

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第6部門第2区分

【発行日】平成17年12月22日(2005.12.22)

【公表番号】特表2002-543478(P2002-543478A)

【公表日】平成14年12月17日(2002.12.17)

【出願番号】特願2000-616162(P2000-616162)

【国際特許分類第7版】

G 0 9 C 1/00

【F I】

G 0 9 C 1/00 6 4 0 B

G 0 9 C 1/00 6 2 0 Z

【誤訳訂正書】

【提出日】平成16年11月4日(2004.11.4)

【誤訳訂正1】

【訂正対象書類名】明細書

【訂正対象項目名】0 0 1 1

【訂正方法】変更

【訂正の内容】

【0 0 1 1】

本発明においては、 k 個の多項式関数の集合 S_1 は公開鍵として供給される。集合 S_1 は、関数 $P_1(x_1, \dots, x_{n+v}, y_1, \dots, y_k), \dots, P_k(x_1, \dots, x_{n+v}, y_1, \dots, y_k)$ を含むことが好ましい。ここで、 k 、 v 及び n は整数であり、 x_1, \dots, x_{n+v} は第1のタイプの $n+v$ 個の変数であり、 y_1, \dots, y_k は第2のタイプの k 個の変数である。集合 S_1 は秘密鍵演算を k 個の多項式関数 $P'_1(a_1, \dots, a_{n+v}, y_1, \dots, y_k), \dots, P'_k(a_1, \dots, a_{n+v}, y_1, \dots, y_k)$ の集合 S_2 に対して適用することによって得ることが好ましい。ここで、 a_1, \dots, a_{n+v} は n 個の「油」変数 a_1, \dots, a_n の集合と v 個の「酢」変数 a_{n+1}, \dots, a_{n+v} の集合を含む $n+v$ 個の変数である。秘密鍵演算は $n+v$ 個の変数 a_1, \dots, a_{n+v} に対する秘密アフィン変換 s を含むことがあることが理解されよう。

【誤訳訂正2】

【訂正対象書類名】明細書

【訂正対象項目名】0 0 5 2

【訂正方法】変更

【訂正の内容】

【0 0 5 2】

本発明は上で具体的に図示し述べたものに制限されることはないことが当業者には理解されよう。むしろ、本発明の範囲は請求項によって定義されるものである。

[表1]

アペンディックス I

不平衡な「油と酢」署名スキーム

A v i a d K i p n i s

N D S T e c h n o l o g i e s

5 H a m a r p e S t . H a r H o t z v i m

J e r u s a l e m - I s r a e l

a k i p n i s @ n d s i s r a e l . c o m

J a c q u e s P a t a r i n , L o u i s G o u b i n
 B u l l S m a r t C a r d s a n d T e r m i n a l s
 6 8 , r o u t e d e V e r s a i l l e s - B P 4 5
 7 8 4 3 1 L o u v e c i e n n e s C e d e x - F r a n c e
 { J . P a t a r i n , L . G o u b i n } @ f r l v . b u l l . f r

要約

[16]で、J. Patarinは、非対称署名を計算するための「油と酢」と呼ばれる新しいスキームを設計した。これは非常に単純なものであり、(秘密鍵と公開鍵の両方で)非常に高速な計算が可能で、スマートカードに実装するときにRAMをほとんど必要としない。このアイデアは、「油」と呼ばれる n 個の未知数と「酢」と呼ばれる $v = n$ 個の未知数により、有限体 K 上で線形秘密関数を用いて二次方程式を隠蔽することにある。この原型のスキームは、A. KipnisとA. Shamirによる[10]で解読されている。本論文では、($v = n$ の代わりに) $v > n$ を用いた、原型のスキームの非常に簡単な変種について研究する。「油」の未知数よりも「酢」の未知数を多くしたため、これらのスキームは「不平衡な油と酢」(UOV)と呼ばれる。

【数1】

$$v \cong n$$

であるときは、[10]の攻撃を拡張することができるが、例えば $v = 2n$ であるときは、スキームの安全保障は依然として未解決の問題である。さらに、

【数2】

$$v \cong \frac{n^2}{2}$$

であるときは、スキームの安全保障は、(非常に自然であるが証明されていない特性を受け入れるとすれば)

【数3】

$$\frac{n^2}{2}$$

個の未知数を持つ n 個の二次方程式の(トラップドアのない)ランダム集合を解く問題とまったく同等である。しかし、(標数2で) $v = n^2$ であるときは、解法を見つけることは一般的には容易であることを示す。次に、「油と酢」アイデアと[14]のHFEスキームを結合することは非常に容易であることを示す。結果として生じるHFEVと呼ばれるスキームは、実用的な観点と理論的な観点の両方から、現時点でも非常に興味深いものと考えられる。UOV署名の長さは192ビットにまで短縮でき、HFEVでは80ビットにまで短縮が可能である。

注： 本論文の拡張版は、著者から入手することができる。

1. 序文

1985年以降、様々な著者([7]、[9]、[12]、[14]、[16]、[17]、[18]、[21]を参照)が、小さい有限体 K 上の多変量二次方程式(またはより高次の方程式)の集合として公開鍵が与えられる公開鍵スキームを提案してきた。

そのような方程式の集合の解を求める一般的な問題は(二次の場合であっても)NP困難である([8]参照)。さらに、未知数の数が例えば $n = 16$ であるときに、最も周知のアルゴリズムでも、しばしば全数検索より有意に優れているとは言えない(n が非常に小さいときはGroebnerベースのアルゴリズムがより効率的である。[6]参照)。

このスキームは、スマートカード実装で必要な速度またはRAMの点から見てしばしば非常に効率的である。(しかし、公開鍵の長さは一般的には1Kバイト以上である。いずれにせよ、公開鍵なしに秘密鍵計算を実行できることに注目することも時には有用である

。) 最も深刻な問題は、(秘密が既知であるときに署名の計算を可能にする、またはメッセージの復号を可能にする目的で) トラップドアを導入するためには、生成される公開方程式の集合は、一般的には生成し得るすべての方程式の小さいサブ集合の 1 つとなり、多くの場合アルゴリズムが解読されていることである。例えば、[7] はその著者によって解読され、[1 2]、[1 6]、[2 1] は解読されている。しかし、多くのスキームはまだ解読されておらず (例えば、[1 4]、[1 7]、[1 8]、[2 0])、また多くの場合、スキームを修復するためにいくつかの非常に単純な変種が提案されている。したがって現時点では、小さい有限体上の多変量多項式で公開鍵アルゴリズムを設計するこのアイデアが (一部のきわめて単純なスキームのみが安全保障されていない中) 非常に強力なアイデアであるかどうかはわからない。

本論文では、2 つの新しいスキーム、U O V および H F E V を提示する。U O V は非常に単純なスキームである。すなわち、([1 6] の) 原型の「油と酢」署名スキームは解読された ([1 0] を参照) が、「油」未知数より「酢」未知数を有意に多くすると (「油」未知数と「酢」未知数の定義はセクション 2 にある)、[1 0] の攻撃は成功せず、(U O V と呼ばれる) このより一般的なスキームの安全保障はなお未解決の問題である。(2 の代わりに) 次数 3 の「油と酢」スキームも調べる。その後、H F E V と呼ばれる別のスキームも提示する。H F E V は、([1 4] の) H F E のアイデアと酢変数のアイデアを結び付けている。H F E V は、原型の H F E スキームより効率的であるように思われる。最後に、セクション 1 3 で、多変量多項式のこの領域の主要スキームについてわかっていることを提示する。

2 . 次数 2 の場合の (原型のおよび不平衡な) 「油と酢」

$K = F_q$ が小さい有限体であるとする (例えば、 $K = F_2$)。n および v は 2 つの整数であるとする。署名されるメッセージ (またはそのハッシュ) は、 $y = (y_1, \dots, y_n)$ によって示される K^n のエレメントとして表される。一般的には、

【数 4】

$$q^n \equiv 2^{128}$$

である (セクション 8 では

【数 5】

$$q^n \equiv 2^{64}$$

も可能であることを示す)。署名 x は、 $x = (x_1, \dots, x_{n+v})$ によって示される K^{n+v} のエレメントとして表される。

秘密鍵

秘密鍵は、以下の 2 つの部分から成る。

1 . 全単射アファイン関数 $s : K^{n+v} \rightarrow K^{n+v}$ 。「アファイン」とは、出力の各構成要素を、K のエレメントを係数として、n + v 個の入力未知数を持つ次数 1 の多項式として記述できることを意味する。

2 . 以下のタイプの n 個の方程式の集合 (S) :

【数 6】

$$\forall i, 1 \leq i \leq n, y_i = \sum \gamma_{ijk} a_j a'_k + \sum \lambda_{ijk} a'_j a'_k + \sum \xi_{ij} a_j + \sum \xi'_{ij} a'_j + \delta_i \quad (S)$$

係数 γ_{ijk} 、 λ_{ijk} 、 ξ_{ij} 、 ξ'_{ij} および δ_i は、これらの n 個の方程式の秘密係数である。値 a_1, \dots, a_n (「油」未知数) および a'_1, \dots, a'_v (「酢」未知数) は、K のエレメントである。これらの方程式 (S) は、 $a_i a_j$ の項を含まないことに注意が必要である。

公開鍵

A は、 $A = (a_1, \dots, a_n, a'_1, \dots, a'_v)$ によって定義される K^{n+v} のエレメントであるとする。A は $x = s^{-1} (A)$ に変換されるが、ここでの s は K^{n+v} か

ら K^{n+v} への秘密の全単射アフィン関数である。各値 y_i ($1 \leq i \leq n$) は、 x_j 個の未知数 ($1 \leq j \leq n+v$) を持つ合計次数 2 の多項式 P_i として書くことができる。 (P) は、以下の n 個の方程式の集合を表す。

【数 7】

$$\forall i, 1 \leq i \leq n, y_i = P_i(x_1, \dots, x_{n+v}) \quad (P)$$

($n+v$ 個の未知数 x_j を持つ) これら n 個の二次方程式 (P) が公開鍵である。

(秘密鍵での) 署名の計算

y の署名 x の計算を以下のように行う。

ステップ 1: n 個の方程式 (S) を満足するような、 K のエレメントである n 個の未知数 a_1, \dots, a_n および K のエレメントである v 個の未知数 a'_1, \dots, a'_v を見つける。これは、以下のように行うことができる。 v 個の酢未知数 a'_i をランダムに選択し、(S) から未知数 a_i をガウス消去法によって計算する (a_i, a_j 項はないので、 a'_i が固定されると (S) 方程式は未知数 a_i でアフィンであるため)。

注釈: 解が見つからない場合は、新しいランダムな酢の未知数を用いて再び試みる。 F_q 上の $n \times n$ 行列が可逆である確率は僅少ではないので、数回の試みの後、少なくとも 1 つの解を得る確率は非常に高い。(この確率は正確には、

【数 8】

$$\left(1 - \frac{1}{q}\right) \left(1 - \frac{1}{q^2}\right) \cdots \left(1 - \frac{1}{q^{n-1}}\right)$$

である。 $q = 2$ では、これは約 30% となり、 $q > 2$ では、この確率はさらに高くなる。

)

ステップ 2: $x = s^{-1}(A)$ を計算する。ここで、 $A = (a_1, \dots, a_n, a'_1, \dots, a'_v)$ であり、 x は y の署名である。

署名の公開検証

y の署名 x は、すべての (P) が満足される場合のみ有効である。その結果、署名が有効であるかをチェックするために秘密は必要ない。これは非対称署名スキームである。

注: 名前「油と酢」は、方程式 (S) で、「油未知数」 a_i と「酢未知数」 a'_j はまったく混じり合わない、すなわち、 a_i, a_j 積がないという事実由来する。しかし、(P) では、この特性は、 s 変換による未知数の「混じり合い」によって隠蔽される。この特性は「十分に隠蔽される」だろうか。実際、この質問は「スキームは安全保障されているか」ということを意味している。 $v = n$ であるスキームは [16] で最初に提示されたので、「原型の油と酢」と呼ぶ。このケースは [10] で解読された。[10] の暗号分析は、 $v < n$ である場合もまったく同じ方法で通用することが非常に簡単にわかる。しかし、ケース $v > n$ は、以下に示すようにはるかに難しい。 $v > n$ であるときに、スキームを「不平衡な油と酢」と呼ぶ。

3. ケース $v = n$ の暗号分析 ([10] より)

[10] の攻撃のアイデアは、本質的には以下のとおりである。すなわち、油変数と酢変数を分離するため、(P) の n 個の公開方程式の二次形式に注目し、線形項をしばらく省略する。 G_i ($1 \leq i \leq n$) は、公開方程式 (P) の各 P_i の二次形式の行列であるとする。集合 (S) にある方程式の二次部分に対応する $2n \times 2n$ 行列

【数 9】

$$\begin{pmatrix} 0 & A \\ B & C \end{pmatrix}$$

での二次形式として表される。この左上の $n \times n$ ゼロ部分行列は、油変数は油変数によっ

て乗算されないという事実による。内部変数を線形関数 s で隠蔽した後、行列

【数 1 0】

$$G_i = S \begin{pmatrix} 0 & A_i \\ B_i & C_i \end{pmatrix} S^t$$

の表現を得る。 S は $2n \times 2n$ の可逆行列である。

定義 3.1: 油部分空間は、後半分がゼロのみである K^{2n} の全ベクトルで構成された線形部分空間と定義する。

定義 3.2: 酢部分空間は、前半分がゼロのみである K^{2n} の全ベクトルで構成された線形部分空間と定義する。

補題 1 E および F が左上に $n \times n$ のゼロ部分行列を持つ $2n \times 2n$ 行列であるとする。 F が可逆である場合は、油部分空間は $E F^{-1}$ の不変部分空間である。

証明: [1 0] を参照されたい。

定義 3.4: 可逆行列 G_j に対して、 G_{ij} を $G_{ij} = G_i G_j^{-1}$ と定義する。

定義 3.5: O を S^{-1} による油部分空間の像とする。

油部分空間を見つけるため、以下の定理を使用する。

定理 3.1 O は、すべての行列 G_{ij} に共通の不変部分空間である。

証明:

【数 1 1】

$$\begin{aligned} G_{ij} &= S \begin{pmatrix} 0 & A_i \\ B_i & C_i \end{pmatrix} S^t (S^t)^{-1} \begin{pmatrix} 0 & A_j \\ B_j & C_j \end{pmatrix} S^{-1} \\ &= S \begin{pmatrix} 0 & A_i \\ B_i & C_i \end{pmatrix} \begin{pmatrix} 0 & A_j \\ B_j & C_j \end{pmatrix}^{-1} S^{-1} \end{aligned}$$

2つの内部行列は、補題 1 の E および F の形式を持つ。したがって、油部分空間は内部項の不変部分空間であり、 O は $G_i G_j^{-1}$ の不変部分空間である。行列集合の共通の不変部分空間を発見する問題は、[1 0] で研究されている。[1 0] のアルゴリズムを適用すると、 O が得られる。 $V + O = K^{2n}$ であるように次元 n の任意部分空間である V を選択すると、同等の油と酢の分離が得られる。そのような分離が得られたら、省略した線形項を戻し、酢変数にランダムな値を選択すると、 n 個の油変数を持つ n 個の線形方程式の集合が残る。

注: $v > n$ であるときは、補題 1 はもはや真ではない。油部分空間は、この場合も E および F によって酢部分空間に写像されるが、 F^{-1} は油部分空間の E による像を必ずしも油部分空間に写像し戻さない。これが、原型の油と酢の暗号分析が、不平衡のケースには有効でない理由である。

4. $v > n$ および $v = n$ であるときの暗号分析

このセクションでは、 $v - n$ が小さい (より正確には、攻撃の予想される複雑さがおおよそ $q^{(v-n)-1} \cdot n^4$ である) かぎり、適用できる上記の攻撃の修正について説明する。

定義 4.1: このセクションでは、油部分空間を、最後の v 座標がゼロのみである K^{n+v} の全ベクトルで構成された線形部分空間と定義する。

定義 4.2: このセクションでは、酢部分空間を、最初の n 座標がゼロのみである K^{n+v} の全ベクトルで構成された線形部分空間と定義する。

このセクションでは、方程式の同次二次項から始める。すなわち、線形項をしばらく省略する。行列 G_i は、以下で表される。

【数 1 2】

$$G_i = S \begin{pmatrix} 0 & A_i \\ B_i & C_i \end{pmatrix} S'$$

上の式で、左上行列は $n \times n$ ゼロ行列、 A_i は $n \times v$ 行列、 B_i は $v \times n$ 行列、 C_i は $v \times v$ 行列、 S は $(n + v) \times (n + v)$ の可逆線形行列である。

定義 4 . 3 : E_i を

【数 1 3】

$$\begin{pmatrix} 0 & A_i \\ B_i & C_i \end{pmatrix}$$

と定義する。

補題 2 形式

【数 1 4】

$$\begin{pmatrix} 0 & A \\ B & C \end{pmatrix}$$

を持つ任意の行列 E に対して、以下が真である。

a) E は、油部分空間を酢部分空間に変換する。

b) 行列 E^{-1} が存在する場合、 E^{-1} による酢部分空間の像は、その中に n 次元油部分空間を包含する次元 v の部分空間である。

証明： a) 油部分空間および酢部分空間の定義から直接導かれる。a) が与えられると、b) が結果として即座に導かれる。

我々が提案しているアルゴリズムは、確率論的である。このアルゴリズムは、 S によって変換された後の油部分空間の不変部分空間を探すものである。最初の試みでアルゴリズムが成功する確率は、低い。したがって、入力を様々に変えてアルゴリズムを繰り返す必要がある。行列 E_1, \dots, E_n の任意の線形結合もまた形式

【数 1 5】

$$\begin{pmatrix} 0 & A \\ B & C \end{pmatrix}$$

を持つ、という特性を利用する。下の定理は、不変部分空間が一定の確率で存在する理由を説明している。

定理 4 . 1 F が行列 E_1, \dots, E_n の可逆線形結合であるとする。その場合、 E_k^{-1} が存在する任意の k に対して、行列 $F E_k^{-1}$ は、 $d = v - n$ の場合に

【数 1 6】

$$\frac{q-1}{q^{2d}-1}$$

以上の確率で、油部分空間の部分空間でもある自明でない不変部分空間を持つ。

証明： 本論文の拡張版を参照されたい。

注： 予想される数の固有ベクトルに対してはるかに少ない労力で、よりよい結果を得ることができる。すなわち、 E_1 は $n - d$ 以上の次元を持つ部分空間であり、 $F E_k^{-1}$ によって次元 n の部分空間に写像される。ゼロでないベクトルがそれ自体のゼロでないスカラー倍のベクトルに写像される確率は、

【数 1 7】

$$\frac{q-1}{q^n-1}$$

である。期待値を得るため、 I_1 にあるゼロでないベクトルの数をそれに乗算する。こうすると、

【数 1 8】

$$\frac{(q-1)(q^{n-d}-1)}{q^n-1}$$

以上である値が得られる。すべての固有ベクトルは $q-1$ 回ずつ数えられているので、次元 1 の不変部分空間の予想される数は、

【数 1 9】

$$\frac{q^{n-d}-1}{q^n-1} \sim q^{-d}$$

以上である。

O をセクション 3 のように定義すると、 O に対して次の結果が得られる。

定理 4.2 F が行列 G_1, \dots, G_n の可逆線形結合であるとする。その場合、 G_k^{-1} が存在する任意の k に対して、行列 $F G_k^{-1}$ は、 $d = v - n$ の場合に

【数 2 0】

$$\frac{q-1}{q^{2d}-1}$$

以上の確率で、 O の部分空間でもある自明でない不変部分空間を持つ。

証明：

【数 2 1】

$$\begin{aligned} FG_k^{-1} &= (\alpha_1 G_1 + \dots + \alpha_n G_n) G_k^{-1} \\ &= S (\alpha_1 E_1 + \dots + \alpha_n E_n) S^t (S^t)^{-1} E_k^{-1} S^{-1} = S (\alpha_1 E_1 + \dots + \alpha_n E_n) E_k^{-1} S^{-1} \end{aligned}$$

内部項は、要求されている確率を持つ油部分空間の不変部分空間である。したがって、同じことが $F G_k^{-1}$ に対しても真であるが、油部分空間の部分空間の代わりに、 O の部分空間を得る。

O をどのように見つけるか

G_1, \dots, G_n のランダムな線形結合を使用し、それに G_k 行列のうちの 1 つの逆行列を乗算する。次に、この行列のすべての最小不変部分空間を計算する（行列 A の最小不変部分空間は、行列 A の自明でない不変部分空間を含まない。これらの部分空間は、 A の固有多項式の既約因数に対応する）。これは、標準線形代数法を使用して確率的多項式時間で行うことができる。この行列は、 O の部分空間である不変部分空間を持つ場合がある。

次の補題は、 O に包含されている部分空間とランダムな部分空間とを区別できるようにする。

補題 3 H が線形部分空間であり、 $H \subseteq O$ である場合、 H のすべての x, y およびすべての i に対して、 $G_i(x, y) = 0$ である（ここでは G_i を双線形形式と考える）。

証明： $x' = xS$ および $y' = yS$ であるような x' および y' が油部分空間に存在する。

【数 2 2】

$$G_i(x, y) = xS \begin{pmatrix} 0 & A_i \\ B_i & C_i \end{pmatrix} S' y' = x' \begin{pmatrix} 0 & A_i \\ B_i & C_i \end{pmatrix} (y')' = 0$$

x' および y' は油部分空間にあるので、最後の項はゼロである。

補題 3 は、 O の部分空間とランダムな部分空間とを区別する多項式テストを与える。使用する行列が O の部分空間でもある最小部分空間を持っていない場合は、 G_1, \dots, G_n の別の線形結合を選択し、それに G_k 行列のうちの 1 つの逆行列を乗算し、再び試みる。このプロセスを約 q^{d-1} 回繰り返した後、かなりの確率で O の少なくとも 1 つのゼロベクトルを見つけることができる。 n 個の独立した O のベクトルを得るまで、このプロセスを続ける。これらのベクトルが O を張る。プロセスの予想される複雑さは、 $q^{d-1} \cdot n^4$ に比例する。ここでは、自明でない不変部分空間を見つけ、各試行で実行する必要がある線形代数演算を項 n^4 がすべて網羅するまでに予想される試行回数を使用する。

5. ケース

【数 2 3】

$$v \cong \frac{n^2}{2}$$

(または

【数 2 4】

$$v \geq \frac{n^2}{2}$$

)

特性

(A) が $(n + v)$ 個の変数 x_1, \dots, x_{n+v} を持つ n 個の二次方程式のランダム集合であるとする(「ランダム」という表現は、これらの方程式の係数が一様かつランダムに選択されていることを意味している)。

【数 2 5】

$$v \cong \frac{n^2}{2}$$

(より一般的には

【数 2 6】

$$v \geq \frac{n^2}{2}$$

)である場合、おそらく、そのような(A)の大部分に対して、 (x'_1, \dots, x'_{n+v}) で記述された(A)の方程式の集合(A')が「油と酢」系である(すなわち、 i n かつ j n で、 $x'_i \cdot x'_j$ の項がない)ような変数の線形変換 $(x_1, \dots, x_{n+v}) \rightarrow (x'_1, \dots, x'_{n+v})$ が存在する。

この特性を正当化する論拠

以下であるとする。

【数 2 7】

$$\begin{cases} x_1 = \alpha_{1,1}x'_1 + \alpha_{1,2}x'_2 + \cdots + \alpha_{1,n+v}x'_{n+v} \\ \vdots \\ x_{n+v} = \alpha_{n+v,1}x'_1 + \alpha_{n+v,2}x'_2 + \cdots + \alpha_{n+v,n+v}x'_{n+v} \end{cases}$$

すべての $x'_i \cdot x'_j$ ($i = 1 \sim n$ かつ $j = 1 \sim n+v$) に対応する (A) の n 個すべての方程式の係数をゼロと記述することによって、 $(n+v) \cdot n$ 個の変数 x'_i, x'_j ($i = 1 \sim n, j = 1 \sim n+v$) を持つ

【数 2 8】

$$n \cdot n \cdot \frac{n+1}{2}$$

個の二次方程式の系が得られる。したがって v 約

【数 2 9】

$$\frac{n^2}{2}$$

であるときは、(A) の大部分に対して方程式のこの系の解を得られると予想することができる。

注釈：

1. この論拠はきわめて自然であるが、完全な数学的証明ではない。
2. 系は解を持つかもしれないが、解を見つけることは難しい問題になると思われる。これが、(適切に選択されたパラメータに対して) 不平衡な「油と酢」スキームが安全保障され得る理由である。すなわち、問題の解決を容易にする変数の線形変換が常に存在するが、そのような変数変換を見つけることは難しいと思われる。
3. セクション 7 では、このセクションの結果にもかかわらず、(少なくとも標数 2 での) $v = n^2$ の選択は推奨されないことを示す。

6. k 個の未知数 ($k > n$) を持つ n 個の二次方程式の集合を解くことは NP 困難である

(本論文の拡張版を参照されたい。)

7. n^2 個 (以上) の未知数を持つ n 個の二次方程式のランダムな集合を解くための (常にではないが) 一般的に効率的なアルゴリズム

このセクションでは、 $v = n^2$ であるときに、 $n+v$ 個の変数を持つ n 個のランダムに選択した二次方程式の系を解くアルゴリズムを説明する。

(S) が以下の系であるとする。

【数 3 0】

$$(S) \begin{cases} \sum_{1 \leq i \leq j \leq n+v} a_{ij1} x_i x_j + \sum_{1 \leq i \leq n+v} b_{i1} x_i + \delta_1 = 0 \\ \vdots \\ \sum_{1 \leq i \leq j \leq n+v} a_{ijn} x_i x_j + \sum_{1 \leq i \leq n+v} b_{in} x_i + \delta_n = 0 \end{cases}$$

アルゴリズムの主なアイデアは、以下のような変数の変換を使用することにある。

【数 3 1】

$$\begin{cases} x_1 = \alpha_{1,1}y_1 + \alpha_{2,1}y_2 + \cdots + \alpha_{n+v,1}y_{n+v} \\ \vdots \\ x_{n+v} = \alpha_{1,n+v}y_1 + \alpha_{2,n+v}y_2 + \cdots + \alpha_{n+v,n+v}y_{n+v} \end{cases}$$

(これらの新しい変数 y_1, \dots, y_{n+v} で記述された) 結果の系 (S') を解くのが容易になるように、上記の $\alpha_{i,j}$ 係数 ($1 \leq i \leq n, 1 \leq j \leq n+v$) を段階的に見つける。

・まず、 $\alpha_{1,1}, \alpha_{1,2}, \dots, \alpha_{1,n+v}$ をランダムに選択する。
 ・次に、(S') が y_1, y_2 項を含まないように $\alpha_{2,1}, \alpha_{2,2}, \dots, \alpha_{2,n+v}$ を求める。
 この条件によって、($n+v$) 個の未知数 $\alpha_{2,j}$ ($1 \leq j \leq n+v$) を持つ n 個の線形方程式から成る系が得られる。

【数 3 2】

$$\sum_{1 \leq i \leq j \leq n+v} a_{ijk} \alpha_{1,i} \alpha_{2,j} = 0 \quad (1 \leq k \leq n)$$

・次に、(S') が y_1, y_3 項または y_2, y_3 項のいずれも含まないように $\alpha_{3,1}, \alpha_{3,2}, \dots, \alpha_{3,n+v}$ を求める。この条件は、($n+v$) 個の未知数 $\alpha_{3,j}$ ($1 \leq j \leq n+v$) を持つ $2n$ 個の線形方程式から成る以下の系と同等である。

【数 3 3】

$$\begin{cases} \sum_{1 \leq i \leq j \leq n+v} a_{ijk} \alpha_{1,i} \alpha_{3,j} = 0 & (1 \leq k \leq n) \\ \sum_{1 \leq i \leq j \leq n+v} a_{ijk} \alpha_{2,i} \alpha_{3,j} = 0 & (1 \leq k \leq n) \end{cases}$$

・以下同様に進める。
 ・最後に、(S') が y_1, y_n 項、 y_2, y_n 項、 \dots 、 y_{n-1}, y_n 項のいずれも含まないように $\alpha_{n,1}, \alpha_{n,2}, \dots, \alpha_{n,n+v}$ を求める。この条件によって、($n+v$) 個の未知数 $\alpha_{n,j}$ ($1 \leq j \leq n+v$) を持つ $(n-1)n$ 個の線形方程式から成る以下の系が得られる。

【数 3 4】

$$\begin{cases} \sum_{1 \leq i \leq j \leq n+v} a_{ijk} \alpha_{1,i} \alpha_{n,j} = 0 & (1 \leq k \leq n) \\ \vdots \\ \sum_{1 \leq i \leq j \leq n+v} a_{ijk} \alpha_{n-1,i} \alpha_{n,j} = 0 & (1 \leq k \leq n) \end{cases}$$

一般的には、これらのすべての線形方程式は、(ガウス消去法によって発見される) 少なくとも 1 つの解を与える。特に、 $n(n-1)$ 個の方程式と ($n+v$) 個の未知数の最後の系は、一般的には $n+v > n(n-1)$ 、すなわち $v > n(n-2)$ になると直ちに 1 つの解を与えるが、これは仮説によって真である。

さらに、 n 個のベクトル

【数 3 5】

$$\begin{pmatrix} \alpha_{1,1} \\ \vdots \\ \alpha_{1,n+v} \end{pmatrix}, \dots, \begin{pmatrix} \alpha_{n,1} \\ \vdots \\ \alpha_{n,n+v} \end{pmatrix}$$

は、ランダム二次系 (S) に対して線形に独立である可能性がきわめて高い。

残りの i, j 個の定数 (すなわち、 $n+1 \leq i \leq n+v$ かつ $1 \leq j \leq n+1$ である定数) は、変数の全単射変換を得るように、ランダムに選択されている。

これらの新しい変数 y_i で系 (S) を記述し直すことによって次の系が得られる。

【数 3 6】

$$(S') \begin{cases} \sum_{i=1}^n \beta_{i,1} y_i^2 + \sum_{i=1}^n y_i L_{i,1}(y_{n+1}, \dots, y_{n+v}) + Q_1(y_{n+1}, \dots, y_{n+v}) = 0 \\ \vdots \\ \sum_{i=1}^n \beta_{i,n} y_i^2 + \sum_{i=1}^n y_i L_{i,n}(y_{n+1}, \dots, y_{n+v}) + Q_n(y_{n+1}, \dots, y_{n+v}) = 0 \end{cases}$$

この系で、各 $L_{i,j}$ はアファイン関数であり、各 Q_i は二次関数である。

次に、以下を満たす y_{n+1}, \dots, y_{n+v} を求める。

【数 3 7】

$$\forall i, 1 \leq i \leq n, \forall j, 1 \leq j \leq n+v, L_{i,j}(y_{n+1}, \dots, y_{n+v}) = 0$$

一般的には、 $v = n^2$ であるかぎり少なくとも 1 つの解が存在する n^2 個の方程式と v 個の未知数の線形系を解かなければならないので、これは可能である。これらの解の 1 つを選択する。一般的には、ガウス消去法によって y_i^2 が与えられる。

次に、標数 2 においては、 $x \mapsto x^2$ は全単射であるため、 y_i^2 のこの表現から y_i の解が容易に見つかる。2 以外の標数では、 2^n が大きすぎないときに (例えば、 $n = 40$ であるときなど) 成功する。 n が大きいときは、二次形式の一般理論に基づいて解を見つける方法がある。スペースがないため、この方法は本論文の拡張版で説明する。

8. 半分のサイズの署名での変種

セクション 2 で説明した UOV では、公開鍵は、 $1 \leq i \leq n$ とした n 個の二次方程式 $y_i = P_i(x_1, \dots, x_{n+v})$ の集合であり、 $y = (y_1, \dots, y_n)$ は署名されるメッセージのハッシュ値である。衝突のないハッシュ関数を使用する場合は、ハッシュ値は少なくとも長さ 128 ビットでなければならない。したがって、 q^n は少なくとも 2^{128} でなければならない。そのため、 $v = 2n$ の場合、署名の典型的な長さは少なくとも $3 \times 128 = 384$ ビットである。

ここでわかるように、半分のサイズの署名を得るために署名設計で小さい変種を作ることが可能である。ここでは、(同じ関連する秘密鍵を持つ) 同じ多項式 P_i を用いるが、ここでチェックする公開方程式は以下とする。

【数 3 8】

$$\forall i, P_i(x_1, \dots, x_{n+v}) + L_i(y_1, \dots, y_n, x_1, \dots, x_{n+v}) = 0$$

この式で、 L_i は (x_1, \dots, x_{n+v}) に基づく線形関数であり、 L_i の係数は、 (y_1, \dots, y_n) に基づくハッシュ関数によって生成される。

例えば、 $(x_1, x_2, \dots, x_{n+v}) = \text{Hash}(y_1, \dots, y_n \parallel i)$ の $L_i(y_1, \dots, y_n, x_1, \dots, x_{n+v}) = x_1 + x_2 + \dots + x_{n+v}$ である。ここで、 $(q^n = 2^{128})$ の代わりに $q^n = 2^{64}$ であるように n を選択するこ

とができる。(注：解 x について全数検索を避けるには、 q^n は 2^{64} 以上でなければならない。) $v = 2n$ および

【数 39】

$$q^n \cong 2^{64}$$

である場合は、署名の長さは $3 \times 64 = 192$ ビットになる。

9. 次数 3 の油と酢

スキーム

セクション 2 で説明した二次「油と酢」スキームは、より高い次数に容易に拡張することができる。次数 3 の場合、隠蔽方程式の集合 (S) は、すべての $i \in n$ に対して以下のタイプのものである。

【数 40】

$$y_i = \sum \gamma_{ijk} a_j a'_k a'_l + \sum \mu_{ijkl} a'_j a'_k a'_l + \sum \lambda_{ijk} a'_j a'_k \\ + \sum \nu_{ijk} a'_j a'_k + \sum \xi_{ij} a_j + \sum \xi'_{ij} a'_j + \delta_i \quad (S)$$

係数 γ_{ijk} 、 μ_{ijkl} 、 λ_{ijk} 、 ν_{ijk} 、 ξ_{ij} 、 ξ'_{ij} および δ_i は、これらの n 個の方程式の秘密係数である。これらの方程式 (S) は、 a_j 、 a_k 、 a_l または a'_j 、 a'_k の項を持たないことに注意する必要がある。未知数 a'_k が固定されると、これらの方程式は未知数 a_j でアファインとなる。

公開鍵の計算、署名の計算および署名の検証は、前と同じように行われる。

$v = n$ であるときの次数 3 の「油と酢」の最初の暗号分析

公開鍵の二次部分を見て、次数 2 の「油と酢」に対してとまったく同じ方法でそれを攻撃することができる。これは、 $v = n$ であるときに成功すると予想される。

注：二次部分がない（すなわち、公開鍵が次数 3 と同質である）場合、またはこの攻撃がうまくいかない場合は、変数のランダムなアファイン変換を適用してもう一度試みるのが常に可能である。

【数 41】

$$v \leq (1 + \sqrt{3})n$$

であり、 K が標数 2 以外であるときの次数 3 の「油と酢」の暗号分析 (D. Coppersmith のアイデアより、[4] 参照)

主なアイデアは、ある方向での「線形性」を検出することである。以下になるような値 $d = (d_1, \dots, d_{n+v})$ の集合 V を探す。

【数 42】

$$\forall x, \forall i, 1 \leq i \leq n, P_i(x+d) + P_i(x-d) = 2P_i(x) \quad (\#)$$

各 x_k の中間値がゼロ係数を持つように記述することによって、 $(n+v)$ 個の未知数 d_j を持つ $n \cdot (n+v)$ 個の二次方程式が得られる。

(各単項式 $x_i x_j x_k$ では、 $(x_j + d_j)(x_k + d_k)(x_l + d_l) + (x_j - d_j)(x_k - d_k)(x_l - d_l) - 2x_j x_k x_l$ 、すなわち、 $2(x_j d_k d_l + x_k d_j d_l + x_l d_j d_k)$ となる。)

さらに、正しい d のベクトル空間は次元 n であるため、暗号分析者は d の約 $n-1$ 個の座標 d_k を指定することができる。したがって、 $(v+1)$ 個の未知数 d_j を持つ $n \cdot (n+v)$ 個の二次方程式を解くことが残る。 v が大きすぎないとき（典型的には、

【数 4 3】

$$\frac{(v+1)^2}{2} \leq n(n+v)$$

であるとき、すなわち、

【数 4 4】

$$v \leq (1 + \sqrt{3})n$$

であるとき)は、これは容易であると予想される。結果として、 v 約

【数 4 5】

$$(1 + \sqrt{3})n$$

であり、 $|K|$ が奇数であるときは、スキームを解読する簡単な方法が与えられる。

注 1: v が

【数 4 6】

$$(1 + \sqrt{3})n$$

よりかなり大きいとき(これは二次のケースで見たものよりも不平衡な限界である)は、現時点ではスキームを解読する方法は不明である。

注 2: まったく奇妙なことに、次数 3 の「油と酢」スキームのこの暗号分析は、次数 2 の「油と酢」スキームでは使えない。理由は、次数 2 では、

【数 4 7】

$$\forall x, \forall i, 1 \leq i \leq n, P_i(x+d) + P_i(x-d) = 2P_i(x)$$

と記述すると、 $(n+v)$ 個の未知数 d_j を持つ次数 2 の方程式が n 個しか与えられないことによる(解を求める方法は不明である)。(各単項式 $x_j x_k$ では、 $(x_j + d_j)(x_k + d_k) + (x_j - d_j)(x_k - d_k) - 2x_j x_k$ 、すなわち、 $2d_j d_k$ となる。)

注 3: 次数 2 では、不平衡な「油と酢」公開鍵は、

【数 4 8】

$$v \cong \frac{n^2}{2}$$

であるときに n 個の二次方程式のほとんどすべての集合を網羅すると予想されることを見てきたが、次数 3 でも同様の特性が見られる。すなわち、

【数 4 9】

$$v \cong \frac{n^3}{6}$$

であるときは、公開鍵は n 個の三次方程式のほとんどすべての集合を網羅すると予想される(証明は同様である)。

10. もう 1 つのスキーム: HFEV

「最も単純な」HFEスキーム([14]の表記を使用する)では、 $b = f(a)$ であり、 $f(a)$ は以下の形態を持つ。

【数 5 0】

$$f(a) = \sum_{i,j} \beta_{ij} a^{q^{ij} + q^{\varphi_{ij}}} + \sum_i \alpha_i a^{q^{\varepsilon_i}} + \mu_0, \quad (1)$$

上記の β_{ij} 、 α_i および μ_0 は、体

【数 5 1】

$$F_{q^n}$$

の元素である。 v は整数であるとする (v は、追加の x_i 変数の数、すなわち、スキームに追加する「酢」変数の数になる)。 $a' = (a'_1, \dots, a'_v)$ が K の変数の v タプルであるとする。今度は、(1) の各 i が、基底における各 n 個の i 構成元素が、酢変数 a'_1, \dots, a'_v の秘密ランダム線形関数であるような

【数 5 2】

$$F_{q^n}$$

の元素であるとする。そして (1) では、 μ_0 が、基底における各 n 個の μ_0 構成元素が、変数 a'_1, \dots, a'_v の秘密ランダム二次関数であるような

【数 5 3】

$$F_{q^n}$$

の元素であるとする。そうすると、 $n + v$ 個の変数 $a_1, \dots, a_n, a'_1, \dots, a'_v$ は、変数 x_1, \dots, x_{n+v} を得るために秘密全単射アフィン関数 s によって混じり合う。以前と同様、 $t(b_1, \dots, b_n) = (y_1, \dots, y_n)$ となり、ここでの t は秘密全単射アフィン関数である。次に、公開鍵は n 個の方程式 $y_i = P_i(x_1, \dots, x_{n+v})$ として与えられる。署名を計算するには、酢値 a'_1, \dots, a'_v を単にランダムに選択するだけでよい。次に、値 μ_0 および i を計算する。そうすると、単変量方程式 (1) が

【数 5 4】

$$F_{q^n}$$

で解かれる (解は a で表される)。

例: $K = F_2$ であるとする。HFEV では、例えば、隠蔽多項式は以下であるとする。

【数 5 5】

$$f(a) = a^{17} + \beta_{16} a^{16} + a^{12} + a^{10} + a^9 + \beta_8 a^8 + a^6 + a^5 + \beta_4 a^4 + a^3 + \beta_2 a^2 + \beta_1 a + \beta_0,$$

この式で、 $a = (a_1, \dots, a_n)$ (a_1, \dots, a_n は「油」変数) であり、 $\beta_1, \beta_2, \beta_4, \beta_8$ および β_{16} は v 個の酢変数を持つ n 個の秘密線形関数によって与えられ、 β_0 は v 個の酢変数を持つ n 個の秘密線形関数によって与えられるとする。この例では、署名を次のように計算する。すなわち、酢変数をランダムに選択し、結果の次数 17 の方程式を a で解く。

注: UOV とは異なり、HFEV では、(a^{17}, a^{12}, a^{10} などの) 油 \times 油の項、($\beta_{16} a^{16}, \beta_8 a^8$ などの) 油 \times 酢の項、および (β_0 の) 酢 \times 酢の項を持つ。

シミュレーション

Nicolas Courtois は、HFEV によるシミュレーションを行い、そのすべてのシミュレーションでは、酢変数の数が 3 以上であるときに、低い次数の複数のアフ

ァイン方程式はない（これは非常に素晴らしい）。詳細については、本論文の拡張版を参照されたい。

1 1 . U O V のパラメータの具体例

現時点で、例えば、 $n = 64$ 、 $v = 128$ （または $v = 192$ ）および $K = F_2$ を選択することが可能であるように思われる。この署名スキームは、セクション 8 のスキームであり、署名の長さは、このケースでは 192 ビット（または 256 ビット）にすぎない。可能なパラメータのその他の例は、本論文の拡張版で示す。

注： $K = F_2$ を選択すると、公開鍵はしばしば大きくなる。したがって、より大きい K とより小さい n を選択することが実用的である場合が多い。そうすると、公開鍵の長さをかなり短縮することができる。しかし、 K および n を固定したときでも、標準形で公開鍵を取得し、この標準の表現を元の表現よりもやや短くするために、公開鍵で簡単な変換を行うことは常に可能である。詳細については、本論文の拡張版を参照されたい。

1 2 . H F E V のパラメータの具体例

現時点で、 v に小さい値（例えば、 $v = 3$ ）および d に小さい値（例えば、 $n = 77$ 、 $v = 3$ 、 $d = 33$ 、 $K = F_2$ ）を選択することは可能であるように思われる。この署名スキームは、（誕生日パラドックスを避けるため）本論文の拡張版で説明する。ここでは、署名の長さは 80 ビットにすぎない。可能なパラメータのその他の例は、本論文の拡張版で示す。

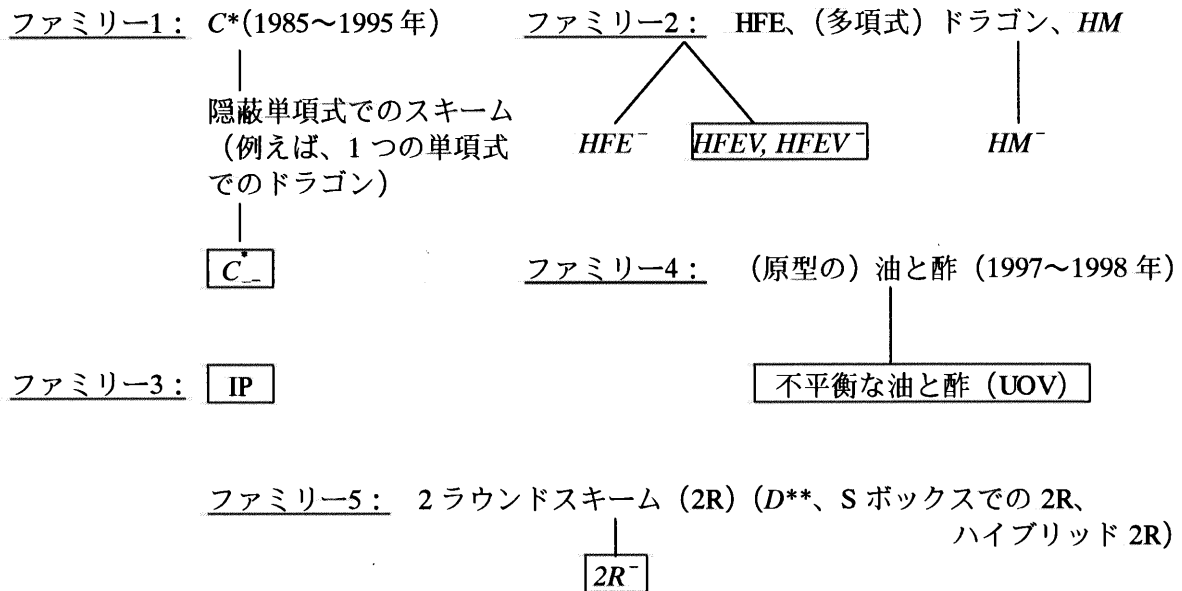
1 3 . 小さい有限体上で多変量多項式を用いた公開鍵スキームに関する（1999年5月時点での）最新技術

最近、本論文で説明している U O V や H F E V など、より優れたスキームを設計するための多くの新しいアイデアが導入されている。その他のアイデアには、一部の変数を固定して一部の代数特性を隠蔽するもの、いくつかの真にランダムな二次方程式を導入し、それらを元の方程式と混じり合わせるものなどがある（本論文の拡張版を参照）。しかし、まだ公表されていない論文[1]、[2]、[3]、[5]などにあるように、以前のスキームへのより巧みな攻撃を設計するための多くの新しいアイデアも導入されている。そのため、この分野は急速に変動しており、一見混乱しているようにも見える。さらに、「暗号分析」という表現を「暗号解読」の意味で使用している著者もあり、また、必ずしも「暗号解読」を意味しない「安全保障についての分析」の意味でこの語を使用している著者もいる。このセクションでは、主要なスキームに関して現在までにわかっていることを説明する。

小さい有限体上の多変量多項式に基づいた大きな公開鍵のファミリーは、トラップドアを導入する方法によってまたは安全保障が依存する困難な問題によって特徴付けられる 5 つの主要なファミリーに分類することができる。最初のファミリーは、「隠蔽単項式」スキームを持つ。このスキームの主なアイデアは、秘密鍵計算のために有限体上でべき乗化 $x \cdot x^d$ を計算するというものである。2 番目のファミリーでは、（複数の単項式がある）多項式関数が隠蔽される。3 番目のファミリーは、安全保障は同形写像問題に依存する。4 番目のファミリーでは、安全保障は、その構成の全体または一部から 2 つの多変量二次多項式の分解を発見する難しさに依存する。最後に、5 番目のファミリーでは、秘密鍵計算はガウス計算法に基づく。これらのファミリーにある主要スキームを下の図で説明する。各ファミリーで最も興味あるスキームであると思われるものを長方形で囲んでいる。 C^* は、すべてのうちで最初のスキームであり、これらのスキームすべての原型と見ることができる。このスキームは、[12]で設計され、[13]で解読された。

・（一部の「ドラゴン」スキームなど）隠蔽単項式でのスキームは、[15]で研究され、それらの大部分は安全保障されないことが示されている。（[20]で研究された） C^* は（現時点で）、スマートカードでの（時間および RAM の点で）最も効率的な署名スキームである。このスキームは、解読されていない（しかしその安全保障に大きな信頼を置くには、あまりにも単純すぎる、もしくはあまりにも C^* に近すぎるようである）。

【数 5 6】



・ H F E は、[1 4] で設計された。その安全保障についての最新の結果は、[1] および [2] にある。これらの論文では、非常に巧妙な攻撃が説明されている。しかし、現時点では、適切に選択された今なお合理的なパラメータにより、解読するために必要な計算がまだ大きすぎるため、このスキームは解読されていないようである。例えば、[1 4] の拡張版で提供された 5 0 0 米ドルの最初のチャレンジの賞金はまだ獲得されていない (これは、 F_2 上で $n = 8 0$ および $d = 9 6$ とする純粋な H F E である)。

・ H F E $^-$ は、公開方程式の一部が公開されていない H F E そのものである。[1] および [2] により、これを行うことが推奨されるであろう (原型の H F E は、それなしでも安全保障されるかもしれないという事実にかかわらず)。[1 4] の拡張版では、H F E $^-$ についての 5 0 0 米ドルの 2 番目のチャレンジが説明されている。

・ H F E V は、本論文で説明している。H F E V および H F E V $^-$ は、解読するのが非常に難しいようである。さらに、H F E V は、原型の H F E よりも効率的であり、わずか 8 0 ビットの公開鍵署名を実現することができる。

・ H M および H M $^-$ は、[2 0] で設計された。これらのスキームの分析はほとんど行われていない (しかし我々は H M ではなく H M $^-$ の使用を推奨できるかもしれない)。

・ I P は、[1 4] で設計された。I P スキームには、現在までで最も優れた安全保障の証明がある ([1 9] を参照)。I P は、非常に単純であり、グラフ同形写像の見事な一般化と見ることができる。

・ 原型の「油と酢」は、[1 6] で提示され、[1 0] で解読された。

・ U O V は、本論文で説明している。I P とともに、これらは確実に最も単純なスキームである。

・ 2 R は、[1 7] および [1 8] で設計された。[3] により、入力に少なくとも 1 2 8 ビットが必要であり、また [5] により、(以前は公開されていた) 公開方程式のすべてを公開しないことが賢明かもしれない。これにより、2 R $^-$ アルゴリズムになる ([5] で示されている 2 R スキームの分解アルゴリズムの効率は、まだ完全には明確でない)。

注釈 1: これらのスキームは、理論的な興味の対象ではあるが、(I P を例外として) その安全保障は、明確に定義され困難であるとみなされた問題には直接には関係しない。したがって、これらのスキームを現実の製品に実装することは果たして妥当であろうか。確かに、取り扱いに注意を要する用途におけるすべての安全保障をこのようなスキームに依存することはやや危険であると我々は考える。しかし現時点では、R S A スマートカードはより高価であるために、スマートカードアプリケーションの大部分は秘密鍵アルゴリズム (例えば、トリプル D E S) を使用している。したがって、既存の秘密鍵スキーム (の代わりとしてではなく) に加えて、以前の公開鍵スキームの 1 つを低コストのスマート

カードに入れることが妥当であろう。そうすれば、安全保障を高めることができ、スマートカードの価格を依然として安く抑えられる（コプロセッサは必要ない）。安全保障は、秘密鍵アルゴリズムのマスター秘密鍵（マスター秘密鍵に依存するリスクがある）および新しい低コストの公開鍵スキーム（スキームに安全保障の証明がないリスクがある）に依存することになる。極端に短い署名長（または短いブロック暗号）が必要なときは、事実上選択肢はないことも挙げられる。現時点では、多変量スキームのみが64～256ビットの長さを持つことができるからである。

注釈2： 多変量多項式での新しいスキームが発見される際、トラップドアがどのように導入されているかを必ずしも説明する必要はない。その場合には、ある種の「秘密 - 公開鍵」スキームを得ることになる。誰でも公開鍵から署名を検証することができる（または公開鍵から暗号化することができる）ため、このスキームは明らかに公開鍵スキームであるが、秘密鍵計算を計算する方法（すなわち、トラップドアが導入されている方法）は明らかにされておらず、公開鍵から推測することはできないので、スキームは秘密である。例えば、（公開する代わりに）HFEVでこれを行うことができたかもしれない。

14. 結論

本論文では、「酢変数」を用いた新しい2つの公開鍵スキームであるUOVおよびHFEVを提示した。このようなスキームを研究したことにより、一般二次形式の系の解についての非常に一般的な特性を分析することとなった。さらに、セクション13に提示している一般的な見解から、これら2つのスキームは、小さい有限体での多変量多項式に基づいた5つの主要スキームファミリーの2つとして、現時点で最も興味あるスキームであると考えられる。これは数年後でもまだ真であろうか。

参考文献

- [1] 匿名、「HFE公開鍵暗号システムの暗号分析」、未公表
- [2] 匿名、「隠蔽体式(HFE)の実際の暗号分析」、未公表
- [3] 匿名、「PatarinのSボックスを用いた2ラウンド公開鍵システムの暗号分析」、未公表
- [4] D. Coppersmith、私信、電子メール
- [5] Z. Dai、D. Ye、K. - Y. Lam、「写像構成に基づいた非対称暗号への素因数分解攻撃」、未公表
- [6] J. - C. Faugere、私信
- [7] H. Fell、W. Diffie、「多項式代入に基づく公開鍵アプローチの分析」、CRYPTO'85の議事録、Springer-Verlag、vol. 218、p. 340～349
- [8] M. Garey、D. Johnson、「コンピュータと計算の至難性、NP完全性の理論へのガイド」、Freeman、p. 251
- [9] H. Imai、T. Matsumoto、「非対称的暗号システムを構築するための代数法」、代数アルゴリズムおよびエラー訂正コード(AAEC-3)、Grenoble、1985年、Springer-Verlag、LNCS n°229
- [10] A. Kipnis、A. Shamir、「油と酢署名スキームの暗号分析」、CRYPTO'98の議事録、Springer、LNCS n°1462、pp. 257～266
- [11] R. Lidl、H. Niederreiter、「有限体」、Encyclopedia of Mathematics and its applications、第20巻、Cambridge University Press
- [12] T. Matsumoto、H. Imai、「効果的な署名検証とメッセージ暗号化のための公開二次多項式のタプル」、EUROCRYPT'88の議事録、Springer-Verlag、pp. 419～453
- [13] Jacques Patarin、「Eurocrypt'88の松本・今井公開鍵スキームの暗号分析」、CRYPTO'95の議事録、Springer-Verlag、pp. 248～261

- [14] J. Patarin, 「隠蔽体式 (HFE) と多項式の同形 (IP) : 非対称的アルゴリズムの新しい2つのファミリー」、EUROCRYPT '96の議事録、Springer、pp. 33 ~ 48
- [15] Jacques Patarin, 「隠蔽単項式を用いた非対称暗号」、CRYPTO '96の議事録、Springer、pp. 45 ~ 60
- [16] J. Patarin, 「油と酢署名スキーム」、暗号に関する Dagstuhl ワークショップで発表、1997年9月 (発表用透明フィルム)
- [17] J. Patarin, L. Goubin, 「トラップドア単方向置換と多変量多項式」、ICICS '97の議事録、Springer、LNCS n° 1334、pp. 356 ~ 368
- [18] J. Patarin, L. Goubin, 「Sボックスを用いた非対称暗号」、ICICS '97の議事録、Springer、LNCS n° 1334、pp. 369 ~ 380
- [19] J. Patarin, L. Goubin, N. Courtois, 「多項式の同形の改良アルゴリズム」、EUROCRYPT '98の議事録、Springer、pp. 184 ~ 200
- [20] J. Patarin, L. Goubin, N. Courtois, 「 C^* および HM : 松本・今井による2つのスキーム周囲の変種」、ASIACRYPT '98の議事録、Springer、pp. 35 ~ 49
- [21] A. Shamir, 「D. Coppersmith および J. Stern によって発見された暗号化の単純なスキームおよびその暗号分析」、暗号に関する Luminy ワークショップで発表、1995年9月