(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4183387号
(P4183387)
(45)発行日　平成20年11月19日(2008.11.19)　(24)登録日　平成20年9月12日(2008.9.12)

(51)Int.Cl.　F I
G09C 1/00 (2006.01)　G09C 1/00 640B
G09C 1/00 620Z

請求項の数 15　(全 28 頁)

(21)出願番号	特願2000-616162 (P2000-616162)	(73)特許権者	595143078
(86)(22)出願日	平成12年4月28日 (2000.4.28)		ブル・セー・ペー・８
(65)公表番号	特表2002-543478 (P2002-543478A)		フランス国、７８９３０・ルーブシエンヌ、ルート・ドウ・ベルサイユ、６８
(43)公表日	平成14年12月17日 (2002.12.17)	(74)代理人	100062007
(86)国際出願番号	PCT/IB2000/000692		弁理士　川口　義雄
(87)国際公開番号	WO2000/067423	(72)発明者	パタラン，ジヤツク
(87)国際公開日	平成12年11月9日 (2000.11.9)		フランス国、エフ－７８２２０・ビロフレ、リユ・アメデ－デイイ、１１
審査請求日	平成13年1月26日 (2001.1.26)	(72)発明者	キプニス，アビアド
審判番号	不服2005-4793 (P2005-4793/J1)		イスラエル国、９２５４２・エルサレム、ハパルマツハ・ストリート・７
審判請求日	平成17年3月18日 (2005.3.18)	(72)発明者	グバン，ルイ
(31)優先権主張番号	99401048.6		フランス国、エフ－７５０１５・パリ、リユ・ブラウン・セカール、３
(32)優先日	平成11年4月29日 (1999.4.29)		
(33)優先権主張国	欧州特許庁 (EP)		

最終頁に続く

(54)【発明の名称】公開鍵を署名する方法とシステム

(57)【特許請求の範囲】

【請求項１】

公開鍵発生器により、ｋ個の多項式関数の集合Ｓ１を公開鍵として供給するステップであり、前記集合Ｓ１が関数$P_1(x_1,\ldots,x_{n+v},y_1,\ldots,y_k)$，．．．，$P_k(x_1,\ldots,x_{n+v},y_1,\ldots,y_k)$を含み、ここで、ｋ、ｖ及びｎは整数であり、「酢」変数の数ｖは「油」変数の数ｎより大きく、$x_1,\ldots,x_{n+v}$は第１のタイプのｎ＋ｖ個の変数であり、$y_1,\ldots,y_k$は第２のタイプのｋ個の変数であり、前記集合Ｓ１が、ｋ個の多項式関数$P'_1(a_1,\ldots,a_{n+v},y_1,\ldots,y_k)$，．．．，$P'_k(a_1,\ldots,a_{n+v},y_1,\ldots,y_k)$の集合Ｓ２に対して秘密鍵演算を適用することによって得られ、ここで、$a_1,\ldots,a_{n+v}$は、ｎ個の「油」変数$a_1,\ldots,a_n$の集合とｖ個の「酢」変数$a_{n+1},\ldots,a_{n+v}$の集合を含むｎ＋ｖ個の変数である、前記ステップと；

署名器へ、署名されるメッセージを提供するステップと；

前記署名器により、前記メッセージに対してハッシュ関数を適用して、ｋ個の値の列$b_1,\ldots,b_k$を発生するステップと；

前記署名器により、前記ｋ個の値の列$b_1,\ldots,b_k$を前記集合Ｓ２のそれぞれの変数$y_1,\ldots,y_k$に代入して、ｋ個の多項式関数$P''_1(a_1,\ldots,a_{n+v}),\ldots,P''_k(a_1,\ldots,a_{n+v})$の集合Ｓ３を発生するステップと；

前記署名器により、前記ｖ個の「酢」変数$a_{n+1},\ldots,a_{n+v}$に対してｖ個の値$a'_{n+1},\ldots,a'_{n+v}$を選択するステップと；

前記署名器により、式$P''_1(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0,...,P''_k(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0$の集合を解いて、値$a'_1,...,a'_n$の解を得るステップと；

前記署名器により、秘密鍵演算を適用して、値$a'_1,...,a'_{n+v}$をディジタル署名$e_1,...,e_{n+v}$に変換するステップと；

を含む、ディジタル署名暗号方法。

【請求項２】

検証器により、前記ディジタル署名を検証するステップをさらに含む、請求項１に記載の方法。

【請求項３】

前記検証ステップが：

前記署名$e_1,...,e_{n+v}$、前記メッセージ、前記ハッシュ関数及び前記公開鍵を得るステップと；

前記ハッシュ関数を前記メッセージに対して適用して、ｋ個の値の列$b_1,...,b_k$を発生するステップと；

式$P_1(e_1,...,e_{n+v},b_1,...,b_k)=0,...,P_k(e_1,...,e_{n+v},b_1,...,b_k)=0$が満足されることを検証するステップと；

を含む、請求項２に記載の方法。

【請求項４】

前記集合Ｓ２が、「酢」変数が追加された隠蔽体式（ＨＦＥ）スキームであるＨＦＥＶスキームのｋ個の多項式関数の集合ｆ（ａ）を含む、請求項１に記載の方法。

【請求項５】

前記集合Ｓ２が、「酢」変数の数ｖが「油」変数の数ｎより大きい「油と酢」スキームである不平衡「油と酢」（ＵＯＶ）スキームのｋ個の多項式関数の集合Ｓを含む、請求項１に記載の方法。

【請求項６】

q^vが2^{32}より大きくなるようにｖが選択され、ここでｑが有限体Ｋのエレメントの数である、請求項１に記載の方法。

【請求項７】

前記供給ステップが、前記集合Ｓ２のｋ個の多項式関数の部分集合Ｓ２’から前記集合Ｓ１を得るステップを含み、前記部分集合Ｓ２’は、前記ｋ個の多項式関数$P'_1(a_1,...,a_{n+v},y_1,...y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$中の変数$y_1,...,y_k$のいずれかを含む構成要素の全ての係数がゼロであり、また、「酢」変数の数ｖが「油」変数の数ｎより大きいことを特徴とする、請求項１に記載の方法。

【請求項８】

前記集合Ｓ２が、ＵＯＶスキームのｋ個の多項式関数の集合Ｓを含み、また、「酢」変数の数ｖが：

（ａ）次数２の「油と酢」スキームにおける体Ｋの２以外の各標数ｐに対して、ｖが不等式$q^{(v-n)-1}*n^4>2^{40}$を満足するという条件と；

（ｂ）次数３の「油と酢」スキームにおけるｐ＝２に対して、ｖがｎ＊（１＋ｓｑｒｔ（３））より大きく$n^3/6$以下であるという条件と；

（ｃ）次数３の「油と酢」スキームにおける２以外の各ｐに対して、ｖがｎより大きくn^4以下であるという条件と；

の内の１つの条件を満足するように選択される、請求項７に記載の方法。

【請求項９】

前記集合Ｓ２が、ＵＯＶスキームのｋ個の多項式関数の集合Ｓを含み、また、「酢」変数の数ｖが、次数２の「油と酢」スキームにおける体Ｋの標数ｐ＝２に対して不等式$v<n^2$と$q^{(v-n)-1}*n^4>2^{40}$を満足するように選択される、請求項７に記載の方法。

【請求項１０】
前記秘密鍵演算が、ｎ＋ｖ個の変数$a_1, \ldots, a_{n+v}$に対する秘密アフィン変換ｓを含む、請求項１に記載の方法。
【請求項１１】
前記集合Ｓ２が単変量多項式から誘導されたｋ個の関数を含む式を含む、請求項４に記載の方法。
【請求項１２】
前記単変量多項式が１００，０００以下の次数の単変量多項式を含む、請求項１１に記載の方法。
【請求項１３】
請求項１に記載のディジタル署名暗号方法により生成したディジタル署名を検証器により検証する方法であって、該方法が：
前記署名$e_1, \ldots, e_{n+v}$、前記メッセージ、前記ハッシュ関数及び前記公開鍵を得るステップと；
前記ハッシュ関数を前記メッセージに対して適用して、ｋ個の値の列$b_1, \ldots, b_k$を発生するステップと；
式$P_1(e_1, \ldots, e_{n+v}, b_1, \ldots, b_k)=0, \ldots, P_k(e_1, \ldots, e_{n+v}, b_1, \ldots, b_k)=0$が満足されることを検証するステップと；
を含む方法。
【請求項１４】
「酢」変数の数ｖが：
（ａ）体Ｋの各標数ｐが２以外であり「油と酢」署名方法の次数が２である場合、ｖが不等式$q^{(v-n)-1} * n^4 > 2^{40}$を満足するという条件と；
（ｂ）ｐ＝２であり前記「油と酢」署名方法の次数が３である場合、ｖがｎ＊（１＋ｓｑｒｔ（３））より大きく$n^3/6$以下であるという条件と；
（ｃ）各ｐが２以外であり、前記「油と酢」署名方法の次数が３である場合、ｖがｎより大きくn^4以下であるという条件と；
の内の１つを満足するように選択される、請求項１３に記載の方法。
【請求項１５】
前記集合Ｓ２がＵＯＶスキームのｋ個の多項式関数の集合Ｓを含み、また、「酢」変数の数ｖが、次数２の「油と酢」スキームにおける体Ｋの標数ｐ＝２に対して不等式$v < n^2$と$q^{(v-n)-1} * n^4 > 2^{40}$を満足するように選択される、請求項１３に記載の方法。
【発明の詳細な説明】
【０００１】
（技術分野）
本発明は一般的には暗号に関し、より具体的には公開鍵暗号に関する。
【０００２】
（背景技術）
最初の公開鍵暗号スキームは１９７５年に導入された。それ以来、多くの公開鍵スキームが開発されて公開されてきた。多くの公開鍵スキームは整数ｎ（昨今、ｎは一般的には５１２ビットと１０２４ビットの間にある）を法とした算術計算を必要とする。
【０００３】
ビット数ｎの値が比較的大きいため、このような公開鍵スキームは、動作が比較的遅く、ランダムアクセスメモリー（ＲＡＭ）や他の計算リソースを大いに消費するものと考えられている。これらの問題は、スマートカードの適用分野など計算リソースが制限されている適用分野では特に緊急の課題である。したがって、これらの問題を克服するために、ｎを法とした算術計算をあまり必要としない他の公開鍵スキームファミリーが開発されてきた。これらの他のファミリーの中には、例えば２と2^{64}との間の比較的小さい数学的有限体上の、ｋ個の多変数多項式の集合として、公開鍵が与えられるスキームがある。

【０００４】
このｋ個の多変数多項式の集合は次のように書くことが可能である：
$y_1 = P_1(x_1, \ldots x_n)$
$y_2 = P_2(x_1, \ldots x_n)$
.
.
.
$y_k = P_k(x_1, \ldots x_n)$
ここで、$P_1, \ldots, P_k$は、小さい総次数の、一般的には８以下、多くの場合においてはちょうど２という次数の多変数多項式である。
【０００５】
このようなスキームの例には、Ｔ．ＭａｔｓｕｍｏｔｏとＨ．ＩｍａｉのＣ＊スキーム、Ｊａｃｑｕｅ　ＰａｔａｒｉｎのＨＦＥスキーム及びＪａｃｑｕｅ　Ｐａｔａｒｉｎの「油と酢」スキームの基本形態がある。
【０００６】
Ｃ＊スキームは、Ｓｐｒｉｎｇｅｒ出版社、ＥＵＲＯＣＲＹＰＴ’８８の議事録、４１９～４５３ページの「効率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組」という題名の記事に説明されている。ＨＦＥスキームは、Ｓｐｒｉｎｇｅｒ出版社、ＥＵＲＯＣＲＹＰＴ’９６の議事録の３３～４８ページの「隠蔽体式（ＨＦＥ）と多項式の同形（ＩＰ）：非対称アルゴリズムの新しい２つのファミリー」という題名の記事に説明されている。Ｊａｃｑｕｅ　Ｐａｔａｒｉｎの「油と酢」スキームの基本的形態は１９９７年９月の暗号に関するＤａｇｓｔｕｈｌ　Ｗｏｒｋｓｈｏｐに提出された「油と酢署名スキーム」という題名の記事に説明されている。
【０００７】
しかしながら、Ｃ＊スキームと「油と酢」スキームの基本的形態とは、Ｃ＊スキームと「油と酢」スキームの基本的形態双方の暗号解読が見つかってしまい、Ｓｐｒｉｎｇｅｒ出版社ＬＮＣＳ　ｎ°１４６２、ＣＲＹＰＴＯ’９８の議事録の２５７～２６６ページの「油と酢署名スキームの暗号解読」という題名の記事中にＡｖｏｉｄ　ＫｉｐｎｉｓとＡｄｉ　ｓｈａｍｉｒによって公開されているという点で安全でないことが分かっている。ＨＦＥスキームの構成の弱点は「ＨＦＥ公開鍵暗号システム」と「隠蔽体式（ＨＦＥ）の実際の暗号解読」という題名の２つの非公開記事中に記載されているが現在のところ、ＨＦＥスキームは暗号漏洩(compromise)されているとは考えられてはいない。その理由は、良く選択され、いまだ妥当なパラメータの場合、ＨＦＥスキームを解読するために必要な計算の回数はなおも多すぎるからである。
【０００８】
関連技術の１部の態様が次の出版物に記載されている：
Ｓｈａｍｉｒに対する米国特許第５，２６３，０８５号に、ある合成数ｎを法としたｍ個の未知数をもつ、ｋ個の多項式から成る系を解く困難さに基づいたセキュリティを持つ新しいタイプのディジタル署名スキームが記載されており；
Ｓｈａｍｉｒに対する米国特許第５，３７５，１７０号には、小さい鍵を有し、算術演算をほとんど必要としない新しいクラスの双有理順列(birational permutation)に基づいた新規なディジタル署名スキームが記載されている。
【０００９】
上記と本明細書全てにわたる参照文献の開示は参照してここに組み込まれるものである。
【００１０】
（発明の開示）
本発明は、一般的には数学的有限体Ｋ上の、ｋ個の多変数多項式の集合として公開鍵を与えるディジタル署名暗号スキームのセキュリティを向上させることを追求する。本発明は、特に、「油と酢」スキームとＨＦＥスキームという基本的形態のセキュリティを向上させることを追求する。本発明に従ってセキュリティを向上させるように修正された「油

と酢」スキームは本書では不平衡「油と酢」（ＵＯＶ）スキームと呼ばれる。本発明に従ってセキュリティを向上させるように修正されたＨＦＥスキームは本書ではＨＦＥＶスキームと呼ばれる。

【００１１】

本発明においては、ｋ個の多項式関数の集合Ｓ１は公開鍵として供給される。集合Ｓ１は、関数$P_1(x_1,\ldots,x_{n+v},y_1,\ldots,y_k),\ldots,P_k(x_1,\ldots,x_{n+v},y_1,\ldots,y_k)$を含むことが好ましい。ここで、ｋ、ｖ及びｎは整数であり、$x_1,\ldots,x_{n+v}$は第１のタイプのｎ＋ｖ個の変数であり、$y_1,\ldots,y_k$は第２のタイプのｋ個の変数である。集合Ｓ１は秘密鍵演算をｋ個の多項式関数$P'_1(a_1,\ldots,a_{n+v},y_1,\ldots y_k),\ldots P'_k(a_1,\ldots,a_{n+v},y_1,\ldots,y_k)$の集合Ｓ２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、$a_1,\ldots,a_{n+v}$はｎ個の「油」変数$a_1,\ldots,a_n$の集合とｖ個の「酢」変数$a_{n+1},\ldots,a_{n+v}$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$a_1,\ldots,a_{n+v}$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。

【００１２】

署名すべきメッセージが提供されると、ハッシュ関数がそのメッセージに対して適用されてｋ個の値の列$b_1,\ldots,b_k$を発生する。このｋ個の値の列$b_1,\ldots,b_k$をそれぞれ集合Ｓ２の変数$y_1,\ldots,y_k$に代入してｋ個の多項式関数$P''_1(a_1,\ldots,a_{n+v}),\ldots,P''_k(a_1,\ldots,a_{n+v})$の集合Ｓ３を発生するのが好ましい。次に、ｖ個の値$a'_{n+1},\ldots,a'_{n+v}$をランダムに又は所定の選択アルゴリズムに従ってｖ個の「酢」変数$a_{n+1},\ldots,a_{n+v}$に対して選択する。

【００１３】

ひとたびｖ個の値$a'_{n+1},\ldots,a'_{n+v}$が選択されると、式$P''_1(a_1,\ldots,a_n,a'_{n+1},\ldots,a'_{n+v})=0,\ldots,P''_k(a_1,\ldots,a_n,a'_{n+1},\ldots,a'_{n+v})=0$の集合を解いて、$a'_1,\ldots,a'_n$の解を得るのが好ましい。次に、秘密鍵演算を適用して$a'_1,\ldots,a'_{n+v}$をディジタル署名$e_1,\ldots,e_{n+v}$に変換する。

【００１４】

このように発生したディジタル署名$e_1,\ldots,e_{n+v}$は、例えばコンピュータ又はスマートカードを含む検証器によって検証される。ディジタル署名を検証するために、検証器は、署名$e_1,\ldots,e_{n+v}$、メッセージ、ハッシュ関数及び公開鍵を得るのが好ましい。次に、検証器はハッシュ関数をメッセージに対して適用してｋ個の値の列$b_1,\ldots,b_k$を発生する。ひとたびｋ個の値$b_1,\ldots,b_k$が発生すると、検証器は式$P_1(e_1,\ldots,e_{n+v},b_1,\ldots,b_k)=0,\ldots,P_k(e_1,\ldots,e_{n+v},b_1,\ldots,b_k)=0$が満足されることを検証することによってディジタル署名を検証するのが好ましい。

【００１５】

このようにして、本発明による好ましい実施形態は、ｋ個の多項式関数の集合Ｓ１を公開鍵として供給するステップであり、前記集合Ｓ１は関数$P_1(x_1,\ldots,x_{n+v},y_1,\ldots,y_k),\ldots,P_k(x_1,\ldots,x_{n+v},y_1,\ldots,y_k)$を含み、ここで、ｋ、ｖ及びｎは整数であり、$x_1,\ldots,x_{n+v}$は第１のタイプのｎ＋ｖ個の変数であり、$y_1,\ldots,y_k$は第２のタイプのｋ個の変数であり、集合Ｓ１は秘密鍵演算をｋ個の多項式関数$P'_1(a_1,\ldots,a_{n+v},\ldots,y_1,\ldots,y_k),\ldots,P'_k(a_1,\ldots,a_{n+v},\ldots,y_k)$の集合Ｓ２に適用することによって得られ、ここで、$a_1,\ldots,a_{n+v}$は、ｎ個の「油」変数$a_1,\ldots,a_n$の集合とｖ個の「酢」変数$a_{n+1},\ldots,a_{n+v}$の集合を含むｎ＋ｖ個の変数である、前記ステップと；署名されるメッセージを提供するステップと；ハッシュ関数をこのメッセージに対して適用してｋ個の値の列$b_1,\ldots,b_k$を発生す

るステップと；集合Ｓ２の変数y_1，．．．，y_kにそれぞれｋ個の値の列b_1，．．．，b_kを代入してｋ個の多項式関数Ｐ’’$_1$（a_1，．．．，a_{n+v}），．．．，Ｐ’’$_k$（a_1，．．．，a_{n+v}）の集合Ｓ３を発生するステップと；ｖ個の「酢」変数a_{n+1}，．．．，a_{n+v}に対してｖ個の値a'_{n+1}，．．．，a'_{n+v}を選択するステップと；式Ｐ’’$_1$（a_1，．．．，a_n，a'_{n+1}，．．．，a'_{n+v}）＝０，．．．，Ｐ’’$_k$（a_1，．．．，a_n，a'_{n+1}，．．．，a'_{n+v}）＝０の集合を解いてa'_1，．．．，a'_nの解を得るステップと；秘密鍵演算を適用してa'_1，．．．，a'_{n+v}をディジタル署名e_1，．．．，e_{n+v}に変換するステップと；を含むディジタル署名暗号方法を提供する。

【００１６】

この方法はまたディジタル署名を検証するステップを含むのが好ましい。この検証ステップは：署名e_1，．．．，e_{n+v}、メッセージ、ハッシュ関数及び公開鍵を得るステップと；ハッシュ関数をメッセージに対して適用してｋ個の値の列b_1，．．．，b_kを発生するステップと；式P_1（e_1，．．．，e_{n+v}，b_1，．．．，b_k）＝０，．．．，P_k（e_1，．．．，e_{n+v}，b_1，．．．，b_k）＝０が満足されることを検証するステップと；を含むのが好ましい。

【００１７】

この秘密鍵演算はｎ＋ｖ個の変数a_1，．．．，a_{n+v}に対する秘密アフィン変換ｓのステップを含むのが好ましい。

【００１８】

集合Ｓ２はＨＦＥＶスキームのｋ個の多項式関数の集合ｆ（ａ）を含むのが好ましい。このような場合、集合Ｓ２は単変量多項式から誘導されたｋ個の関数を含む式を含むのが好ましい。単変量多項式は１００，０００以下の次数の単変量多項式を含むのが好ましい。

【００１９】

代替例として、集合Ｓ２はＵＯＶスキームのｋ個の多項式関数の集合Ｓを含む。

【００２０】

上記の供給ステップは「酢」変数の数ｖを「油」変数の数ｎより大きくなるように選択するステップを含むのが好ましい。ｖは、q^vが2^{32}より大きくなるように選択されるが、ここで、ｑは有限体Ｋのエレメントの数である。

【００２１】

本発明の好ましい実施形態によれば、上記の供給ステップは、集合Ｓ２の内のｋ個の多項式関数の部分集合Ｓ２’から集合Ｓ１を得るステップを含んでいるが、この部分集合Ｓ２’の標数は、ｋ個の多項式関数Ｐ’$_1$（a_1，．．．，a_{n+v}，y_1，．．．，y_k），．．．，Ｐ’$_k$（a_1，．．．，a_{n+v}，y_1，．．．，y_k）中のy_1，．．．，y_kという変数のいずれかを含む構成要素のすべての係数がゼロであり、また、「酢」変数の数ｖが「油」変数の数ｎより大きいことにある。

【００２２】

集合Ｓ２はＵＯＶスキームのｋ個の多項式関数の集合Ｓを含み、また、「酢」変数の数ｖが、次の条件：すなわち（ａ）次数２の「油と酢」スキーム中の体Ｋの２以外の各標数ｐに対して、ｖが不等式$q^{(v-n)-1}*n^4>2^{40}$となることと、（ｂ）次数３の「油と酢」スキーム中のｐ＝２に対して、ｖがｎ＊（１＋ｓｑｒｔ（３））より大きく、n^3／６以下であることと、（ｃ）次数３の「油と酢」スキーム中の２以外の各ｐに対して、ｖがｎより大きく、n^4以下であること、の内の１つを満足するように選択されるのが好ましい。「酢」変数の数ｖは、次数２の「油と酢」スキーム中の体Ｋの標数ｐ＝２に対して不等式$v<n^2$、$q^{(v-n)-1}*n^4>2^{40}$を満足するように選択されるのが好ましい。

【００２３】

また本発明の好ましい実施形態によれば、「油と酢」方法の改善が提供されるが、この改善は「油」変数より多い数の「酢」変数を用いるステップを含んでいる。「酢」変数の数ｖは、次の条件：すなわち（ａ）体Ｋの２以外の各標数ｐと次数２の「油と酢」署名方法

に対して、ｖが不等式ｑ$^{（ｖ－ｎ）－１}$＊ｎ^{４}＞２^{４０}を満足することと、（ｂ）ｐ＝２と次数３の「油と酢」署名方法に対して、ｖがｎ＊（１＋ｓｑｒｔ（３））より大きくｎ^{３}／６以下であるということと、（ｃ）２以外の各ｐと次数３の「油と酢」署名方法に対して、ｖがｎより大きく、また、ｎ^{４}以下であること、の内の一を満足する用に選択されるのが好ましい。「酢」変数の数ｖは、次数２の「油と酢」スキーム中の体Ｋの標数ｐ＝２に対して不等式ｖ＜ｎ^{２}とｑ$^{（ｖ－ｎ）－１}$＊ｎ^{４}＞２^{４０}を満足するように選択されるのが好ましい。

【００２４】

本発明は次の図面と共に以下の詳細な説明を読めばより完全に理解されよう。

【００２５】

付録Ｉは、ＥＵＲＯＶＲＹＰＴ’９９の議事録中のＳｐｒｉｎｇｅｒ出版社による出版用に提出されたＡｖｉａｄ　Ｋｉｐｎｉｓ、Ｊａｃｑｕｅ　Ｐａｔａｒｉｎ及びＬｏｕｉｓ　Ｇｏｕｂｉｎによる、ＵＯＶスキームとＨＦＥＶスキームの変形形態を説明している記事である。

【００２６】

（発明を実施するための最良の形態）

メッセージに対してディジタル署名を発生してこれを検証するシステム１０、すなわち本発明のある好ましい実施形態に従って構成され動作するシステム１０の好ましい実現例の略ブロック図である図１を参照されたい。

【００２７】

システム１０は、スマートカードリーダー２５を介してスマートカード２０と通信する、汎用コンピュータなどのコンピュータ１５を含むのが好ましい。コンピュータ１５は、通信バス４０を介してデータを通信するディジタル署名発生器３０とディジタル署名検証器３５を含むのが好ましい。スマートカード２０は、通信バス５５を介してデータを通信するディジタル署名発生器４５とディジタル署名検証器５０を含むのが好ましい。

【００２８】

一般的な公開鍵署名スキーム適用分野では、メッセージの署名器と署名済みメッセージの受領器とが、公開された公開鍵と用いられるハッシュ関数とに関して一致することが理解されよう。ハッシュ関数が暗号漏洩している場合、署名器と受領器はハッシュ関数を変更することに同意する。公開鍵の発生器は署名器でも受領器でもある必要がないことが理解されよう。

【００２９】

ディジタル署名検証器３５は、ディジタル署名発生器３０とディジタル署名発生器４５の内の一方によって発生される署名を検証するのが好ましい。同様に、ディジタル署名検証器５０は、ディジタル署名発生器３０とディジタル署名発生器４５の内の一方によって発生した署名を検証する。

【００３０】

第１のプロセッサ（図示せず）中でメッセージに対するディジタル署名を発生する好ましいディジタル署名暗号方法の略フローチャートの図２Ａと、第２のプロセッサ（図示せず）中で図２Ａのディジタル署名を検証する好ましいディジタル署名暗号方法の略フローチャートである図２Ｂをここで参照すると、図２Ａと２Ｂの方法は、本発明のある好ましい実施形態に従って動作することが分かる。

【００３１】

図２Ａと２Ｂの方法はハードウエア、ソフトウエア、またはハードウエアとソフトウエアを組み合わせて実現され得ることが理解されよう。さらに、第１のプロセッサと第２のプロセッサは同一であってもよい。代替例としては、本方法は、第１のプロセッサが例えばコンピュータ１５中に含まれており、第２のプロセッサがスマートカード２０中に含まれている、又はこの逆である図１のシステム１０によって実現されている。

【００３２】

図２Ａと２Ｂの方法及び図２Ａと２Ｂの方法の適用例が、本書に組み込まれている付録Ｉ

に記載されている。図２Ａと２Ｂの方法の適用例は、「油と酢」スキームとＨＦＥスキームの基本的形態を修正し、これによってそれぞれＵＯＶとＨＦＥＶをもたらすために採用されうる。

【００３３】

付録Ｉに、１９９９年5月2～6日に予定されていたＥＵＲＯＣＲＹＰＴ’９９の議事録中のＳｐｒｉｎｇｅｒ出版社による出版のために提出されたＡｖｉａｄ　Ｋｉｐｎｉｓ、Ｊａｃｑｕｅ　Ｐａｔａｒｉｎｋ、Ｌｏｕｉｓ　Ｇｏｕｂｉｎによる未出版の記事が含まれている。付録Ｉに含まれているこの記事はまた、小さい署名を持つ、ＵＯＶスキームとＨＦＥＶスキームの変形形態を記載している。

【００３４】

図２Ａのディジタル署名暗号方法においては、ｋ個の多項式関数の集合Ｓ１は、例えば図１の発生器３０や図１の発生器４５や外部公開鍵発生器（図示せず）であったりする公開鍵（図示せず）の発生器によって公開鍵として供給されるのが好ましい（ステップ１００）。

【００３５】

集合Ｓ１は、関数$P_1(x_1,\ldots,x_{n+v},y_1,\ldots,y_k),\ldots,P_k(x_1,\ldots,x_{n+v},y_1,\ldots,y_k)$を含むのが好ましい。ここで、ｋ、ｖ及びｎは整数であり、$x_1,\ldots,x_{n+v}$は第１のタイプのｎ＋ｖ個の変数であり、$y_1,\ldots,y_k$は第２のタイプのｋ個の変数である。集合Ｓ１は、秘密鍵演算をｋ個の多項式関数$P'_1(a_1,\ldots,a_{n+v},y_1,\ldots,y_k),\ldots,P'_k(a_1,\ldots,a_{n+v},y_1,\ldots,y_k)$の集合Ｓ２に対して適用することによって得るのが好ましいが、ここで、$a_1,\ldots,a_{n+v}$は、ｎ個の「油」変数$a_1,\ldots,a_n$の集合とｖ個の「酢」変数$a_{n+1},\ldots,a_{n+v}$の集合を含むｎ＋ｖ個の変数である。この秘密鍵演算はｎ＋ｖ個の変数$a_1,\ldots,a_{n+v}$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。

【００３６】

「油」変数と「酢」変数という用語は、１９９７年９月の暗号学に関するＤａｇｓｔｕｈｌ　Ｗｏｒｋｓｈｏｐで提示された「油と酢署名スキーム」という題名の上記の記事に記載されているＪａｃｑｕｅ　Ｐａｔａｒｉｎの「油と酢」スキームの基本的形態で定義されているような「油と酢」変数のことである。

【００３７】

署名されるメッセージが提供される（ステップ１０５）と、署名器はハッシュ関数をそのメッセージに適用して、ｋ個の値の列$b_1,\ldots,b_k$を発生する（ステップ１１０）のが好ましい。署名器は、例えば、図１の発生器３０であったり発生器４５であったりする。ｋ個の値の列$b_1,\ldots,b_k$は、集合Ｓ２のそれぞれの変数$y_1,\ldots,y_k$に代入して、ｋ個の多項式関数$P''_1(a_1,\ldots,a_{n+v}),\ldots,P''_k(a_1,\ldots,a_{n+v})$の集合Ｓ３を発生する（ステップ１１５）のが好ましい。したがって、ｖ個の値の列$a'_{n+1},\ldots,a'_{n+v}$はｖ個の「酢」変数$a_{n+1},\ldots,a_{n+v}$に対してランダムに選択される（ステップ１２０）。代替例として、ｖ個の値$a'_{n+1},\ldots,a'_{n+v}$は所定の選択アルゴリズムに従って選択される。

【００３８】

ひとたびｖ個の値$a'_{n+1},\ldots,a'_{n+v}$が選択されると、式$P''_1(a_1,\ldots,a_n,a'_{n+1},\ldots,a'_{n+v})=0,\ldots,P''_k(a_1,\ldots,a_n,a'_{n+1},\ldots,a'_{n+v})=0$の集合を解いて、$a'_1,\ldots,a'_n$に対する解を得るのが好ましい（ステップ１２５）。次に、秘密鍵演算を適用して、$a'_1,\ldots,a'_{n+v}$をディジタル署名$e_1,\ldots,e_{n+v}$に変換する（ステップ１３０）。

【００３９】

発生されたディジタル署名$e_1,\ldots,e_{n+v}$は、例えば図１の検証器３５又は検

証器５０を含むことができるディジタル署名の検証器（図示せず）によって図２Ｂを参照して説明される方法に従って検証される。ディジタル署名を検証するために、検証器は、署名$e_1, \ldots, e_{n+v}$、メッセージ、ハッシュ関数及び公開鍵を得るのが好ましい（ステップ２００）。次に、検証器はハッシュ関数をメッセージに適用して、ｋ個の値の列$b_1, \ldots, b_k$を発生する（ステップ２０５）。ひとたびｋ個の値$b_1, \ldots, b_k$が発生すると、検証器は式$P_1(e_1, \ldots, e_{n+v}, b_1, \ldots, b_k) = 0, \ldots, P_k(e_1, \ldots, e_{n+v}, b_1, \ldots, b_k) = 0$が満足されることを検証することによってディジタル署名を検証するのが好ましい（ステップ２１０）。

【００４０】

上述のようにディジタル署名を発生して検証する操作は、付録Ｉに記載するＵＯＶのｋ個の多項式関数の集合Ｓを含むことを集合Ｓ２に対して許可することによってＵＯＶに対して用いられることが理解されよう。代替例として、上記のディジタル署名の発生と検証操作は、付録Ｉに記載されるＨＦＥＶスキームのｋ個の多項式関数の集合ｆ（ａ）を含むことを集合Ｓ２に対して許可することによってＨＦＥＶに対して用いられることもできる。

【００４１】

付録Ｉで述べるように、図２Ａと２Ｂの方法によって、良く知られているＲＳＡスキームなどの従来の数値理論暗号スキームで得られるディジタル署名より、一般的に小さいディジタル署名を得ることが可能となる。

【００４２】

本発明のある好ましい実施形態によれば、集合Ｓ２がＵＯＶスキームのｋ個の多項式関数の集合Ｓを含んでいる場合、集合Ｓ１は、「油」変数の数ｎより大きいように選択されている「酢」変数の数ｖを与えられる。ｖはまた、q^vが2^{32}（ここで、ｑは集合Ｓ１、Ｓ２及びＳ３が与えられる有限体Ｋのエレメントの数である）より大きくなるように選択される。

【００４３】

Ｓ１は集合Ｓ２のｋ個の多項式関数の部分集合Ｓ２’から得るのがさらに好ましいが、ここで、Ｓ２’は、ｋ個の多項式関数$P'_1(a_1, \ldots, a_{n+v}, y_1, \ldots, y_k), \ldots, P'_k(a_1, \ldots, a_{n+v}, y_1, \ldots, y_k)$中の$y_1, \ldots, y_k$変数の内のどの変数を含む構成要素でも全ての係数がゼロであり、また、「酢」変数の数ｖが「油」変数の数ｎより大きいことを特徴としている。

【００４４】

基本的「油と酢」スキームにおいては、「酢」変数の数ｖは、「油」変数の数ｎに等しくなるように選択される。このようにｖ個の変数を選択するために、本発明の発明者の一人であるＡｖｉａｄ　Ｋｉｐｎｉｓと、Ａｄｉ　ＳｈａｍｉｒはＳｐｒｉｎｇｅｒ、ＬＮＣＳ　ｎ°１４６２、ＣＲＹＰＴＯ’９８の議事録の２５７～２６６ページで、基本的「油と酢」スキームの安全性を無効とする、暗号シ解読を示している。加えて、ＫｉｐｎｉｓとＳｈａｍｉｒによって記載されたと同じ方法を適用することによって、基本的「油と酢」スキームは、「油」変数の数ｎより低いいかなる数ｖの「酢」変数に対しても安全性が無効とされることが示される。

【００４５】

本発明の発明者は、付録Ｉに記載するように、「油と酢」スキームは、「油と酢」スキームを「酢」変数の数ｖが「油」変数の数ｎよりも大きくなるように修正することによって不平衡にされると、結果として得られる不平衡な「油と酢」（ＵＯＶ）スキームは安全性があることを発見した。

【００４６】

具体的には、ＵＯＶの次数が２でありｐが２以外のあらゆる値である場合に対して（ここでｐは体Ｋの標数であり、また１の付加次数である）、ＵＯＶスキームは、不等式$q^{(v-n)-1} * n > 2^{40}$を満足するｖの値に対して安全であると考えられる。ＵＯＶの次数が２でありｐ＝２である場合、「酢」変数の数ｖは、不等式$v < n^2$であり、$q^{(v-n)-1} * n^4 > 2^{40}$を満足するように選択されうる。$n^2$／２より大きく$n^2$以下で

あるｖの値に対して、ＵＯＶはまた安全であると考えられ、集合Ｓ１を解くことは、ｋ個の式のランダム集合を解くことと同じほど困難であると考えられることが理解されよう。ｎ^{2}より大きいｖの値に対しては、ＵＯＶは安全でないと考えられる。

【００４７】

さらに、ＵＯＶの次数が３でありｐ＝２である場合、ＵＯＶスキームは、実質的にｎ＊（１＋ｓｑｒｔ（３））より大きくｎ^{3}／６以下であるであるｖの値に対して安全であると考えられる。ｎ^{3}／６より大きくｎ^{3}／２以下であるｖの値に対しては、ＵＯＶはやはり安全であると考えられ、また、集合Ｓ１を解くことはｋ個の式のランダム集合を解くことと同じほど困難であることが理解されよう。ｎ^{3}／２より大きいｖの値とｎ＊（１＋ｓｑｒｔ（３））未満であるｖの値に対しては、ＵＯＶは安全でないと考えられる。

【００４８】

加えて、ＵＯＶが次数３でありｐが２以外の数である場合、ＵＯＶスキームは、実質的にｎより大きくｎ^{4}以下であるｖの値に対して安全であると考えられる。ｎ^{3}／６より大きくｎ^{4}以下であるｖの値に対して、ＵＯＶはまた安全であると考えられ、また、集合Ｓ１を解くことはｋ個の式のランダム集合を解くことと同じほど困難であることが理解されよう。ｎ^{4}より大きいｖの値とｎ未満であるｖの値に対して、ＵＯＶは安全でないと考えられる。

【００４９】

集合Ｓ２がＨＦＥＶスキームのｋ個の多項式関数の集合ｆ（ａ）を含んでいる場合、集合Ｓ２は単変量多項式から誘導されたｋ個の関数を含む式を含くんでいるのが好ましい。単変量多項式は、Ｋ上の次数ｎの拡大体上で１００，０００以下の次数の多項式を含んでいるのが好ましい。

【００５０】

ＵＯＶスキームとＨＦＥＶスキームに対して選択されるパラメータの例を付録Ｉに示す。

【００５１】

分かりやすいように、互いに別々の実施形態を説明する中で記載されている本発明の様々な特徴もまた、１つの実施形態中に組み合わされて提供されていることが理解されよう。逆に、簡潔にするため、１つの実施形態を説明する中で記載されている本発明の様々な特徴もまた、互いに別々に又は適切に組み合わせて提供されうる。

【００５２】

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

Ａｖｉａｄ　Ｋｉｐｎｉｓ
ＮＤＳ　Ｔｅｃｈｎｏｌｏｇｉｅｓ
５　Ｈａｍａｒｐｅ　Ｓｔ．Ｈａｒ　Ｈｏｔｚｖｉｍ
Ｊｅｒｕｓａｌｅｍ－Ｉｓｒａｅｌ
ａｋｉｐｎｉｓ@ｎｄｓｉｓｒａｅｌ．ｃｏｍ
Ｊａｃｑｕｅｓ　Ｐａｔａｒｉｎ，Ｌｏｕｉｓ　Ｇｏｕｂｉｎ
Ｂｕｌｌ　ＳｍａｒｔＣａｒｄｓ　ａｎｄ　Ｔｅｒｍｉｎａｌｓ
６８，ｒｏｕｔｅ　ｄｅ　Ｖｅｒｓａｉｌｌｅｓ－ＢＰ４５
７８４３１　Ｌｏｕｖｅｃｉｅｎｎｅｓ　Ｃｅｄｅｘ－Ｆｒａｎｃｅ
｛Ｊ．Ｐａｔａｒｉｎ，Ｌ．Ｇｏｕｂｉｎ｝@ｆｒｌｖ．ｂｕｌｌ．ｆｒ

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Ｇｒｏｂｎｅｒ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、[１２]、[１６]、[２１]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、[１４]、[１７]、[１８]、[２０]）、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、ＵＯＶおよびＨＦＥＶを提示する。ＵＯＶは非常

に単純なスキームである。すなわち、（[１６]の）原型の「油と酢」署名スキームは解読された（[１０]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）、[１０]の攻撃は成功せず、（ＵＯＶ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、ＨＦＥＶと呼ばれる別のスキームも提示する。ＨＦＥＶは、（[１４]の）ＨＦＥのアイデアと酢変数のアイデアを結び付けている。ＨＦＥＶは、原型のＨＦＥ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１３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$_{1}$，…，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】

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

である（セクション８では

【数５】

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

も可能であることを示す）。署名ｘは、ｘ＝（ｘ$_{1}$，…，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$^{n+v}$→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】

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

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$_{1}$，…，ａ$_{n}$（「油」未知数）およびａ’$_{1}$，…，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$_{1}$，…，ａ$_{n}$，ａ’$_{1}$，…，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ァイン関数である。各値ｙ$_{i}$（１≦ｉ≦ｎ）は、ｘ$_{j}$個の未知数（１≦ｊ≦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】

$$\forall i,\ 1 \le i \le n,\ y_i = P_i(x_1, ..., x_{n+v}) \qquad (P)$$

（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$_{1}$，…，ａ$_{n}$およびＫのエレメントであるｖ個の未知数ａ’$_{1}$，…，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$_i$でアファインであるため）。

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×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$_1$，…，ａ$_n$，ａ’$_1$，…，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に由来する。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≦ｉ≦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は対応する２ｎ×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×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１０】

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

の表現を得る。Ｓは２ｎ×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×ｎのゼロ部分行列を持つ２ｎ×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ＥＦ$^{-1}$の不変部分空間である。

証明：　[１０]を参照されたい。
定義３．４：　可逆行列G_jに対して、G_{ij}を$G_{ij}=G_iG_j^{-1}$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１１】

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

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$G_iG_j^{-1}$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、[１０]で研究されている。[１０]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１２】

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

上の式で、左上行列はｎ×ｎゼロ行列、A_iはｎ×ｖ行列、B_iはｖ×ｎ行列、C_iはｖ×ｖ行列、Ｓは（ｎ＋ｖ）×（ｎ＋ｖ）の可逆線形行列である。
定義４．３：　E_iを
【数１３】

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

と定義する。
補題２　形式
【数１４】

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

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$_1$，…，Ｅ$_n$の任意の線形結合もまた形式
【数１５】

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

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$_1$，…，Ｅ$_n$の可逆線形結合であるとする。その場合、Ｅ$_k$$^{-1}$が存在する任意のｋに対して、行列ＦＥ$_k$$^{-1}$は、ｄ＝ｖ－ｎの場合に
【数１６】

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

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、Ｉ$_1$はｎ－ｄ以上の次元を持つ部分空間であり、ＦＥ$_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１７】

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

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１８】

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

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１９】

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

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$_1$，…，Ｇ$_n$の可逆線形結合であるとする。その場合、Ｇ$_k$$^{-1}$が存在する任意のｋに対して、行列ＦＧ$_k$$^{-1}$は、ｄ＝ｖ－ｎの場合に
【数２０】

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

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２１】

$$FG_k^{-1} = (\alpha_1 G_1 + \cdots + \alpha_n G_n) G_k^{-1}$$
$$= S(\alpha_1 E_1 + \cdots + \alpha_n E_n) S^t (S^t)^{-1} E_k^{-1} S^{-1} = S(\alpha_1 E_1 + \cdots + \alpha_n E_n) E_k^{-1} S^{-1}$$

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ＦＧ$_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$，…，Ｇ$_n$のランダムな線形結合を使用し、それにＧ$_k$行列のうちの１つの逆行列を乗算する。次に、この行列のすべての最小不変部分空間を計算する（行列Ａの最小不変部分空間は、行列Ａの自明でない不変部分空間を含まない。これらの部分空間は、Ａの固有多項式の既約因数に対応する）。これは、標準線形代数法を使用して確率的多項式時間で行うことができる。この行列は、Ｏの部分空間である不変部分空間を持つ場合がある。
次の補題は、Ｏに包含されている部分空間とランダムな部分空間とを区別できるようにする。
補題３　Ｈが線形部分空間であり、Ｈ⊂Ｏである場合、Ｈのすべてのｘ，ｙおよびすべてのｉに対して、Ｇ$_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２２】

$$G_i(x,y) = xS \begin{pmatrix} 0 & A_i \\ B_i & C_i \end{pmatrix} S^t y^t = x' \begin{pmatrix} 0 & A_i \\ B_i & C_i \end{pmatrix} (y')^t = 0$$

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$_1$，…，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$^{d-1}$・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２３】

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

（または

【数２４】

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

）

特性

（Ａ）が（ｎ＋ｖ）個の変数ｘ$_1$，…，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２５】

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

（より一般的には

【数２６】

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

）である場合、おそらく、そのような（Ａ）の大部分に対して、（ｘ’$_1$，…，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’$_i$・ｘ’$_j$の項がない）ような変数の線形変換（ｘ$_1$，…，ｘ$_{n+v}$）→（ｘ’$_1$，…，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２７】

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

すべてのｘ’$_i$・ｘ’$_j$（ｉ≦ｎかつｊ≦ｎ）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）・ｎ個の変数α$_{i,j}$（１≦ｉ≦ｎ＋ｖ、１≦ｊ≦ｎ）を持つ

【数２８】

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

個の二次方程式の系が得られる。したがってｖ≧約

【数２９】

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

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３０】

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

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３１】

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

（これらの新しい変数ｙ$_1$，…，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α$_{i,j}$係数（１≦ｉ≦ｎ、１≦ｊ≦ｎ＋ｖ）を段階的に見つける。
・まず、α$_{1,1}$，…，α$_{1,n+v}$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α$_{2,1}$，…，α$_{2,n+v}$を求める。この条件によって、（ｎ＋ｖ）個の未知数α$_{2,j}$（１≦ｊ≦ｎ＋ｖ）を持つｎ個の線形方程式から成る系が得られる。
【数３２】

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

・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α$_{3,1}$，…，α$_{3,n+v}$を求める。この条件は、（ｎ＋ｖ）個の未知数α$_{3,j}$（１≦ｊ≦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３３】

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

・以下同様に進める。
・最後に、（Ｓ’）が$y_1 y_n$項、$y_2 y_n$項，…，$y_{n-1} y_n$項のいずれも含まないように$\alpha_{n,1}$，…，$\alpha_{n,n+v}$を求める。この条件によって、（ｎ＋ｖ）個の未知数$\alpha_{n,j}$（１≦ｊ≦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３４】

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

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３５】

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

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$\alpha_{i,j}$個の定数（すなわち、ｎ＋１≦ｉ≦ｎ＋ｖかつ１≦ｊ≦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３６】

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

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}，…，y_{n+v}を求める。
【数３７】

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

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、$x \rightarrow x^2$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≦ｉ≦ｎとしたｎ個の二次方程式$y_1 = P_i(x_1, \cdots, x_{n+v})$の集合であり、ｙ＝（$y_1, \cdots, y_n$）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}でなければならず、そのため、ｖ＝２ｎの場合、署名の典型的な長さは少なくとも３×１２８＝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３８】

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

この式で、L_iは（$x_1, \cdots, x_{n+v}$）に基づく線形関数であり、L_iの係数は、（$y_1, \cdots, y_n$）に基づくハッシュ関数によって生成される。
例えば、（$\alpha_1, \alpha_2, \cdots, \alpha_{n+v}$）＝Ｈａｓｈ（$y_1, \cdots, y_n$｜｜ｉ）の$L_i$（$y_1, \cdots, y_n, x_1, \cdots, x_{n+v}$）＝$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_{n+v} x_{n+v}$，である。ここで、（$q^n \geqq 2^{128}$の代わりに）$q^n \geqq 2^{64}$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３×６４＝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≦ｎに対して以下のタイプのものである。
【数４０】

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

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ことが常に可能である。

【数４１】

$$v \le \left(1+\sqrt{3}\right)n$$

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，…，d_{n+v}）の集合Ｖを探す。
【数４２】

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

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・（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）－２$x_j x_k x_l$、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・（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４３】

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

であるとき、すなわち、
【数４４】

$$v \le \left(1+\sqrt{3}\right)n$$

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４５】

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

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４６】

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

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４７】

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

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）－$2x_jx_k$、すなわち、$2d_jd_k$となる。）

注３：　次数２では、不平衡な「油と酢」公開鍵は、

【数４８】

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

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４９】

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

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５０】

$$f(a)=\sum_{i,j}\beta_{ij}a^{q^{\theta ij}+q^{\varphi ij}}+\sum_{i}\alpha_i a^{q^{\varepsilon i}}+\mu_0, \qquad (1)$$

上記のβ_{ij}、α_iおよびμ_0は、体

【数５１】

$$F_{q^n}$$

のエレメントである。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，…，a'_v）がＫの変数のｖ‐タプルであるとする。今度は、（１）の各α_iが、基底における各ｎ個のα_i構成エレメントが、酢変数a'_1，…，a'_vの秘密ランダム線形関数であるような

【数５２】

$$F_{q^n}$$

のエレメントであるとする。そして（１）では、μ_oが、基底における各ｎ個のμ_0構成エレメントが、変数a'_1，…，a'_vの秘密ランダム二次関数であるような

【数５３】

$$F_{q^n}$$

のエレメントであるとする。そうすると、ｎ＋ｖ個の変数a_1，…，a_n，a'_1，…，a'_vは、変数x_1，…，x_{n+v}を得るために秘密全単射アファイン関数ｓによって混じり合う。以前と同様、ｔ（b_1，…，b_n）＝（y_1，…，y_n）となり、ここでのｔは秘密全単射アファイン関数である。次に、公開鍵はｎ個の方程式$y_i=P_i$（x_1，…，x_{n+v}）として与えられる。署名を計算するには、酢値a'_1，…，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α_iを計算する。そうすると、単変量方程式（１）が

【数５４】

$$F_{q^n}$$

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５５】

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

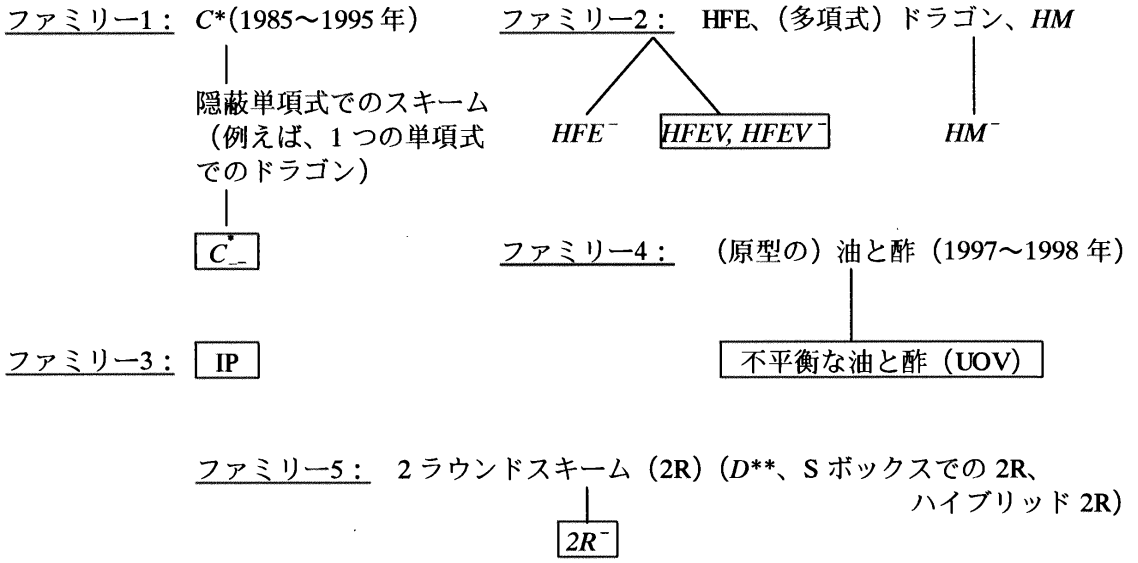
この式で、ａ＝（ａ$_1$，…，ａ$_n$）（ａ$_1$，…，ａ$_n$は「油」変数）であり、β$_1$、β$_2$、β$_4$、β$_8$およびβ$_{16}$はｖ個の酢変数を持つｎ個の秘密線形関数によって与えられ、β$_0$はｖ個の酢変数を持つｎ個の秘密線形関数によって与えられるとする。この例では、署名を次のように計算する。すなわち、酢変数をランダムに選択し、結果の次数１７の方程式をａで解く。
注：　ＵＯＶとは異なり、ＨＦＥＶでは、（ａ^{17}、ａ^{12}、ａ^{10}などの）油×油の項、（β$_{16}$ａ^{16}、β$_8$ａ^{8}などの）油×酢の項、および（β$_0$の）酢×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。
１１．ＵＯＶ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。
１２．ＨＦＥＶ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。
１３．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ＵＯＶやＨＦＥＶ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妙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おり、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 $x \rightarrow x^d$ 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５６】



・ＨＦＥは、[１４]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、[１４]の拡張版で提供された５００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＝８０およびｄ＝９６とする純粋なＨＦＥである）。

・ＨＦＥ⁻は、公開方程式の一部が公開されていないＨＦＥ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ＨＦＥ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）。[１４]の拡張版では、ＨＦＥ⁻についての５００米ドルの２番目のチャレンジが説明されている。

・ＨＦＥＶは、本論文で説明している。ＨＦＥＶおよびＨＦＥＶ⁻は、解読するのが非常に難しいようである。さらに、ＨＦＥＶは、原型のＨＦＥよりも効率的であり、わずか８０ビットの公開鍵署名を実現することができる。

・ＨＭおよびＨＭ⁻は、[２０]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ＨＭではなくＨＭ⁻の使用を推奨できるかもしれない）。

・ＩＰは、[１４]で設計された。ＩＰ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（[１９]を参照）。ＩＰ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、[１６]で提示され、[１０]で解読された。
・ＵＯＶは、本論文で説明している。ＩＰとともに、これらは確実に最も単純なスキームである。
・２Ｒは、[１７]および[１８]で設計された。[３]により、入力に少なくとも１２８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、２Ｒ－アルゴリズムになる（[５]で示されている２Ｒ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、（ＩＰ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、ＲＳＡ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ＤＥＳ）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、ｐｐ．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（ＡＡＥＣＣ－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、ＬＮＣＳｎ°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

【図面の簡単な説明】

【図１】　メッセージに対してディジタル署名を発生してこれを検証するシステムであり、本発明の好ましい実施形態に従って構成され動作するシステムの好ましい実現例の略ブロック図である。

【図２Ａ】　メッセージに対してディジタル署名を発生する好ましいディジタル署名暗号方法であり、本発明の好ましい実施形態に従って動作する方法の略フローチャートである。

【図２Ｂ】　図２Ａのディジタル署名を検証する好ましいディジタル署名暗号方法であり、本発明の好ましい実施形態に従って動作する方法の略フローチャートである。

【図１】

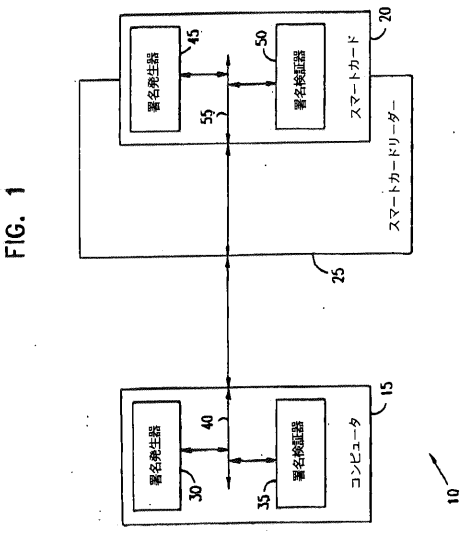
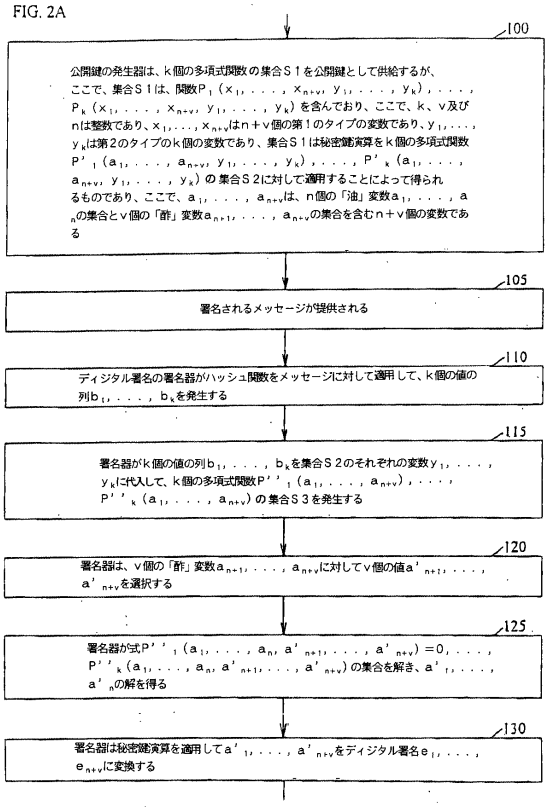


FIG. 1

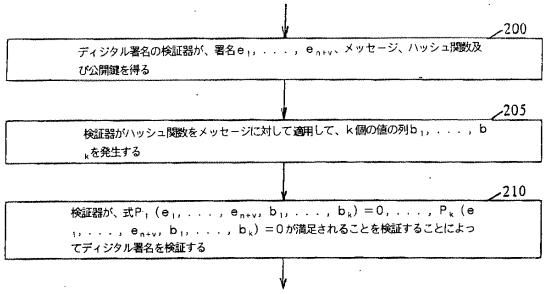
【図２Ａ】

FIG. 2A



【図２Ｂ】

FIG. 2B



フロントページの続き

合議体
審判長　吉岡　浩
審判官　野仲　松男
審判官　鈴木　匡明

(56)参考文献　特表平１０－５０５４３９（ＪＰ，Ａ）
A. Kipnis and A. Shamir, “Cryptanalysis of the Oil and Vinegar Signature Scheme”, Advances in Cryptology－CRYPTO ’98（LNCS 1462），（独），Springer－Verlag, 1998年, Vol. 1462, p. 257－266
J. Patarin, “Hidden Field Equations（HFE） and Isomorphisms of Polynomials （IP）: two new Families of Asymmetric Algorithms”, EUROCRYPT ’96 Proceedings（LNCS 1070），（独），Springer－Verlag, 1996年, Vol. 1070, p. 33－48

(58)調査した分野(Int.Cl.，ＤＢ名)
G09C1/00