぶことにする．quadratic function の逆像を求めることは，多変数連立 2 次方程式を解くことになるため，一般には NP 困難である．しかし，容易に逆像を計算できる quadratic function も存在する．多変数非線型方程式に基づく暗号では，容易に逆像を計算できる quadratic function F と $\mathbb{F}_q$ 上の可逆な線形（もしくは，アフィン）変換 T, U を用いて，公開鍵を $P = T \circ F \circ U$ とし，秘密鍵を T, U とする．以下では，このような F のことを central map と呼ぶことにする．

署名生成の際には，メッセージ m から署名 σ を $\sigma = U^{-1} \circ F^{-1} \circ T^{-1}(m)$ によって求め，検証の際には m と公開鍵 P から，一致検証 $P(\sigma) = m$ を検査することによって，署名の受理もしくは不受理を判定する．

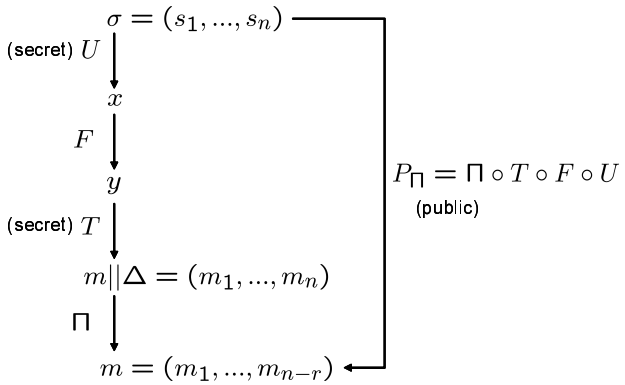

図 1: 多変数非線型方程式に基づく方式の概略

2.2 C^* 方式

C^* は，1988 年に松本-今井 によって提案された方式である [4]．この方式では，ベクトル空間 ${\mathbb{F}_q}^n$ の元を拡大体 $\mathbb{F}_{q^n}/\mathbb{F}_q$ の元とみなして，central map として $F(x) = x^{q^\theta+1} = x^{q^\theta} \cdot x$ $(\theta \in \mathbb{Z}_{>0})$ を用いる．写像 $x \mapsto x^{q^\theta}$ を $x = (x_1, ..., x_n) \in {\mathbb{F}_q}^n$ の座標で書き直せば x^{q^θ} の各座標は $x_1, ..., x_n$ の 1 次式で記述できるため，$F(x)$ の各座標は $x_1, ..., x_n$ の 2 次式で表現できる．また，F および P が可逆となるには $\gcd(q^\theta + 1, q^n - 1) = 1$ である必要があるため，q は 2 べきでなくてはならない．

2.3 Patarin の攻撃

1995 年に Patarin によって C^* の公開鍵から署名を偽造する攻撃を示した [8]．この攻撃は $\mathbb{F}_{q^n}$ において $y = F(x)$ から，両辺を $q^\theta - 1$ 乗して，xy をかけることによって得られる等式

$$y^{q^\theta} x - y x^{q^{2\theta}} = 0 \qquad (1)$$

を利用する．$(x_1, ..., x_n) \in {\mathbb{F}_q}^n$ を $x \in \mathbb{F}_{q^n}$ の座標表現，$(y_1, ..., y_n) \in {\mathbb{F}_q}^n$ を $y \in \mathbb{F}_{q^n}$ の座標表現とすると，(1) 式から，x_i, y_j について 1 次の方程式が n 個得られる．構成から，メッセージ $m = (m_1, m_2, ..., m_n)$ は T を用いて $m = Ty$ によって得られ，署名 $\sigma = (s_1, ..., s_n)$ は U を用いて $\sigma = U^{-1}x$ によって得られることがわかるため，(1) 式から，以下の形の n 個の方程式が得られることがわかる．

$$\sum_{i=1}^{n} \sum_{j=1}^{n} \gamma_{ij}^{(k)} m_i s_j + \sum_{i=1}^{n} (\alpha_i^{(k)} m_i + \beta_i^{(k)} s_i) + \delta_0^{(k)} = 0 \qquad (k = 1, ..., n).$$

P は公開鍵であるため，攻撃者は $m' = P(\sigma')$ を満たす対 (m', σ') を得ることが出来るので，複数の対を (1) 式に代入して，連立 1 次方程式を解くことにより $\gamma_{ij}^{(k)}$, $\alpha_i^{(k)}$, $\beta_i^{(k)}$, $\delta_0^{(k)}$ を決定することができる．

この攻撃を避けるために，Patarin らが提案した方式が C^{*-} 方式 [9] である．

2.4 C^{*-} 方式と SFLASH

C^{*-} 方式は，C^* の公開鍵 P から $r(< n)$ 個の 2 次式を単純に削除した方式である．具体的には $\Pi : {\mathbb{F}_q}^n \to {\mathbb{F}_q}^{n-r}$ を自然な射影 $(x_1, ..., x_n) \mapsto (x_1, ..., x_{n-r})$ とするとき，C^{*-} 方式の公開鍵 P_Π を $P_\Pi = \Pi \circ U \circ F \circ S$ とする方式である．(このように，多変数非線型方程式に基づく方式から，幾つかの方程式を削除することをマイナスオプションといい，方式の略称に “– ” を付与することでマイナスオプションを表す．)

Patarin らは，C^{*-} の公開鍵 P_Π から C^* の公開鍵 P を得るひとつの方法を示し その計算量が $O(q^r)$ である

ことを示した．したがって，現実の使用を前提とした場合，少なくとも $q^r \geq 2^{80}$ とする必要がある．

NESSIE プロジェクトにおいて，Patarin らは具体的なパラメータを定めた C^{*-} 方式を SFLASH$v2$ として提案し，推奨方式に採択された [5]．また，その後の評価を受けて，より安全なパラメータを与えた SFLASH^{v3} も提案している．以下にそのパラメータを示す．

- SFLASH^{v2} : $q = 2^7,\ n = 37,\ \theta = 11,\ r = 11$
- SFLASH^{v3} : $q = 2^7,\ n = 67,\ \theta = 33,\ r = 11$

この設定を含む C^{*-} のほとんどのパラメータ選択において，2007 年に Dubois らは，C^{*-} の公開鍵 P_Π から r 個の 2 次式を再構成し，C^* の公開鍵 P' を復元する方法を示した．これにより， 2.3 節で示した攻撃を可能とすることが出来る．P_Π から P' の復元する方法の概略を示す．

3 Dubois らの攻撃の概略

3.1 基本的なアイデア

2.3 節で示した攻撃を可能とするためには，C^{*-} の公開鍵 $P_\Pi = (p_1, ..., p_{n-r})$ から，$P_\Pi = \Pi \circ P'$ を満たす C^* の公開鍵 $P' = (p_1, ..., p_{n-r}, p'_{n-r+1}, ..., p'_n)$ を求められればよい．ただし，P' は C^* の公開鍵 $P = T \circ F \circ U = (p_1, ..., p_n)$ と一致する必要はない．n 個の 2 次式 $\{p_1, ..., p_n\}$ によって張られる $\mathbb{F}_q$ 上のベクトル空間と，n 個の 2 次式 $\{p_1, ..., p_{n-r}, p'_{n-r+1}, ..., p'_n\}$ によって張られる $\mathbb{F}_q$ 上のベクトル空間とが一致していればよい．

$\xi \in \mathbb{F}_{q^n}$ に対して写像 $M_\xi : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ を $x \mapsto \xi x$ とする．(M_ξ はベクトル空間 ${\mathbb{F}_q}^n$ 上の線形写像とみなすことも出来ることに注意されたい．) このとき $F \circ M_\xi = M_{F(\xi)} \circ F$ が成り立つ．ここで，$N_\xi := U^{-1} \circ M_\xi \circ U$ とすれば，

$$\begin{aligned} P_\Pi \circ N_\xi &= \Pi \circ T \circ F \circ U \circ N_\xi \\ &= \Pi \circ T \circ F \circ U \circ (U^{-1} \circ M_\xi \circ U) \\ &= \Pi \circ T \circ F \circ M_\xi \circ U \\ &= \Pi \circ (T \circ M_{F(\xi)}) \circ (F \circ U) \end{aligned}$$

ここで，$T \circ M_{F(\xi)}$ が $\{aT; a \in \mathbb{F}_q\}$ と異なる変換を与えていれば，$P_\Pi \circ N_\xi$ の r 個の座標 (の 2 次式) は P_Π の座標 (の 2 次式) とは $\mathbb{F}_q$ 上線形独立であることが期待される．したがって，上記の性質を満たす N_ξ を求めればよい．

3.2 差分を用いた解析

[2, 3] では，N_ξ を求めるために，差分 (differential) を利用した．まず，その定義を示す：

Definition 3.1. $\Phi : {\mathbb{F}_q}^n \to {\mathbb{F}_q}^n$ を quadratic function とするとき，

$$D\Phi(a, x) := \Phi(x + a) - \Phi(x) - (\Phi(a) - \Phi(0))$$

を Φ の差分 (differential) と呼ぶ．

$\mathbb{F}_q$ 上 n 変数の quadratic function $\Phi(x_1, ..., x_n)$ に対して，定義から $a, x \in {\mathbb{F}_q}^n$ に対して symmetric になる．また，$D\Phi((x_1, ..., x_n), (a_1, ..., a_n))$ は $x_i a_j$ $(i \neq j)$ による $\mathbb{F}_q$ 上の線形結合で表すことができる．(Φ における定数と 1 次の項は $D\Phi$ の定義からキャンセルされる．また，$(x_i + a_i)(x_j + a_j) - x_i x_j - a_i a_j = x_i a_j + x_j a_i$ であり，$(x_i + a_i)^2 - x_i^2 - a_i^2 = 2a_i x_i = 0$ となるためである．) 従って，$D\Phi$ は，bilinear symmetric form になる．

C^* および C^{*-} における $F(x) = x^{q^\theta+1}$ の差分は $DF(a, x) = a^{q^\theta} x + a x^{q^\theta}$ となる．また，C^* の公開鍵 $P = T \circ F \circ U$ と C^{*-} の公開鍵 $P_\Pi = T \circ F \circ U$ の公開鍵の差分は以下のとおりになる．

$$\begin{aligned} DP(a, x) &= T \circ DF(U(a), U(x)) \\ DP_\Pi(a, x) &= \Pi \circ T \circ DF(U(a), U(x)) \end{aligned}$$

(ここで，DP_Π は P_Π から計算できることに注意されたい．) DP_Π と N_ξ に関して，以下の性質が成り立っている．

$$\begin{aligned} &DP_\Pi(a, N_\xi(x)) + DP_\Pi(N_\xi(a), x) \\ &\quad = \Pi \circ T \circ M_{\xi^{q^\theta}+\xi} \circ T^{-1}(DP(a, x)) \end{aligned} \tag{2}$$

Dubois らは [2, 3] において $(n, \theta) > 1$ の場合と，(SFLASH のパラメータ設定を含む) $(n, \theta) = 1$ の場合に分けて，C^{*-} の解析を行っている．

$\gcd(n, \theta) = d > 1$ の場合　上記 (2) 式において，$\xi^{q^\theta} + \xi = 0$ $(\xi \in \mathbb{F}_{q^d})$ であれば (2) 式 の右辺は 0 になる．$DP_\Pi \circ N_\xi$ の各座標は $N_\xi = (\eta_{ij})$ の各成分 η_{ij} の 1 次式で表される．[2] では，heuristic な議論と実験により，$r < n - 3$ であれば連立方程式により N_ξ を求めることが出来ることを示している．

$\gcd(n, \theta) = 1$ の場合　$(n, \theta) = 1$ の場合，$\xi^{q^\theta} + \xi = 0$ となる $\xi \in \mathbb{F}_{q^n}$ は $\mathbb{F}_q$ の元であるため，N_ξ は単位行列の定数倍になり，$P_\Pi \circ N_\xi$ から新たな 2 次式は得られない．したがって，前述の解法を用いることができない．

(2) 式の右辺は C^* の公開鍵の差分 $DP = (dp_1, ..., dp_n)$ にアフィン変換 $T \circ M_{\xi^{q^\theta}+\xi} \circ T^{-1}$ を作用させたものであるため，(2) の左辺の各座標は $dp_1, ..., dp_n$ の各座標の線形和で表現できる．Dubois らは，特殊な $\xi \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$ を用いれば，左辺のいくつかの座標は既知の DP_Π の座標 $dp_1, ..., dp_{n-r}$ の線形和で表現できる可能性に着目した．

[3] では heuristic な議論と数値実験により，$r < (n-2)/3$ であれば，左辺の 3 つの座標が $dp_1, ..., dp_{n-r}$ の線形和で表現できるという条件をつけることで，線型方程式を解くことにより N_ξ を構成できることを示した．[1]

4 ℓIC- 方式とその攻撃

本節では，2007 年に提案された Ding たちの方式 ℓIC [1] と，ℓIC にマイナスオプションをつけて具体的なパラメータを与えた $3IC$- の概略を示し，差分を用いることによって，$3IC$- の公開鍵から $3IC$ の公開鍵を求めることが出来ることを示す．

4.1 ℓIC 方式

[1] において，Ding らは C^* とは異なる central map を用いた多変数 2 次多項式系 ℓIC を提案した．本小節では，ℓIC の central map の概略を示す．

$\mathbb{F}_{q^k} = \mathbb{F}_q(t)$ を k 次拡大体とし，$n = k\ell$ とする．ここで $\mathbb{F}_q$ 上のベクトル空間としての同型写像 $\phi : {\mathbb{F}_q}^n \to {\mathbb{F}_{q^k}}^\ell$

$$(x_1, ..., x_n) \mapsto (x_1 + x_2 t + ... + x_k t^{k-1},\ ...\ , x_{n-k+1} + ... + x_n t^{k-1})$$

によって，${\mathbb{F}_q}^n$ と ${\mathbb{F}_{q^k}}^\ell$ を同一視する．また有限集合 $\{1, ..., \ell\} \subset \mathbb{N}$ に対して

$$\mu : \{1, ..., \ell\} \to \{1, ..., \ell\},\ \mu(i) := \begin{cases} 1 & (\text{for } i = \ell) \\ i+1 & (\text{otherwise}) \end{cases}$$

とする．このとき $F_{\ell IC} : {\mathbb{F}_{q^k}}^\ell \to {\mathbb{F}_{q^k}}^\ell$, $(A_1, ..., A_\ell) \mapsto (B_1, ..., B_\ell)$ を

$$B_1 := \begin{cases} A_1 A_2 & (\ell\text{: odd}) \\ A_1^q A_2 & (\ell\text{: even}) \end{cases},\ B_i := A_i A_{\mu(i)} \text{ for } i \neq 1$$

とする．$F_{\ell IC}$ は $\prod_{i=1}^{\ell} A_i \neq 0$ であれば，$F_{\ell IC}^{-1}$ の計算が可能である．また，$F_{\ell IC}$ を $\mathbb{F}_q$ 上の関数とみなせば，quadratic function になる．このような central map を用いた暗号系を「ℓIC 型の多変数 2 次多項式暗号」と呼ぶ．ℓIC 型の多項式暗号系では，2 つの ${\mathbb{F}_q}^n$ 上のアフィン変換 T, U を秘密鍵として，公開鍵を $P = T \circ F_{\ell IC} \circ U$ とする．

[1] では，C^* からデジタル署名方式 C^{*-} を構成するのと同様にして，ℓIC から デジタル署名方式 ℓIC- を構成している．つまり，$\Pi : {\mathbb{F}_q}^n \to {\mathbb{F}_q}^{n-r}$ を自然な射影 $(x_1, ..., x_n) \mapsto (x_1, ..., x_{n-r})$ とするとき，公開鍵 P_Π を $P_\Pi = \Pi \circ U \circ F_{\ell IC} \circ S$ とする方式が ℓIC-である．また，その実用的なインスタンスとして，$q = 2^8$ とした場合の $3IC$- のパラメータを提案している．そのインスタンスを表 1 に示す．

[1] では，上記の方式を拡張して $r < n/2$ まで N_ξ を構成する方法についても述べられている．

解読計算量	n	ℓ	k	r
2^{80}	30	3	10	10
2^{96}	36	3	12	12
2^{128}	48	3	16	16

表 1: [1] において主張されている $3IC$- の安全性

ただし，[1] では Dubois らによって発表された Asiacrypt 2006 のランプセッションで発表された SFLASH の解析の発表を受けて，ℓIC- の使用は薦めていない．しかし，これは [2, 3] が論文として公開される前であったため，[1] では $3IC$- に対する Dubois らの攻撃の詳細な評価を与えていない．

以下では，$3IC$- に対する Dubois らの差分を用いた攻撃が可能であることを示す．

4.2 差分を用いた $3IC$- の解析

本節では $F_{\ell IC} : (A_1, A_2, A_3) \mapsto (A_1A_2, A_2A_3, A_3A_1)$ を単に F とあらわし，$3IC$ の公開鍵を $P = T \circ F \circ U$, $3IC$- の公開鍵を $P_\Pi = \Pi \circ T \circ F \circ U$ とする．

$(\xi_1, \xi_2, \xi_3) \in {\mathbb{F}_{q^k}}^3$ に対して，

$$\begin{aligned} M_{(\xi_1,\xi_2,\xi_3)} : {\mathbb{F}_{q^k}}^3 &\to {\mathbb{F}_{q^k}}^3 \\ (A_1, A_2, A_3) &\mapsto (\xi_1 A_1, \xi_2 A_2, \xi_3 A_3) \end{aligned}$$

とする．このとき，$F \circ M_{(\xi_1,\xi_2,\xi_3)} = M_{F(\xi_1,\xi_2,\xi_3)} \circ F$ が成り立つ．3.1 節で示したのと同様に，$N_{(\xi_1,\xi_2,\xi_3)} := U^{-1} \circ M_{(\xi_1,\xi_2,\xi_3)} \circ U$ とすれば，

$$\begin{aligned} P_\Pi \circ N_{(\xi_1,\xi_2,\xi_3)} &= \Pi \circ T \circ F \circ U \circ N_{(\xi_1,\xi_2,\xi_3)} \\ &= \Pi \circ T \circ F \circ M_{(\xi_1,\xi_2,\xi_3)} \circ U \\ &= \Pi \circ (T \circ M_{F(\xi_1,\xi_2,\xi_3)}) \circ (F \circ U) \end{aligned}$$

ここで，$T \circ M_{F(\xi_1,\xi_2,\xi_3)}$ が $\{aT; a \in \mathbb{F}_q\}$ と異なる変換を与えていれば，$P_\Pi \circ N_{(\xi_1,\xi_2,\xi_3)}$ の r 個の座標 (の 2 次式) は P_Π の座標 (の 2 次式) とは $\mathbb{F}_q$ 上線形独立であることが期待される．したがって，上記の性質を満たす N_ξ を求めればよい．

$\mathbf{A} = (A_1, A_2, A_3), \mathbf{X} = (X_1, X_2, X_3)$ とするとき，F の差分 DF は

$$DF(\mathbf{A}, \mathbf{X}) = (A_1X_2 + A_2X_1, A_2X_3 + A_3X_2, A_3X_1 + A_1X_3)$$

となる．ここで，簡単な計算から，

$$DF(M_{(\xi_1,\xi_2,\xi_3)}(\mathbf{A}), \mathbf{X}) + DF(\mathbf{A}, M_{(\xi_1,\xi_2,\xi_3)}(\mathbf{X})) = M_{(\xi_1+\xi_2,\xi_2+\xi_3,\xi_3+\xi_1)}(DF(\mathbf{A}, \mathbf{X}))$$

であることがわかる．上記の式より，$a, x \in {\mathbb{F}_q}^n$ と P の差分 $DP(a, x) = T \circ DF(U(a), U(x))$ と P_Π の差分

$DP_\Pi(a,x) = \Pi \circ T \circ DF(U(a), U(x))$ に対して，次の式が成り立つ:

$$DP_\Pi(N_{(\xi_1,\xi_2,\xi_3)}(a), x) + DP_\Pi(a, N_{(\xi_1,\xi_2,\xi_3)}(x)) = \Pi \circ T \circ M_{(\xi_1+\xi_2,\xi_2+\xi_3,\xi_3+\xi_1)} \circ T^{-1}(DP(a,x)). \quad (3)$$

ここで，$\xi_1 = \xi_2 = \xi_3$ とすると，(3) 式の右辺は 0 になる．$DP_\Pi \circ N_{(\xi,\xi,\xi)}$ の各座標は $N_{(\xi,\xi,\xi)} = (\eta_{ij})$ の各成分 η_{ij} の 1 次式で表されるため，連立方程式により $N_{(\xi,\xi,\xi)}$ を求めることが出来る．

評価　ここでは，$N_{(\xi,\xi,\xi)}$ を構成できる r の上限値について議論する．各 (a,x) について，

$$DP_\Pi(L(a), x) + DP_\Pi(a, L(x)) = 0 \quad (4)$$

は各座標で考えると，$L = (\eta_{ij})$ を係数とする $n-r$ 個の方程式を作る．しかし，上記の式は，すべての $a, x \in {\mathbb{F}_q}^n$ に関して成り立つ必要があるため，$a_i x_j$ の係数はすべて 0 でなくてはならない．また，上記の左辺は bilinear かつ symmetric であるため，$a_i x_j$ $(1 \le i < j \le n)$ の係数が 0 であればよい．従って，(η_{ij}) を不定元とする $(n-r)\frac{n(n-1)}{2}$ 個の 1 次方程式が得られる．

一方，$N_{(\xi,\xi,\xi)}$ は，$\xi \in \mathbb{F}_{q^k}$ によって決まるため，$\mathbb{F}_q$ 上 k 次元である．よって，

$$(n-r)\frac{n(n-1)}{2} \ge n^2 - k \quad (5)$$

であれば，$a_i x_j$ $(1 \le i \le j \le n)$ の係数によって定まる方程式で $N_{(\xi,\xi,\xi)}$ を特定するのに十分な方程式が得られると考えられる．したがって，Π によって削除された座標が $r \le r_{\max}$，

$$r_{\max} = n - \left\lceil 2\frac{n^2-k}{n(n-1)} \right\rceil = n - 3 \quad (6)$$

を満たせば，上記の方法から N_ξ を構成することが出来ると思われる．従って，表 1 で示したすべてのパラメータに対して，$N_{(\xi,\xi,\xi)}$ が構成可能である．

上記の議論から $N_{(\xi,\xi,\xi)}$ を構成することが可能となり，$3IC^-$ の公開鍵から $3IC$ の公開鍵を復元することが可能となる．

5　おわりに

本稿では，Ding らの提案した $3IC^-$ の公開鍵の差分をとることによって，heuristic な議論から $3IC$ の公開鍵が復元できることを示した．同様にして ℓIC $(\ell \ne 3)$ の場合にも同様の議論が成立すると考えられる．今後の課題としては，本稿で示した解析の検証実験や，厳密な理論付け，復元した $3IC$ の公開鍵から署名を偽造の可能性について評価する必要がある．

また，他の多変数非線形方程式に基づく方式に対する差分を用いる攻撃の有効性の検証も大きな課題のひとつである．

参考文献

[1] J. Ding, C. Wolf and B. Yang. "ℓ-Invertible Cycles for $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic Public Key Cryptography", In PKC 2007, LNCS 4450, pp. 266-281, Springer-Verlag, 2007.

[2] V. Dubois, P. A. Fouque, and J. Stern. "Cryptanalysis of SFLASH with Slightly Modified Parameters." In EUROCRYPT 2007, LNCS 4515, pp. 264-275, Springer-Verlag, 2007.

[3] V. Dubois, P. A. Fouque, and J. Stern. "Practical Cryptanalysis of SFLASH." In CRYPTO 2007, LNCS 46222, pp. 1-12. Springer-Verlag, 2007.

[4] T. Matsumoto and H. Imai. "Public Quadratic Polynomial-tuples for Efficient Signature-Verification and Message-Encryption." In EUROCRYPT 1988, LNCS 330, pp. 419-453. Springer-Verlag, 1988.

[5] NESSIE. New European Schemes for Signatures Integrity and Encryption. Portfolio of recommended cryptographic primitives. `http://www.nessie.eu.org/index.html`

[6] T. Miyazawa, T. Kobayashi, S. Oda, I. Nakamura and A. Kanai. "Implementation of improved "Quantum public-key cryptosystem"," Proc. of PQCrypto 2006, pp. 181-191 , available at `http://postquantum.cr.yp.to/` (2006).

[7] T. Okamoto, K. Tanaka, and S. Uchiyama."Quantum Public Key Cryptosystems," In CRYTPTO 2000, LNCS 1880, pp. 147-165, Springer-Verlag (2000).

[8] J. Patarin. "Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt' 88." In CRYPTO' 95, LNCS 963, pp. 248-261. Springer-Verlag, 1995.

[9] J. Patarin, N. Courtois, and L. Goubin. "FLASH, a Fast Multivariate Signature Algorithm." In CT-RSA 01, LNCS 2020, pp. 297-307. Springer-Verlag, 2001.

[10] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring", Proc. 35nd Annual Symposium on Foundations of Computer Science (Shafi Goldwasser, ed.), IEEE Computer Society Press (1994), 124-134.