[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/32 (2006.01)

[12] 发明专利说明书

专利号 ZL 00801038.2

[45] 授权公告日 2006 年 11 月 15 日

[11] 授权公告号 CN 1285191C

[22] 申请日 2000.4.28 [21] 申请号 00801038.2

[30] 优先权

[32] 1999. 4.29 [33] EP [31] 99401048.6

[86] 国际申请 PCT/IB2000/000692 2000.4.28

[87] 国际公布 WO2000/067423 英 2000.11.9

[85] 进入国家阶段日期 2001.2.5

[71] 专利权人 CP8 技术公司

地址 法国卢旺茨那斯

[72] 发明人 雅克·帕塔林 阿维德·基普尼斯 路易斯·古宾

审查员 刘剑波

[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所

代理人 马 浩

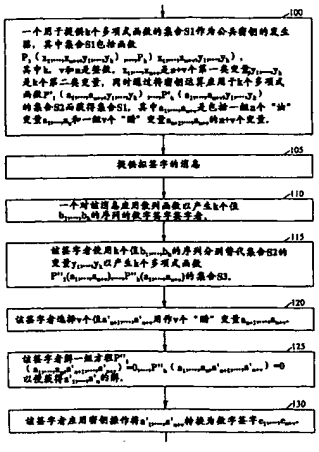
权利要求书 2 页 说明书 29 页 附图 3 页

[54] 发明名称

公共密钥签字的方法和系统

[57] 摘要

本发明提供了一种用于数字签字的加密方法。提供 k 个多项式函数的集合 S1 用作公共密钥，其中 k，v 和 n 是整数，x_1，...，x_{n+v}是 n + v 个第一类变量而 y_1，...，y_k是 k 个第二类变量，集合 S1 通过将密钥运算应用于 k 个多项式函数 $P'_k(a_1, \ldots, a_{n+v}, y_1, \ldots, y_k)$ 的集合 S2 而获得，其中 a_1，...，a_{n+v}指包括 n 个“油”变量和 v 个“醋”变量的集合的 n + v 个变量。提供拟签字的消息及对该消息应用散列函数以产生 k 个值 b_1，...，b_k的序列。这 k 个值用于替代集合 S2 的 k 个变量 y_1，...，y_k以产生 k 个多项式函数 $P''_k(a_1, \ldots, a_{n+v})$的集合 S3，同时选择 v 个值 a'_{n+1}，...，a'_{n+v}用作 v 个“醋”变量。解一组方程 $P''_k(a_1, \ldots, a'_{n+v}) = 0$ 以获得 a'_1，...，a'_n的解同时应用密钥运算将该解转换为数字签字。



1.一种数字签名加密方法，包括:

提供k个多项式函数的集合S1作为公共密钥，该集合S1包括函数$P_1(x_1,...,x_{n+v},y_1,...,y_k),...,P_k(x_1,...,x_{n+v},y_1,...,y_k)$，其中k,v和n是整数，$x_1,...,x_{n+v}$是n+v个第一类变量，而$y_1,...,y_k$是k个第二类变量，通过将密钥运算应用于k个多项式函数$P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$的集合S2而获得集合S1，其中$a_1,...,a_{n+v}$是一个包括一组n个“油”变量$a_1,...,a_n$和一组v个“醋”变量$a_{n+1},...,a_{n+v}$的n+v个变量;

提供将被签名的消息;

对该消息应用散列函数以产生k个值$b_1,...,b_k$的序列;

使用k个值$b_1,...,b_k$的序列分别替代集合S2的变量$y_1,...,y_k$以产生k个多项式函数$P''_1(a_1,...,a_{n+v}),...,P''_k(a_1,...,a_{n+v})$的集合S3;

选择v个值$a'_{n+1},...,a'_{n+v}$用作v个“醋”变量$a_{n+1},...,a_{n+v}$;

解一组方程$P''_1(a_1, ..., a_n,a'_{n+1}, ..., a'_{n+v}) = 0, ..., P''_k(a_1,..., a_n,a'_{n+1}, ..., a'_{n+v})=0$来获得$a'_1,...,a'_n$的解;

应用所述密钥运算将$a'_1,...,a'_{n+v}$转换为数字签名$e_1,...,e_{n+v}$; 以及

获取所述数字签名$e_1,...,e_{n+v}$。

2.根据权利要求1的方法，包括证实数字签名的步骤。

3.根据权利要求2的方法，其中证实步骤包括以下步骤:

获得签名$e_1,...,e_{n+v}$、消息、散列函数和公共密钥;

对此消息应用该散列函数来产生k个值$b_1,...,b_k$的序列; 以及

通过验证方程组$P_1(e_1,...,e_{n+v},b_1,...,b_k)=0, ..., P_k(e_1,..., e_{n+v}, b_1, ...,b_k)=0$被满足来证实所述数字签名。

4.根据权利要求1的方法，其中所述集合S2包括隐藏域等式醋HFEV方案的k个多项式函数的集合f(a)。

5.根据权利要求1的方法，其中集合S2包括不平衡油和醋UOV方案的k个多项式函数的集合S。

6.根据权利要求1的方法，其中所述提供k个多项式函数的集合S1的步骤包括选择“醋”变量的个数v为大于“油”变量的个数n的步骤。

7.根据权利要求1的方法，其中选择v以使q^v大于2^{32}，这里的q是有限域K的元素数目。

8.根据权利要求1的方法，其中所述提供k个多项式函数的集合S1的步骤包括从集合S2的k个多项式函数的子集合S2'中获得集合S1的步骤，子集合S2'的特征在于涉及k个多项式函数$P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$中任一变量$y_1,...,y_k$的分量的所有系数都是零，以及“醋”变量的个数v大于“油”变量的个数n。

9.根据权利要求8的方法，其中集合S2包括不平衡油和醋UOV方案的k个多项式函数的集合S，同时选择“醋”变量的个数v为满足以下条件中的一个：

(a)对于2次“油与醋”方案的域K中除2以外的每个特征p而言，v满足不等式$q^{(v-n)-1}*n^4>2^{40}$，

(b)对于3次“油与醋”方案中p = 2而言，v大于n*(1+sqrt(3))及低于或等于$n^3/6$，及

(c)对于3次“油与醋”方案中除2以外的每个p而言，v大于n及低于或等于n^4。

10.根据权利要求8的方法，其中集合S2包括不平衡油和醋UOV方案的k个多项式函数的集合S，同时选择“醋”变量的个数v使得对于2次“油与醋”方案的域K中特征p = 2而言，满足不等式$v<n^2$和$q^{(v-n)-1}*n^4>2^{40}$。

11.根据权利要求1的方法，其中所述密钥操作包括对n+v个变量$a_1,...,a_{n+v}$的秘密仿射变换s。

12.根据权利要求4的方法，其中所述集合S2包括一个从单变量多项式中导出的k个函数的表示式。

13.根据权利要求12的方法，其中所述单变量多项式包括一个其次数小于或等于100,000的单变量多项式。

公共密钥签字的方法和系统

本发明一般涉及密码学，更具体地涉及公共密钥密码学。

第一个公共密钥密码方案是在1975年引进的。自那时以来，开发和发布了许多公共密钥方案。许多公共密钥方案要求某些对整数n进行按模计算的算术运算，当今n通常为512至1024位之间。

由于n的位数相对地大，这类公共密钥方案在运行中相对地慢，被认为对随机存取存储器（RAM）和其他计算资源带来很重负担。当计算资源有限时例如在智能卡的应用中这类问题很尖锐。因此，为克服这类问题，已经开发了其他系列的不要求许多模n算术运算的公共密钥方案。在这类其他系列中有一些方案，其中公共密钥设定为一组在有限算术域K上的多变量多项式方程，其中K相对地小，例如在2至2^{64}之间。

该组k多变量多项式方程可以书写如下:

$y_1=P_1(x_1,...,x_n)$

$y_2=P_2(x_1,...,x_n)$

.

.

.

$y_k=P_k(x_1,...,x_n)$,

其中$P_1,...,P_k$是小次数多变量多项式，通常其次数小于或等于8，在许多情况下正好等于2。

这类方案的例子包括T. Matsumoto和H. Imai的C*方案，Jacques Patarin的HFE方案及Jacques Patarin的“油与醋”方案的基本形式。

在Proceedings of EUROCRYPT'88, Springer-Verlag, 第419-453页的文章“用于有效的签字证实和消息加密的公共二次多项式组”中描述了C*方案。在Proceedings of EUROCRYPT'96, Springer-Verlag,

第33-48页上的论文“隐藏域方程（HFE）和多项式的同构性（IP）：不对称算法的两个新族”中描述了HFE方案。1997年9月在Dagstuhl Workshop on Cryptography上宣读的论文“油与醋签字方案”中描述了Jacques Patarin的“油与醋”方案的基本形式

但在Proceedings of EUROCRYPT'98, Springer-Verlag LNCS no.1462,pp.257-266上Aviad Kipnis和Adi Shamir的论文“油与醋签字方案的加密分析”所公开发表的C*方案和“油与醋”方案的基本形式两者的加密分析中，业已证明了C*方案和“油与醋”方案的基本形式的不安全性。在两篇没有发表的名为“HFE公共密钥加密系统的加密分析”和“隐藏域方程（HFE）的实际加密分析”文中描述了HFE方案中的结构弱点，但现在并不认为HFE方案是一种妥协方案，这是因为对于良好选择的和合理的参数而言，用于破解HFE方案的计算量仍然很大。

在以下出版物中描述了相关技术的某些方面:

颁发给Shamir的美国专利5,263,085描述了新型数字签字方案，其安全性基于解出模合成n（modulo a composite n）的m个未知数k个多项式方程的难度；及

颁发给Shamir的美国专利5,375,170描述了新型数字签字方案，其安全性基于新类的双有理排列，这些排列具有小密钥并且要求很少算术运算。

以上提及的所有参考资料的公开内容和整个现有说明书都综合于此作为参考。

本发明试图改进数字签字加密方案的安全性，其中公共密钥给定为一组通常在有限算术域K上的多变量多项式方程。具体地说，本发明试图改进“HFE方案和油与醋”的基本形式的安全性。根据本发明修改而改进了安全性的“油与醋”方案在此称为不平衡“油与醋”（UOV）方案。根据本发明修改而改进了安全性的HFE方案在此称为HFEV方案。

在本发明中，提供k个多项式函数的集合S1用作公共密钥。集合S1最好包括函数$P_1(x_1,...,x_{n+v},y_1,...,y_k),...,P_k(x_1,...,x_{n+v},y_1,...,y_k)$，其中k，v和n是整数，$x_1,...,x_{n+v}$是n+v个第一类变量，而$y_1,...,y_k$是k个第二类变量。集合S1最好通过将密钥运算应用于k个多项式函数$P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$的集合S2而获得，其中$a_1,...,a_{n+v}$是一个包括一组n个“油”变量$a_1,...,a_n$和一组v个“醋”变量$a_{n+1},...,a_{n+v}$的n+v个变量。应知密钥运算可能包括对n+v个变量$a_1,...,a_{n+v}$的保密仿射变换s。

当提供拟签字的消息时，可以对该消息应用散列函数以产生k个值$b_1,...,b_k$的序列。这k个值$b_1,...,b_k$的序列最好用于分别替代集合S2的变量$y_1,...,y_k$以产生k个多项式函数$P''_1(a_1,...,a_{n+v}),...,P''_k(a_1,...,a_{n+v})$的集合S3。然后可以或者随机地或者按照预定选择算法来选择v个值$a'_{n+1},...,a'_{n+v}$用作v个“醋”变量$a_{n+1},...,a_{n+v}$。

一旦选择了v个值$a'_{n+1},...,a'_{n+v}$，最好解一组方程$P''_1(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0,...,P''_k(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0$来获得$a'_1,...,a'_n$的解。然后可以应用密钥运算将$a'_1,...,a'_{n+v}$转换为数字签字$e_1,...,e_{n+v}$。

所生成的数字签字$e_1,...,e_{n+v}$可以由证实器来证实，该证实器可能包括例如计算机或智能卡。为证实数字签字，证实器最好获得签字$e_1,...,e_{n+v}$、消息、散列函数和公共密钥。然后证实器可以对消息应用散列函数来产生k个值$b_1,...,b_k$的序列。一旦产生了k个值$b_1,...,b_k$的系列，证实器最好能通过证实满足方程$P_1(e_1,...,e_{n+v},b_1,...,b_k)=0,...,P_k(e_1,...,e_{n+v},b_1,...,b_k)=0$，从而证实该数字签字。

为此，提供了根据本发明优选实施例的数字签字加密方法，该方法包括以下步骤：提供k个多项式函数的集合S1作为密钥，该集合S1包括函数$P_1(x_1,...,x_{n+v},y_1,...,y_k),...,P_k(x_1,...,x_{n+v},y_1,...,y_k)$，其中k,v和n是整数，$x_1,...,x_{n+v}$是n+v个第一类变量，$y_1,...,y_k$是k个第二类变量，以及通过对k个多项式函数$P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$的集合S2应用密钥运算而获得集合S1，其中$a_1,...,a_{n+v}$是包括n个“油”变量

$a_1,...,a_n$的集合和v个“醋”变量$a_{n+1},...,a_{n+v}$的集合的n+v个变量，提供准备签字的消息，对消息应用散列函数以便产生k个值的系列$b_1,...,b_k$，分别将k个值的系列$b_1,...,b_k$替代集合S2的变量$y_1,...,y_k$以产生k个多项式函数$P''_1(a_1,...,a_{n+v}),...,P''_k(a_1,...,a_{n+v})$的集合S3，为v个“醋”变量$a_{n+1},...,a_{n+v}$选择v个值$a'_{n+1},...,a'_{n+v}$，解一组方程$P''_1(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0,...,P''_k(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0$以获得$a'_1,...,a'_n$的解以及应用密钥运算将$a'_1,...,a'_{n+v}$转换为数字签字$e_1,...,e_{n+v}$。

该方法最好包括证实数字签字的步骤。证实步骤最好包括以下步骤：获得签字$e_1,...,e_{n+v}$、消息、散列函数和公用密钥，对消息应用散列函数来产生k个值$b_1,...,b_k$的序列，以及证实满足方程组$P_1(e_1,...,e_{n+v},b_1,...,b_k)=0,...,P_k(e_1,...,e_{n+v},b_1,...,b_k)=0$。

密钥运算最好包括对n+v个变量$a_1,...,a_{n+v}$的保密仿射变换s。

集合S2最好包括HFEV方案的k个多项式函数的集合f(a)。在此情况下，集合S2最好包括一个包括从单变量多项式中导出的k个函数的表达式。该单变量多项式最好包括一个其次数小于或等于100,000的单变量多项式。

或者，集合S2可包括UOV方案的k个多项式函数的集合S。

上述提供步骤最好能包括选择“醋”变量的个数v为大于“油”变量的个数n的步骤。最好选择v为可使q^v大于2^{32}，其中q是有限域K的元数。

根据本发明的优选实施例，上述提供步骤包括从集合S2的k个多项式函数的子集合S2'中获得集合S1的步骤，子集合S2'的特征在于涉及k个多项式函数$P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$中任一变量$y_1,...,y_k$的分量的所有系数都是零，以及“醋”变量的个数v大于“油”变量的个数n。

集合S2最好包括UOV方案的k个多项式函数的集合S，且最好选择“醋”变量的个数v满足以下条件中之一：(a)对于2次“油与醋”方案的域K中除2以外的每个特征p而言，v满足不等式$q^{(v-n)-1}*n^4>2^{40}$，(b)对于3次“油与醋”方案中p=2而言，v大于n*(1+sqrt(3))及低于或等于

$n^3/6$; (c)对于3次“油与醋”方案的域K中除2以外的每个特征p而言，v大于n及低于或等于n^4。最好选择“醋”变量的个数v使得对于2次“油与醋”方案的域K中特征p = 2而言，满足不等式$v<n^2$和$q^{(v-n)-1}*n^4>2^{40}$。

根据本发明优选实施例还提供了对“油与醋”签字方法的改进，该改进包括使用比“油”变量更多的“醋”变量的步骤。最好选择“醋”变量的个数v满足以下条件中之一: (a)对于域K中除2以外的每个特征p和对于2次“油与醋”签字方法而言，v满足不等式$q^{(v-n)-1}*n^4>2^{40}$，(b)对于p = 2和对于3次“油与醋”签字方法而言，v大于n*(1+sqrt(3))及低于或等于$n^3/6$; (c)对于除2以外的每个p和对于3次“油与醋”签字方法而言，v大于n及低于或等于n^4。最好选择“醋”变量的个数v使得对于2次“油与醋”方案的域K中特征p = 2而言，满足不等式$v<n^2$和$q^{(v-n)-1}*n^4>2^{40}$。

根据下面结合附图对本发明的详细描述，将使本发明得到更能全面的理解。

图1是用于示明消息生成和证实数字签字的系统的优选实施例的简化框图，该系统根据本发明优选实施例进行构造和操作;

图2A是用于示明对消息生成数字签字的优选数字签字加密方法的简化流程图，该方法根据本发明优选实施例进行构造和操作;

图2B是用于示明证实图2A的数字签字的优选数字签字加密方法的简化流程图，该方法根据本发明优选实施例进行构造和操作。

附录I是准备由Springer-Verlag在Proceedings of Eurocrypt'99中出版的由Aviad Kipnis, Jacques Patarin和Louis Goubin所写文章，该文章描述了UOV和HFEV方案的变动内容。

现在参照图1，它是用于生成消息和证实数字签字的系统10的优选实施例的阐述性简化框图，系统10根据本发明优选实施例进行构造和操作。

系统10最好包括一个计算机15，例如通用计算机，它通过智能卡阅读器25与智能卡20通信。计算机15最好能包括一个数字签字发生器30和一个数字签字证实器35，它可能通过通信总线40交换数据。智能卡20

最好能包括一个数字签字发生器45和一个数字签字证实器50，它能通过通信总线55交换数据。

应知在通常的公共密钥签字方案应用中，消息的签字者和所签字的消息的接收者是一致商定公布的公共密钥和拟使用的散列函数的。在对散列函数采取折衷办法的情况下，签字者和接收者可能同意改变散列函数。应知公共密钥发生器不必是签字者或接收者。

数字签字证实器35最好能证实由数字签字发生器30和数字签字发生器45中的一个所生成的签字。类似地，数字签字证实器50可能证实由数字签字发生器30和数字签字发生器45中的一个所生成的签字。

现在参照图2A，它是用于在第一处理器（未示出）内对消息生成数字签字的优选数字签字加密方法的阐述性简化流程图，同时参照图2B，它是用于在第二处理器内证实图2A的数字签字的优选数字签字加密方法的阐述性简化流程图，图2A和2B的方法根据本发明优选实施例进行构造和操作。

应知道可以在硬件中，软件中或硬件和软件的组合中实施图2A和2B的方法。此外，第一处理器和第二处理器可以是相同的。或者，可以由图1的系统10实施该方法，其中第一处理器可以包括于例如计算机15中，第二处理器可以包括于智能卡20内，反之亦然。

图2A和2B的方法和图2A和2B的方法的应用描述于包括于此处的附录中。图2A和2B的方法可用于修改“油与醋”方案的基本形式和HFE方案，从而分别产生UOV和HFEV方案。

附录I包括一篇由Springer-Verlag出版的于1999年5月2－6日召开的Proceedings of EUROCRYPT'99中宣读而尚未发表的由Aviad Kipnis，Jacques Patarin和Louis Goubin编写的论文。包括于附录I的该论文也描述了具有小签字的UOV和HFEV方案的变动情形。

在图2A的数字签字加密方法中，k个多项式函数的集合S1最好由公共密钥发生器（未示出）作为公共密钥提供（步骤100），该发生器可能是例如图1的发生器30，图1的发生器45或一外部公共密钥发生器（未示出）。

集合S1最好包括函数$P_1(x_1,...,x_{n+v},y_1,...,y_k),...,P_k(x_1,...,x_{n+v},y_1,...,y_k)$，其中k，v和n是整数，$x_1,...,x_{n+v}$是n+v个第一类变量，而$y_1,...,y_k$是k个第二类变量。集合S1最好通过将密钥运算应用于k个多项式函数$P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$的集合S2而获得，其中$a_1,...,a_{n+v}$是包括一组n个“油”变量$a_1,...,a_n$和一组v个“醋”变量$a_{n+1},...,a_{n+v}$的n+v个变量。应知密钥运算可能包括对n+v个变量$a_1,...,a_{n+v}$的仿射变换s。

名词“油”变量和“醋”变量系指JacquesPatarin的“油与醋”方案的基本形式中定义的“油”变量和“醋”变量，该方案描述于以上所述的于1997年9月在Dagstuhl Workshop on Cryptgraphy上宣读的名为“油与醋签字方案”的论文中。

最好是在提供需要签字的消息时（步骤105），签字者可以对该消息应用散列函数来产生k个值$b_1,...,b_k$的序列（步骤110）。签字者可以是例如图1的发生器30或发生器45。k个值$b_1,...,b_k$的序列最好用于分别替代集合S2的变量$y_1,...,y_k$以便产生k个多项式函数$P''_1(a_1,...,a_{n+v}),...,P''_k(a_1,...,a_{n+v})$的集合S3（步骤115）。然后可以随机地选择v个值$a'_{n+1},...,a'_{n+v}$用作v个“醋”变量$a_{n+1},...,a_{n+v}$（步骤120）。或者可以按照预定选择算法来选择v个值$a'_{n+1},...,a'_{n+v}$。

一旦选择了v个值$a'_{n+1},...,a'_{n+v}$，最好解一组方程$P''_1(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0,...,P''_k(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0$以求得$a'_1,...,a'_n$的解（步骤125）。然后可以应用密钥运算将$a'_1,...,a'_{n+v}$转换为数字签字$e_1,...,e_{n+v}$（步骤130）。

所生成的数字签字$e_1,...,e_{n+v}$可以根据参照图2B所描述的方法由数字签字证实器（未示出）来证实，该证实器可以包括图1的证实器35或证实器50。为证实数字签字，证实器最好获得签字$e_1,...,e_{n+v}$、消息、散列函数和公共密钥（步骤200）。然后证实器可以对消息应用散列函数来产生k个值$b_1,...,b_k$的序列（步骤205）。一旦产生了k个值$b_1,...,b_k$的序列，证实器最好能通过证实满足了方程

$P_1(e_1,...,e_{n+v},b_1,...,b_k)=0,...,P_k(e_1,...,e_{n+v},b_1,...,b_k)=0$，从而证实该数字签字（步骤210）。

应知以上所述的数字签字的生成和证实可如附录I中所描述地通过允许集合S2包括UOV方案的k个多项式函数的集合S而能用于UOV。或者，通过允许集合S2包括HFEV方案的k个多项式函数的集合f(a)，可证以上所述的数字签字的生成和证实可如附录I中所描述地用于HFEV。

如附录I中所述，图2A和2B的方法允许获得数字签字，它们通常小于在传统数论加密方案例如众所周知的RSA方案中获得的数字签字。

根据本发明的优选实施例，当S2包括UOV方案的k个多项式函数的集合S时，可提供个数v的“醋”变量给集合S1，v选择为大于“油”变量的个数n。或者，可以选择v为能使q^v大于2^{32}，其中q是有限域K的元数，而在此有限域K上提供集合S1，S2和S3。

尤为最好的是，可以从集合S2的k个多项式函数的子集合S2'中获得集合S1，子集合S2'的特征在于涉及k个多项式函数$P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$中任一变量$y_1,...,y_k$的分量其所有系数都是零，以及“醋”变量的个数v大于“油”变量的个数n。

在“油与醋”的基本方案中，选择“醋”变量的个数v为等于“油”变量的个数n。对于v个变量的这一选择，作为本发明的发明者之一的Aviad Kipnis及Adi Shamir已经在以上所述的Proceedings of CRYPTO98, Springer, LNCS no.1462的257－266页上提供了对基本“油与醋”签字方案的加密分析，它证明了基本“油与醋”签字方案的不安全性。此外，通过应用由Kipnis和Shamir所描述的同一方法，能够证明，对于低于“油”变量的个数n的任何“醋”变量的个数v而言，此基本“油与醋”方案是不安全的。

本发明的发明者业已发现，如附录I中所述，如果修改“油与醋”方案，使“醋”变量的个数v大于“油”变量的个数n从而使“油与醋”方案不平衡，则所得不平衡的“油与醋”方案可能是安全的。

具体地说，对于2次UOV和对于除2以外的p的所有值，当v值满足不等式$q^{(v-n)-1}*n^4>2^{40}$时，可以认为UOV方案是安全的，其中p是域K的特征而p是1的加法阶。对于2次UOV方案和对于p = 2而言，可选择“醋”变量的个数v使之满足不等式$v<n^2$和$q^{(v-n)-1}*n^4>2^{40}$。应知对于大于$n^2/2$但小于或等于n^2的v值而言，也可认为UOV是安全的，而求解集合S1则是与求解k个方程的随机组同样的困难。对于高于n^2的v值而言，认为UOV是不安全的。

此外，对于3次UOV和对于p = 2，当v值显著地大于n*(1+sqrt(3))和低于或等于$n^3/6$时，可认为UOV方案安全。应知对于高于$n^3/6$但低于或等于$n^3/2$的v值而言，也可认为UOV是安全的，而求解集合S1则可认为是与求解k个方程的随机组一样地困难。对于高于$n^3/2$的v值和对于低于n*(1+sqrt(3))的v值而言，认为UOV是不安全的。

此外，对于3次UOV和对于2以外的p，当v值显著地大于n及低于或等于n^4时，则认为UOV方案安全。应知对于高于$n^3/6$但低于或等于n^4的v值而言，也可认为UOV是安全的，而求解集合S1则可认为是与解k个方程的随机组一样地困难。对于高于n^4的v值和对于低于n的v值而言，认为UOV是不安全的。

最好，在集合S2包括HFEV方案的k个多项式函数的集合f(a)的情形下，集合S2能包括一个包括从单变量多项式中导出的k个函数的表示式。该单变量多项式最好能包括一个在K之上n次扩展域内次数小于或等于100,000的多项式。

附录I示明了UOV和HFEV方案中所选参数的例子。

应知为清楚起见分别在各个实施例的上下文中描述的本发明的不同特点也能以组合形式提供给单个实施例。相反，为清楚起见而在单个实施例的上下文中描述的本发明的不同特点也可分别或以任何适当的亚组合形式提供。

熟悉现有技术的人当知本发明并不局限于此处已具体示明和描述的内容。相反，本发明的范围只由后附权利要求书定义。

附录I

不平衡油与醋签字方案

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
78451 Louveciennes Cedex - France
{J.Patarin,L.Goubin}@frlv.bull.fr

摘 要

在〔16〕中，J. Patarin设计了一个新方案，称为“油与醋”，用于计算不对称签字。它很简单，可以很快地计算（在秘密和公共密钥两种情况下）而在智能卡实施中需要很小的RAM。此方案的想法包含将二次方程隐藏于有限域K中n个称为“油”的未知数和v=n个称为“醋”的未知数内。此初始方案由A. Kipnis和A. Shamir在〔10〕中提出。在此论文中，我们研究初始方案的某些很简单的变动，其中v>n（而不是v=n）。这些方案称为“不平衡油与醋”（UOV），因为我们具有比“油”未知数更多的“醋”未知数。我们证明，当v≅n时，可以扩充〔10〕的概念，但当例如v≥2n时，该方案的安全性仍然是一个悬案。此外，当$v\cong n^2/2$时，该方案的安全性完全相当于（如果我们接受一个很自然但没有证明的特性的话）解$n^2/2$个未知数的n个二次方程的随机组（没有秘密信息）的问题。然而，我们显示了（在特征2的情形中）当v≥2n时，求解通常是容易的。然后我们将看到，把油与醋的想法和HFE方案综合是容易的〔14〕。现在从实际的和理论的观点两者来看，所得的称为HFEV的方案也都是很有趣的。UOV签字的长度可以短至192位而对于HFEV则可以短至80位。

附注：可从作者处取得此论文的扩展版本。

1.引言

1985年以来，不同作者（见例如[7],[9],[12],[14],[16],[17],[18],[21]）曾提出过某些公共密钥方案，其中公共密钥给定为在小有限域K上的一组多变量二次（或更高次）方程。

解这类方程组的一般问题是NP硬的（参照[8]）（甚至在二次的情形下）。此外，当未知数个数例如n≥16时，最好的已知算法通常并不比彻底搜索好多少（当n很小时，Gröbner基本算法更为有效，见[6]）。

就智能卡实施中的速度或所需RAM而言，通常这些方案是很有效的。（然而，公共密钥的长度通常>1千字节。还有，有时应该注意到可以不用公共密钥来完成密钥的计算）。最严重的问题是，为引进秘密信息（以便允许计算签字或允许将其密钥已知的消息解密），所生成的公共方程组通常成为所有可能方程的小子集，以及在很多情况下已经破解或破译（break）这些算法。例如[7]已由它们的作者破解，而[12],[16],[21]业已破解。然而，有许多方案仍未被破解（例如[14],[17].[18],[20]），还有，在很多情况下提出了某些很简单的变动来修补这些方案。因此，现在我们不知道在小有限域内设计具有多变量多项式的公共密钥算法的想法是否为很有用的想法（其中只有某些过于简单的方案是不安全的）。

在此论文中，我们将提出两个新方案：UOV和HFEV。UOV是一个很简单的方案：初始的油与醋签字方案（[16]的）被破解（见[10]），但如果我们具有比“油”未知数个数多得多的“醋”未知数个数（可在第2段中找到“油”和“醋”未知数的定义），则[10]的处理就不起作用而此更为一般的方案（称为UOV）仍然是一个悬案。我们也可研究3次油与醋方案（而不是2次）。然后我们将提出另一个方案，称为HFEV。HFEV将HFE（[14]的）和醋变量的想法结合起来。HFEV看起来比初始HFE方案更有效。最后，在第13段中，我们提出我们所知道的在此多变量多项式领域中的主要方案。

2.二次（初始的和不平衡的）油与醋

设$K = F_q$为一个小有限域（例如$K = F_2$）。设n和v为两个整数。拟签字的消息（或其散列函数）表示为K^n的一个元素，以$y=(y_1,...,y_n)$表

明。通常$q^n \cong 2^{128}$（在第8段中，我们将了解到$q^n \cong 2^{64}$也可以）。签字x表示为由$x=(x_1,...,x_{n+v})$标明的K^{n+v}的一个元素。

密钥

密钥由两部分组成:

1.一个双射和仿射函数s: $K^{n+v} \rightarrow K^{n+v}$。所谓“仿射”，是指输出的每个分量可以写为n+v个输入未知数的1次多项式，其系数在K中。

2.n个以下类型的方程的集合（S）:

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

系数γ_{ijk},λ_{ijk},ξ_{ij},ξ'_{ij}和δ_i是这些n个方程的密钥系数。值$a_1,...,a_n$（“油”未知数）和$a'_1,...,a'_v$（“醋”未知数）位于K内。注意到这些方程（S）不包含$a_i a_j$项。

公共密钥

设A为由$A = (a_1,...,a_n,a'_1,...,a'_v)$定义的$K^{n+v}$的元素。A转换为$x=s^{-1}(A)$，其中s是自$K^{n+v}$至$K^{n+v}$的秘密的双射和仿射函数。各个值$y_i$（$1 \leq i \leq n$）可写为未知数$x_j$（$1 \leq j \leq n+v$）中总次数为2的多项式$P_i$。我们用（*P*）表示以下n个方程的组:

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

这些n个二次方程（*P*）（在n+v个未知数x_j中）是公共密钥。

签字的计算（带有密钥）

y的签字x的计算如下进行:

步骤1: 求K的n个未知数$a_1,...,a_n$和K的v个未知数$a'_1,...,a'_v$使其满足n个方程（S）。这可以如下进行: 随机地选择v个醋未知数a'_i，然后通过高斯约简从（S）中计算a_i未知数（因为没有$a_i a_j$项，当a'_i是固定时（S）方程在a_i未知数中是仿射的）.

附注: 如果我们求不到解，只需再用新的随机醋未知数来尝试。在几次尝试后，获得至少一个解的概率是很高的，因为在Fq上的一个nxn矩阵为可逆的概率不是可以忽略的。（它确切地是

$(1-\frac{1}{q})(1-\frac{1}{q^2})...(1-\frac{1}{q^{n-1}})$。对于q = 2，此概率近似于30%，而对于q>2，此概率甚至更高。）

步骤2: 计算$x=s^{-1}(A)$，其中$A = (a_1,...,a_n,a'_1,...,a'_v)$。x是y的签字。

签字的公共证实

当且仅当所有（*P*）都得到满足时，y的签字x才是有效的。其结果是，不需任何密钥用于检查签字是否有效：这是不对称签字方案。

附注："油与醋"名称来自以下事实：在方程（S）中"油未知数"a_i和"醋未知数"a'_j并不全混合在一起；不存在a_ia_j乘积。然而在（*P*）中，由于通过s变换而将未知数"混合"，因此隐藏了此一特性。此特性是否"隐藏得足够"？事实上，此问题正好意味着："方案是否安全？"。当v = n时，我们称之为"油与醋"方案，因为首次在[16]中提出此情形。此情形在[10]中被破解。很容易看到，当v<n时，[10]的加密分析可以按完全相同方式进行。然而，我们将看到，v>n的情形要困难得多。当v>n时，我们称之为"不平衡油与醋"方案。

3.v = n情况的加密分析（据[10]）

[10]的处理想法主要如下：为将油变量与醋变量分离，注意（*P*）的n个公共方程的二次形式，暂时忽略线性项。设G_i（$1\le i\le n$）为公共方程（*P*）的二次形式P_i的相应矩阵。集合（*S*）中方程的二次项部分表示为具有形式$\begin{pmatrix}0 & A\\ B & C\end{pmatrix}$的相应的2nx2n矩阵，其左上nxn个零子矩阵由以下事实造成：油变量不能与油变量相乘。在使用线性函数s将内部变量隐藏后，我们得到矩阵的表示式$G_i = S\begin{pmatrix}0 & A_i\\ B_i & C_i\end{pmatrix}S^t$，其中S是可逆2nx2n矩阵。

定义3.1：定义油子空间为K^{2n}中的所有向量的其第二半部分只包含零的线性子空间。

定义3.2：定义醋子空间为K^{2n}中的所有向量的其第一半部分只包含零的线性子空间。

引理1.设E和F为一个2nx2n矩阵，它在左上部分具有nxn个零子矩阵。如果F是可逆的，则油子空间是一个EF^{-1}的不变子空间。

证明：见[10]。

定义3.4：对于一个可逆矩阵G_j，定义$G_{ij} = G_i G_j^{-1}$。

定义3.5：设O为油子空间的S^{-1}的映象。

为求得油子空间，应用以下定理：

定理3.1：O为所有矩阵G_{ij}的公共不变子空间。

证明：

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

$$= S\begin{pmatrix} 0 & A_i \\ B_i & C_i \end{pmatrix} \begin{pmatrix} 0 & A_j \\ B_j & C_j \end{pmatrix}^{-1} S^{-1}$$

该两个在内部的矩阵具有引理1中E和F的形式。因此，油子空间是这种内项的一个不变子空间而O是$G_i G_j^{-1}$的一个不变子空间。[10]中研究了求矩阵集合的公共不变子空间的问题。应用[10]中的算法能给出O。然后取V为n维的任意子空间且使得$V + O = K^{2n}$，它们能给出等效的油和醋的分离。一旦我们得到这种分离后，就将以前略去的线性项放回，我们为醋变量取随机值，从而留下n个油变量的n个线性方程。

附注：当v>n时引理1不再成立。油空间仍然由E和F映射入醋子空间。然而F^{-1}不再一定能使用油子空间的E来将映象映射回至油子空间而这就是为什么在不平衡的情况下初始油与醋的加密分析无效的原因。

4.v>n和v≅n时的加密分析

本节中，我们将描述上述处理问题想法的修正，只要v-n很小，此修正结果就可一直应用（更确切地是，此处理问题想法预期的复杂度近似于$q^{(v-n)-1} \cdot n^4$）。

定义4.1：本节中定义油子空间为K^{n+v}中其最后v个坐标只是零的所有向量的线性子空间。

定义4.2：本节中定义醋子空间为K^{n+v}中其最先n个坐标只是零的所有向量的线性子空间。

本节中，我们从方程的齐次二次项开始，暂时略去线性项。矩阵G_i具有以下表示：

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

其中左上矩阵是nxn零矩阵，A_i是nxv矩阵，B_i是vxn矩阵，C_i是vxv矩阵，而S是(n+v)x(n+v)可逆线性矩阵。

定义4.3：定义E_i为$\begin{pmatrix} 0 & A_i \\ B_i & C_i \end{pmatrix}$。

引理2：对于任何具有$\begin{pmatrix} 0 & A \\ B & C \end{pmatrix}$形式的矩阵E，以下结果成立：

a)E将油子空间变换为醋子空间。

b)如果存在矩阵E^{-1}，则醋子空间的E^{-1}映象是在其中包含n维油子空间的v维子空间。

证明：a)直接从油与醋子空间的定义中得到。

当给出a)时则b)是直接结果。

我们提出的算法是概率性的。它寻找由S变换之后的油子空间的不变子空间。该算法第一次尝试成功的概率是小的。因此我们必须使用不同输入来重复进行。我们使用以下特性：矩阵$E_1,...,E_n$的任何线性组合也具有形式$\begin{pmatrix} 0 & A \\ B & C \end{pmatrix}$。以下定理解释为何一个不变子空间可以在一定概率下存在。

定理4.1：设F为矩阵$E_1,...,E_n$的一个可逆线性组合。则对于使得E_k^{-1}存在E_k^{-1}的任何k而言，矩阵FE_k^{-1}具有一个不无意义的不变子空间，它也是油子空间的子空间，对于d=v-n而言其概率不小于$\frac{q-1}{q^{2d}-1}$。

证明：见本论文的扩展版本。

附注：有可能以少得多的努力为期望的特征向量获得较好结果：I_1是维数不小于n-d的子空间，并且由FE_k^{-1}映射为n维的子空间。一个非零向量映射为它本身的非零倍数的概率是$\frac{q-1}{q^n-1}$。为取得期望值，我们将它乘以I_1中的非零向量的个数。它给出的值不小于$\frac{(q-1)(q^{n-d}-1)}{q^n-1}$。由

于每个特征向量都计数q-1次，因此1维不变子空间的预期个数不小于$\frac{q^{n-d}-1}{q^n-1}\sim q^{-d}$。

我们如节3中那样定义O而对于O我们得到以下结果:

定理4.2: 设F为矩阵$G_1,...,G_n$的一个可逆线性组合。则对于使得G^{-1}_k存在的任何k，矩阵FG^{-1}_k具有一个非平凡不变子空间，它也是O的子空间，对于d=v-n的概率不小于$\frac{q-1}{q^{2d}-1}$。

证明:

$$FG_k^{-1}=(\alpha_1G_1+...+\alpha_nG_n)G_k^{-1}$$
$$=S(\alpha_1E_1+...+\alpha_nE_n)S^t(S^t)^{-1}E_k^{-1}S^{-1}=S(\alpha_1E_1+...+\alpha_nE_n)E_k^{-1}S^{-1}.$$

该内部项是具有所需概率的油子空间的不变子空间。因此，对于FG^{-1}_k同样如此，但我们得到的是O的子空间而不是油子空间的子空间。

如何求O?

取$G_1,...,G_n$的随机线性组合并将其乘以矩阵G_k中的一个的逆矩阵。然后我们计算此矩阵的所有最小不变子空间（矩阵A的最小不变子空间不包含矩阵A的非平凡不变子空间－这些子空间对应于A的特征多项式的不可约因子）。这可以使用标准线性代数技术在概率多项式时间内完成。此矩阵可以具有是O的子空间的不变子空间。

以下引理使我们可以区别包含于O中的子空间与随机子空间。

引理3: 若H是线性子空间且$H\subset O$，则对于H中的每个x,y和每个i，$G_i(x,y)=0$（此处我们视G_i为双线性形式）。

证明: 在油子空间中存在x'和y'使得x'=xS和y'=yS。

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

最后一项为零，这是因为x'和y'在油子空间内。

引理3给出多项式测试，用于区别O的子空间和随机子空间。如果使用的矩阵没有也作为O的子空间的最小子空间，则我们取$G_1,...,G_n$的

另一个线性组合，将它乘以矩阵G_k中的一个的逆矩阵并且再次尝试。在重复此过程大约q^{d-1}次后，我们能在好的概率下找到O的至少一个零向量。我们继续该过程，直至获得O的n个独立向量。这些向量组成了O。该过程的期望复杂度正比于$q^{d-1}\cdot n^4$。此处我们使用期望尝试数，直至求得一个非平凡不变子空间而项n^4包括我们完成每次尝试所需的计算性线性代数运算。

5.$o \cong \frac{n^2}{2}$（或$o \geq \frac{n^2}{2}$）的情况

特性

设（A）为(n+v)个变量$x_1,...,x_{n+v}$的n个二次方程的随机组（“随机”意味着这些方程的系数是均匀地和随机地选择的）。当$o \cong \frac{n^2}{2}$（而更一般地当$o \geq \frac{n^2}{2}$），对于大多数这种（A）有可能存在变量的线性变换$(x_1,...,x_{n+o}) \rightarrow (x'_1,...,x'_{n+o})$使那些用$(x'_1,...,x'_{n+v})$写出的($A$)方程的集合($A'$)是一个“油与醋”系统（即当$i \leq n$和$j \leq n$时没有$x'_i \cdot x'_j$项）。

特性判明的论证

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

通过将所有$x'_i \cdot x'_j$（$i \leq n$和$j \leq n$）的（A）的全部n个方程中的系数写为零，我们获得(n+v)·n个变量$\alpha_{i,j}(1 \leq i \leq n+v,\ 1 \leq j \leq n)$中的$n \cdot n \cdot \frac{n+1}{2}$个二次方程的系统。因此，当v近似地$\geq \frac{n^2}{2}$时，我们可以期望对于绝大多数（$A$）具有此方程组的解。

附注：

1.上述论证是非常自然的，但这不是一个完整的算术证明。

2.上述方程组可能具有一个解。但求解可能是一个困难的问题。这就是不平衡油与醋方案可能安全的原因（对于良好地选择的参数）：常存在一个变量的线性变换使问题易于解决，但寻找变量的这类变换可能是困难的。

3.在节7中我们将看到，不论这一节的结果如何，但都不推荐选择$v \le n^2$（至少在特征为2时）。

6.解k个未知数的n个二次方程（k>n）组是NP硬的

（见此论文的扩展版本）。

7.用于解n^2个（或更多）未知数的n个二次方程的随机组的普遍（并非经常的）有效算法

在本节中，我们描述一个用于解n+v个变量中n个随机地选择的二次方程组的算法，其中$v \ge n^2$。

设（S）为以下系统:

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

该算法的主要想法在于应用变量的变换，例如:

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

它的$\alpha_{i,j}$系数（对于$1\le i\le n$和$1\le j\le n+v$）是逐步求得的，以使所得方程组（S'）（相对于这些新变量$y_1,\dots,y_{n+v}$写出的）便于求解。

·我们通过随机地选择$\alpha_{1,1},\cdots,\alpha_{1,n+v}$开始。

·然后计算$\alpha_{2,1},\cdots,\alpha_{2,n+v}$以使（$S'$）不包含$y_1y_2$项。此条件导致一个具有(n+v)个未知数$\alpha_{2,j}(1\le j\le n+v)$的n个线性方程组:

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

·再计算$\alpha_{3,1},\cdots,\alpha_{3,n+v}$以使（$S'$）既不包含$y_1y_3$项，又不包含$y_2y_3$项。此条件等效于以下(n+v)个未知数$\alpha_{3,j}(1\le j\le n+v)$的2n个线性方程组:

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

·...

·最后，我们计算$\alpha_{n,1},\cdots,\alpha_{n,n+v}$以使（$S'$）既不包含$y_1y_n$项，也不包含$y_2y_n$项，...，又不包含$y_{n-1}y_n$项。此条件给出以下(n+v)个未知数$\alpha_{n,j}(1\leq j\leq n+v)$的(n-1)n个线性方程组:

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

一般而言，所有这些线性方程提供至少一个解（通过高斯约简求得）。具体地说，此n(n-1)个方程和(n+v)个未知数的最后的组一般给出一个解，只要n+v>n(n-1)，即v>n(n-2)，根据假设这是真的。

此外，对于随机二次组（S），n个向量$\begin{pmatrix}\alpha_{1,1}\\ \cdot\\ \cdot\\ \cdot\\ \alpha_{1,n+v}\end{pmatrix},\ldots,\begin{pmatrix}\alpha_{n,1}\\ \cdot\\ \cdot\\ \cdot\\ \alpha_{n,n+v}\end{pmatrix}$很可能是线性无关的。

剩余的$\alpha_{i,j}$常数（即当n+1≤i≤n+v和1≤j≤n+1时的那些常数）是随机地选择的，以便获得变量的双射变换。

通过相对于这些新变量y_i来重写组（S），我们得到以下方程组:

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

其中每个$L_{i,j}$是一个仿射函数而每个Q_i是一个二次函数。

然后计算$y_{n+1},\ldots,y_{n+v}$以使:

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

这是可能的，因为我们必须解n^2个方程和v个未知数的线性方程组，它通常提供至少一个解，只要$v>n^2$。我们取这些解中的一个。一般而言，这通过高斯约简给出y_i^2。

然后在特征2的情形，由于$x \mapsto x^2$是一个双射，我们将容易地从y_i^2的这个表示式中求得y_i的解。在特征≠2的情形下，当2^n不太大（即当例如n≤40）时，它也能成功。当n大时，基于二次形式的一般理论也存在有求解的方法，由于篇幅所限，此方法可从该论文的扩展版本中寻找。

8.具有两次较小签字的变更

在第2描述的UOV中，公共密钥是一组n个二次方程$y_i=P_i(x_1,...,x_{n+v})$（$1\le i\le n$），其中$y=(y_1,...,y_n)$是拟签字的消息的散列值。如果我们使用一个无碰撞散列函数，则该散列值必须至少为128位长。因此，q^n必须至少为2^{128}以使签字的典型长度（若v=2n）至少为3x128 = 384位。

我们将看到，有可能在签字设计中做小的变更以便获得两次较小的签字。该想法是保持相同多项式P_i（具有相同的相关密钥），但现在我们所检查的公共方程是:

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

其中L_i是$(x_1,...,x_{n+v})$中的一个线性函数且其中L_i的系数由$(y,...,y_n)$中的散列函数生成。

例如，$L_i(y_1,...,y_n,x_1,...,x_{n+v})=\alpha_1x_1+\alpha_2x_2+...+\alpha_{n+v}x_{n+v}$，其中$(\alpha_1,\alpha_2,...,\alpha_{n+v})=Hash(y_1,...,y_n||i)$。现在可以选择n以使$q^n\ge2^{64}$（而不是$q^n\ge2^{128}$）。（请注意：$q^n$必须$\ge2^{64}$以便避免对解x的穷举搜索）。若v=2n及$q^n\cong2^{64}$，则签字的长度将是3x64=192位。

9.三次油与醋

方案

节2中描述的二次油与醋方案容易扩展至任何更高的次数。在3次情形下，对于所有i≤n，隐藏方程组（S）为如下类型:

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

系数γ_{ijk},μ_{ijkl},λ_{ijk},ν_{ijk},ξ_{ij},ξ'_{ij}和δ_i是这些n个方程的秘密系数。注意到这些方程（S）不包含$a_j a_k a_1$项或$a_j a_k$项：当a'_k个未知数是固定时，这些方程是a_j个未知数的仿射变换。

公共密钥的计算，签字的计算和签字的验证如上所述地完成。

当v≤n时3次油与醋的第一加密分析

我们可以注意公共密钥的二次部分并可完全与二次“油与醋”同样地处理它。当v≤n时，预期还能在v≤n时工作。

附注：如果没有二次部分（即公共密钥是3次齐次的），或者如果此处理不成功，则总有可能应用变量的随机仿射变换而再进行尝试。

当$v \le (1+\sqrt{3})n$且K为特征≠2时3次“油与醋”的加密分析（根据D. Coppersmith的设想，见[4]）

关键设想是沿某些方向检测“线性”。我们搜索值$d=(d_1,\ldots,d_{n+v})$的集合V以使：

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

通过写作每个未定元具有一个零系数，我们获得$(n+v)\cdot n$个具有$(n+v)$个未知数的二次方程。

（每个单项式$x_i x_j x_k$给出$(x_j+d_j)(x_k+d_k)(x_l+d_l)+(x_j-d_j)(x_k-d_k)(x_l-d_l)-2x_j x_k x_l$，即$2(x_j d_k d_l + x_k d_j d_l + x_l d_j d_k)$。）

此外，加密分析人员能够规定d的n-1个坐标d_k，因为正确的d的向量空间的维数为n。因此剩下来的是解具有$(v+1)$个未知数d_j的$(n+v)\cdot n$个二次方程。当v不太大时（通常当$\frac{(v+1)^2}{2} \le n(n+v)$时），即当$v \le (1+\sqrt{3})n$时，预期这将是容易的。其结果是，当v近似地≤$(1+\sqrt{3})n$和|K|是奇数时，这就提供简单的方法来破解该方案。

附注1: 当v是敏感地大于$(1+\sqrt{3})n$时（这是比我们在二次情形有过的更为不平衡的极限），现在我们还不知道如何去破解该方案。

附注2: 足够奇怪的是3次“油与醋”方案的这一加密分析对2次油与醋方案不起作用。其原因是在2次中书写出

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

时只给出$(n+v)d_j$个未知数的n个二次方程（我们不知道如何去解）。（每个单项式x_jx_k给出$(x_j+d_j)(x_k+d_k)+(x_j-d_j)(x_k-d_k)-2x_jx_k$，即$2d_jd_k$）

附注3: 在二次情形我们已经看到，当$v \cong \frac{n^2}{2}$时，“不平衡油与醋”公共密钥预期会包括所有的n个二次方程组合。在三次情形中，我们具有类似特性: 当$v \cong \frac{n^3}{6}$时，公共密钥预期会包括几乎所有n个立方方程组（证明类似的）。

10.另一个方案: HFEV

在“最简单”HFE方案中（使用[14]中的记号），我们有b=f(a)，这里:

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

其中F_{q^n}是域β_{ij}, α_i和μ_0的元素。设v为一个整数（v将是附加x_i变量的个数，或者是我们将加入方案中的“醋”变量的个数）。设$a'=(a'_1,...,a'_v)$为K的v重变量。现在设（1）中的各个α_i为F_{q^n}的一个元以使在一个基的α_i的各n个分量中的每一个是醋变量$a'_1,...,a'_v$的秘密随机线性函数。还有在（1）中，现在设μ_0为F_{q^n}的一个元以使一个基中的μ_0的n个分量中的每一个是变量$a'_1,...,a'_v$的秘密随机二次函数。然后，n+v个变量$a_1,...,a_n,a'_1,...,a'_v$将与秘密仿射双射S混合以获得变量$x_1,...,x_{n+v}$。还有，如同以前一样，$t(b_1,...,b_n)=(y_1,...,y_n)$，其中t是一个秘密仿射双射函数。然后公共密钥给定为n个方程$y_i=P_i(x_1,...,x_{n+v})$。为计算签字，只需简单随机地选择醋变量$a'_1,...,a'_v$。这时，计算μ_0和α_i的值。然后解出F_{q^n}中（a）的单变量方程（1）。

例子: 设$K=F_2$。在HFEV中，例如使隐藏多项式为:

$$f(a)=a^{17}+\beta_{16}a^{16}+a^{12}+a^{10}+a^{9}+\beta_{8}a^{8}+a^{6}+a^{5}+\beta_{4}a^{4}+a^{3}+\beta_{2}a^{2}+\beta_{1}a+\beta_{0},$$

其中$a=(a_1,...,a_n)$（$a_1,...,a_n$是“油”变量），$\beta_1, \beta_2, \beta_4, \beta_8$和$\beta_{16}$由v个醋变量的n个秘密线性函数给出而$\beta_0$由v个醋变量的n个秘密二次函数给出。在此例中，我们如下地计算一个签字：随机地选择醋变量而解出a的17次方程。

附注：与UOV不同，在HFEV中我们具有油x油项（例如a^{17}、a^{12}、a^{10}等），油x醋项（例如$\beta_{16}a^{16}, \beta_8a^8$等）以及醋x醋项（在$\beta_0$中）。

模拟

Nicolas Courtois在HFEV上做了某些模拟，而在他的所有模拟中，当醋变量的数量≥3时，不存在多个小次数的仿射方程（这是很好的）。更详细的知识参看此论文的扩展版本。

11.UOV参数的具体例子

当前似有可能选择例如n=64，v=128（或v=192）和$K=F_2$。签字方案是节8中的一部分，这一情形下的签字长度只是192位（或256位）。此论文的扩展版本中有更多的可能参数的例子。

附注：如果我们选择$K=F_2$，则公共密钥通常太大。因此通常更为实际的是选择较大的K和较小的n：然后可显著地减小公共密钥的长度。然而，即使当K和n是固定时，也始终可能对公共密钥作某些容易的变换以便用正则方式获得公共密钥从而使此正则表示式稍短于原始表示式。详情参考此论文的扩展版本。

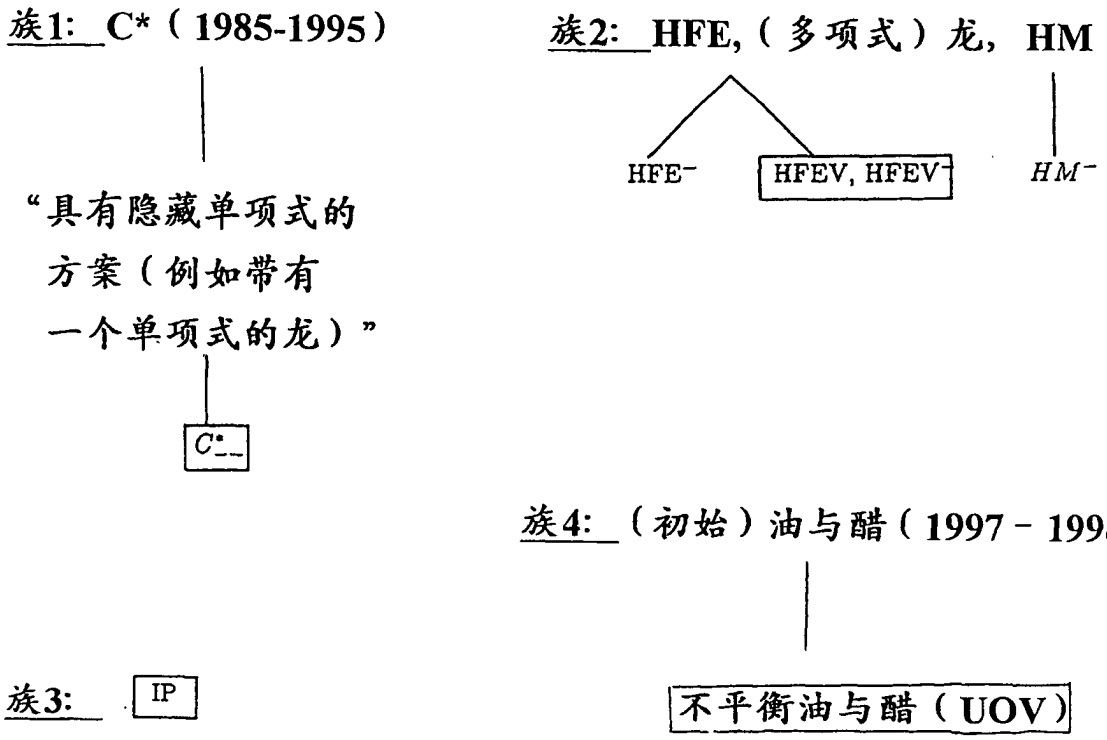
12.HFEV参数的具体例子

当前似有可能选择小的v值（例如v=3）和小的d值（例如n=77，v=3，d=33和$K=F_2$）。此论文的扩展版本中描述了签字方案（为避免生日方块悖论）。此处签字长度只是80位！此论文的扩展版本中有更多可能参数的例子。

13.有关小有限域内多变量多项式的公共密钥方案的当前技术发展水平（1999年5月）

新近来引进了许多新想法用于设计更好的方案，例如本论文的UOV或HFEV。另一个想法是固定某些变量以隐藏某些代数特性，还有一个想法是引入少数真正的随机二次方程和将它们与初始方程混合：见本论文的扩展版本。然而，许多新想法业已引入来设计对先前方案作更好处理，例如尚未发表的论文[1],[2],[3],[5]。因此此领域发展很快而初看起来有点混乱。此外，某些作者对于“破解”使用“加密分析”一词而某些作者则使用含意为“关于安全性的分析”来表达此词，而它不一定意味着“破解”。在本节中，我们描述当前所知道的关于主方案的内容。

在基于小有限域上多变量多项式的公共密钥的大族中，我们可以区别五个主族之间的不同，它们的特征在于引入秘密信息的方式或者在于安全性所依赖的困难问题。在第一族中是“带有隐藏单项式”的方案，即关键想法是在有限域内为密钥计算来计算一个取幂$x \rightarrow x^d$。在第二族的方案中是将多项式函数（具有多于一个单项式）隐藏。在第三族的方案中，安全性依赖于同构性问题。在第四族中，安全性依赖于从两个多变量二次多项式的合成的全部或一部分中难以求得它们的分解结果。最后，在第五族中，密钥计算基于高斯计算。这几个族中的主方案描述于以下图中。每个族中最感兴趣的方案是在一个矩形块中。



C*曾是所有方案中的第一个，而它可以看作所有这些方案的始祖。它是在[12]中设计和在[13]中破解的。

•带有隐藏单项式的方案（例如某些龙方案）已在[15]中研究过，其中已证明它们中极大部分不安全。然而，C*--（在[20]中研究过）是（当今）智能卡中最有效的签字方案（在时间上和RAM使用上）。该方案没有破解（但在其安全性上具有大的可信度方面，它可能似乎太简单或者太接近C*）。

•HFE在[14]中设计。关于其安全性的最近结果包括在[1]和[2]中。在这些论文中，描述了很聪明的处理。然而，当今似乎该方案尚未被破解，因为对于很好地选择的和仍然合理的参数而言，需要处理它的

计算量仍然很大。例如，在[14]中给出的500美元的第一挑战尚未提出权利要求（它是纯HFE，在F_2上具有n=80和d=96）。

•HFE^-是这样一个其中某些公共方程尚未发表的HFE。由于[1]和[2]，它可能推荐来做此事（虽然初始HFE不用它也可能是安全的）。在[14]的扩展版本中描述了关于HFE^-的500美元的第二挑战。

•HFEV描述于本论文中。HFEV和$HFEV^-$看来很难破解。此外，HFEV比初始HFE更为有效，而它能给出只有80位的公共密钥签字！

•HM和HM^-设计于[20]中。在这些方案中只作了很少分析（但可能我们能推荐使用HM^-而不是HM？）

•IP设计于[14]中。迄今为止，IP方案证明对安全性具有最好的保证（见[19]）。IP非常简单并能看作图形同构的很好推广。

•初始“油与醋”是在[16]中提出并且在[10]中破解的。

•UOV描述于本论文中。与IP一起，它们肯定是最简单的方案。

•2R设计于[17]和[18]中。由于[3]，输入中至少必须有128位，而由于[5]，不发表所有（初始）公共方程可能是明智的：这给出了$2R^-$算法（在[5]中给出的对2R方案的分解算法其效率尚不完全清楚）。

附注1：上述这些方案在理论上是令人感兴趣的，但（除IP以外）它们的安全性却不直接依赖于清晰定义的内容因而被认为是困难的问题。为此，将它们实施于实际产品中是否合理？我们认为，在种种敏感性应用中将整个安全性建筑于这类方案之上确实有点冒险。然而，当今大部分智能卡的应用都使用密钥算法（例如三重DES），这是因为RSA智能卡更为昂贵。因此在现有密钥方案之外（而不是替代）再加上以前公共密钥方案中一个低费用智能卡方案是合理的。如此可以增加安全性，但智能卡的费用仍然是低的（不需要协处理器）。安全性然后将依赖于密钥算法的主密钥（存在一些依赖于主密钥的风险）并依赖于新的低费用公共密钥方案（存在着该方案尚没有安全性证明的风险）。还可注意到，当要求极短签字长度时（或短块加密时），实际上没有选择：当今只有多变量方案能够有64至256位之间的长度。

附注2: 当发现新方案具有多变量多项式时，我们不必要解释如何已引进秘密信息。然后我们将获得一种“公共密钥方案”。该方案明显地是一个公共密钥方案，因为任何人能够从公共密钥中证实一个签字（或者能够根据公共密钥进行加密），同时该方案是秘密的，这是由于进行密钥计算的方法（即引进秘密信息的方法）尚未披露而无法从公共密钥中来猜测。例如，我们可能已为HFEV做到此点（而不是发表它）。

14.结论

本文中我们已经提出两个带有“醋变量”的公共密钥方案: UOV和HFEV。这些方案的研究已经引导我们来对一般二次形式系统的解的一般特性进行分析。此外，从节13中提出的一般观点来看，我们发现这两个方案是当今在基于小有限域中多变量多项式的方案的五个族中最令人感兴趣的两个。但它们在今后数年内还仍然会是正确的吗？

参考文献

[1]Anonymous,*公共密钥加密系统HFE的加密分析*，尚未发表。

[2]Anonymous,*隐藏域方程（HFE）的实际加密分析*，尚未发表。

[3]Anonymous,*带有S盒的Patarin的2回转公共密钥系统的加密分析*，尚未发表。

[4]D. coppersmith，*个人通信*，电子邮件。

[5]Z. Dai, D. Ye, K.- Y. Lam，*基于映射合成的非对称密码学的因子分解处理*，尚未发表。

[6]J. C. Faugere，*个人通信*。

[7]H. Fell, W. Diffie，*基于多项式置换的公共密钥方案的分析*，Proceedings of CRYPTO'85, Springer-Verlag, vol. 218, pp.340-349.

[8]M. Garey, D. Johnson，*计算机及无多项式算法的可能性，NP完全性理论入门*，Freeman,p.251.

[9]H. Imai, T. Matsumoto，*构造不对称加密系统的代数方法*，Algebraic Algorithms and Error Correcting Codes(AAECC-3), Grenoble, 1985, Springer-Verlag, LNCS no.229.

[10]A. Kipnis, A. Shamir, *油与醋签字方案的加密分析*, Proceedings of CRYPTO'98, Springer, LNCS no. 1462,pp.257-266.

[11]R. Lidi, H. Niederreiter, *有限域*, Encyclopedia of Mathematics and its applications, volume20, Cambridge University Press.

[12]T. Matsumoto, H. Imai, *有效的签字证实和消息加密的公共二次多项式组*, Proceedings of EUROCRYPT'88, Springer-Verlag, pp. 419-453.

[13]Jacques Patarin, *Eurocrypt'88的Matsumoto和Imai公共密钥方案的加密分析*, Proceedings of CRYPTO'95, Springer-Verlag, pp. 248-261.

[14]J. Patarin, *隐藏域方程（HFE）和多项式的同构性（IP）：不对称算法的两个新族*, Proceedings of EUROCRYPT'96, Springer, pp. 33-48.

[15]Jacques Patarin, *具有隐藏单项式的不对称密码学*, Proceedings of CRYPTO'96, Springer, pp. 45-60.

[16]J. Patarin, *油与醋签字方案*, 提交于Datstudl Workshop on Cryptography, 1997年9月（透明软片）。

[17]J. Patarin, *秘密信息单向排列和多变量多项式*, Proceedings of ICICS'97, Springer, LNCS no.1334, pp. 356-368.

[18]J. Patarin, L. Goubin, *具有S盒的不对称密码学*, Proceedings of ICICS'97, Springer, LNCS no. 1334, pp. 360-380.

[19]J. Patarin, L. Goubin, N. Courtois, *多项式同构性的改进算法*, Proceedings of EUROCRYPT'98, Springer, pp. 184-200.

[20]J. Patarin, L. Goubin, N. Courtois, C^*_{-+}和HM: *有关T. Matsumoto和H. Imai方案的变动*, Proceedings of ASIACRYPT'98, Springer, pp.35-49.

[21]A. Shamir, *由D. Coppersmith和J. Stern发现的简单加密方案及其加密分析*, 宣读于Luminy Workshop on Cryptography, 1995年9月。

图 1

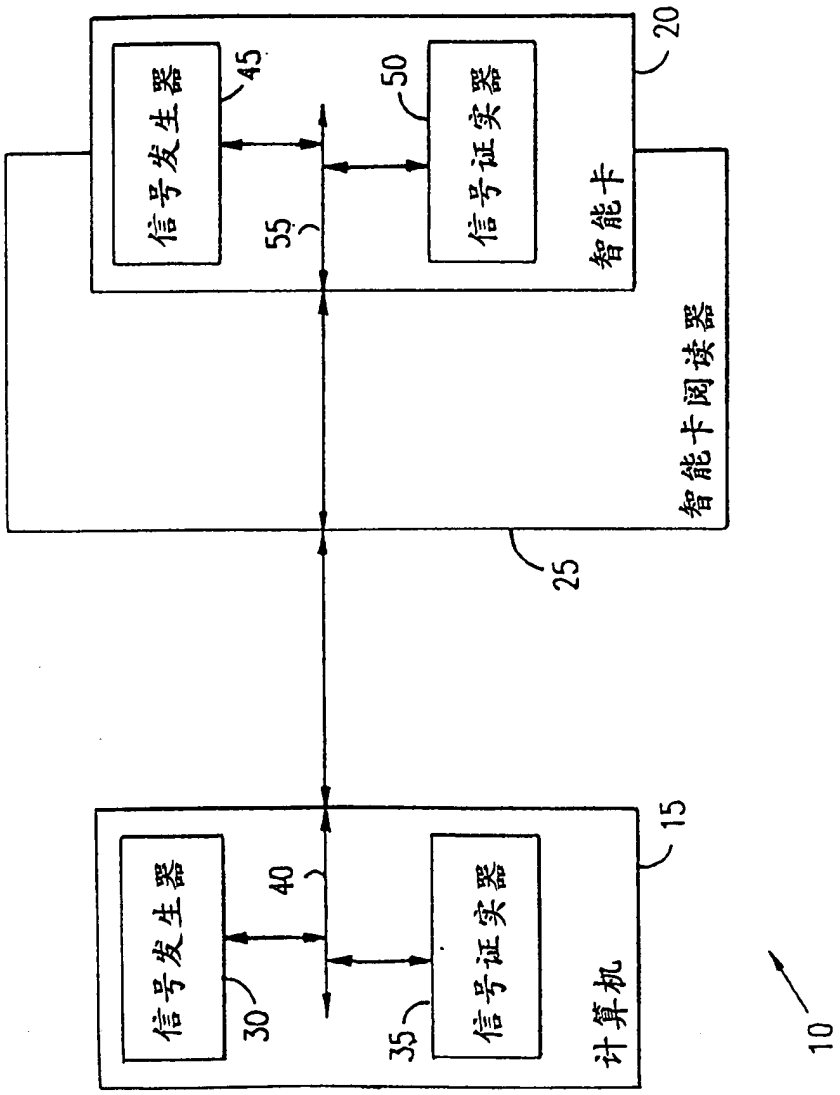

信号发生器
45
50
信号证实器
20
智能卡
55
智能卡阅读器
25
信号发生器
40
信号证实器
30
35
计算机
15
10

图 2A

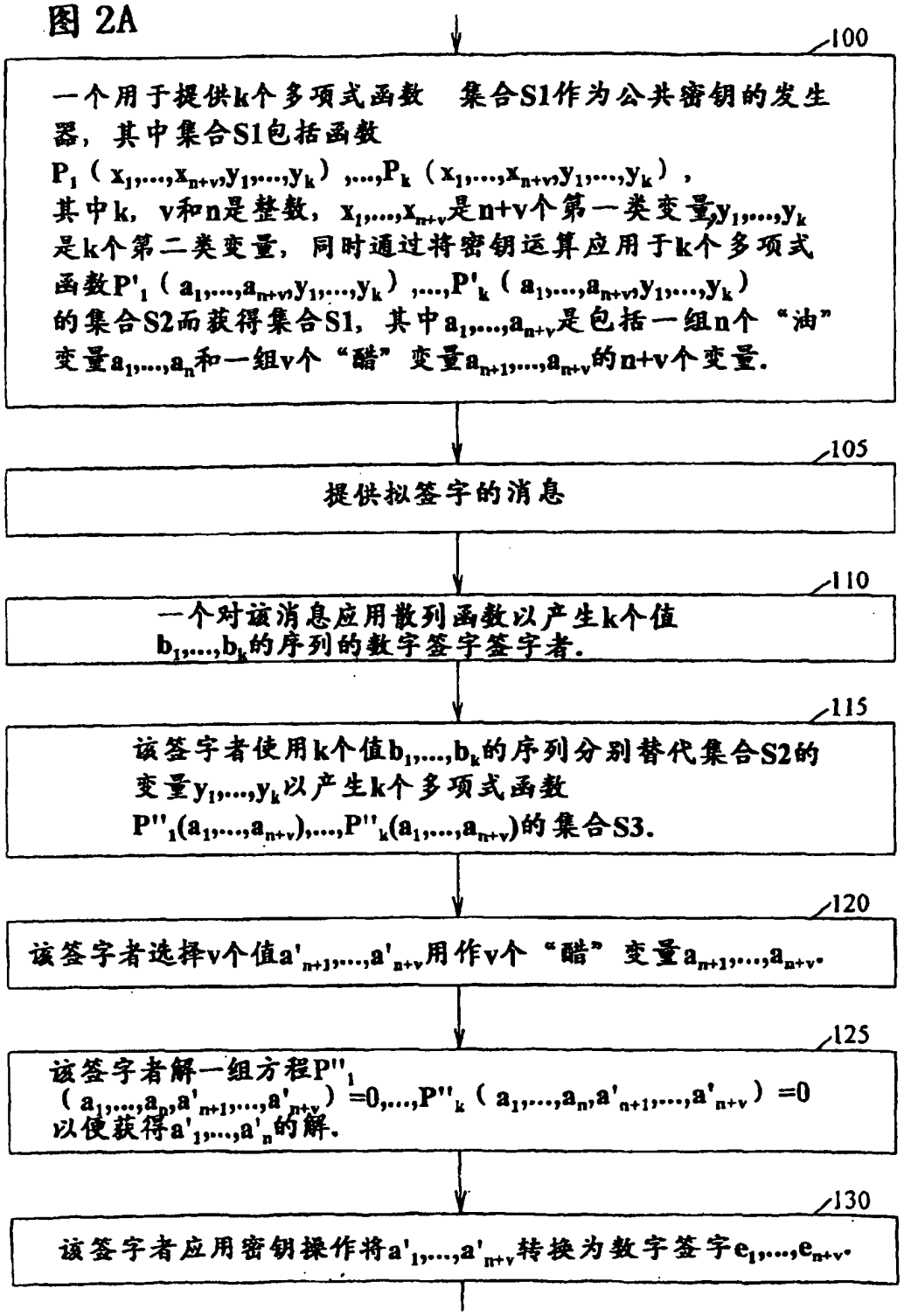
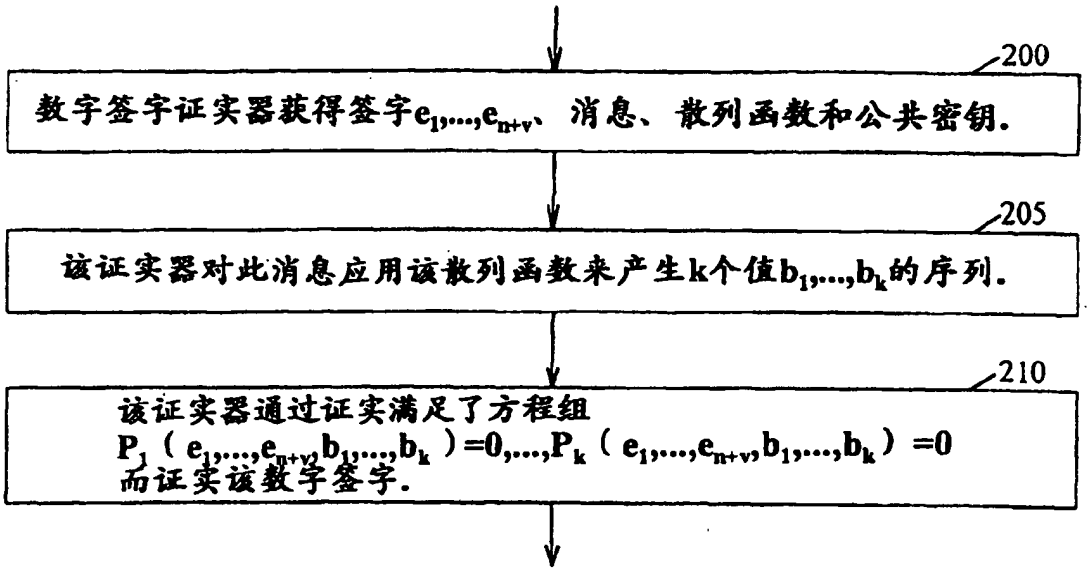

100
一个用于提供k个多项式函数 集合S1作为公共密钥的发生器，其中集合S1包括函数 $P_1(x_1,\ldots,x_{n+v},y_1,\ldots,y_k),\ldots,P_k(x_1,\ldots,x_{n+v},y_1,\ldots,y_k)$，其中k，v和n是整数，$x_1,\ldots,x_{n+v}$是n+v个第一类变量，$y_1,\ldots,y_k$是k个第二类变量，同时通过将密钥运算应用于k个多项式函数$P'_1(a_1,\ldots,a_{n+v},y_1,\ldots,y_k),\ldots,P'_k(a_1,\ldots,a_{n+v},y_1,\ldots,y_k)$的集合S2而获得集合S1，其中$a_1,\ldots,a_{n+v}$是包括一组n个“油”变量$a_1,\ldots,a_n$和一组v个“醋”变量$a_{n+1},\ldots,a_{n+v}$的n+v个变量。
105
提供拟签字的消息
110
一个对该消息应用散列函数以产生k个值$b_1,\ldots,b_k$的序列的数字签字签字者。
115
该签字者使用k个值$b_1,\ldots,b_k$的序列分别替代集合S2的变量$y_1,\ldots,y_k$以产生k个多项式函数$P''_1(a_1,\ldots,a_{n+v}),\ldots,P''_k(a_1,\ldots,a_{n+v})$的集合S3。
120
该签字者选择v个值$a'_{n+1},\ldots,a'_{n+v}$用作v个“醋”变量$a_{n+1},\ldots,a_{n+v}$。
125
该签字者解一组方程$P''_1(a_1,\ldots,a_n,a'_{n+1},\ldots,a'_{n+v})=0,\ldots,P''_k(a_1,\ldots,a_n,a'_{n+1},\ldots,a'_{n+v})=0$以使获得$a'_1,\ldots,a'_n$的解。
130
该签字者应用密钥操作将$a'_1,\ldots,a'_{n+v}$转换为数字签字$e_1,\ldots,e_{n+v}$。

图 2B


200
数字签字证实器获得签字$e_1,...,e_{n+v}$、消息、散列函数和公共密钥。
205
该证实器对此消息应用该散列函数来产生k个值$b_1,...,b_k$的序列。
210
该证实器通过证实满足了方程组
$P_1(e_1,...,e_{n+v},b_1,...,b_k)=0,...,P_k(e_1,...,e_{n+v},b_1,...,b_k)=0$
而证实该数字签字。