(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101099329 B
(45)授权公告日 2012.12.26

(21)申请号 200580046426.X
(22)申请日 2005.11.14
(30)优先权数据
60/626,884 2004.11.12 US
PCT/IB2004/003700 2004.11.11 WO
(85)PCT申请进入国家阶段日
2007.07.11
(86)PCT申请的申请数据
PCT/CA2005/001720 2005.11.14
(87)PCT申请的公布数据
WO2006/050605 EN 2006.05.18
(73)专利权人 塞尔蒂卡姆公司
地址 加拿大安大略省
(72)发明人 斯科特·A.·万斯通
罗伯特·P.·加朗特
丹尼尔·R.·L.·布朗
马里纳斯·斯特罗伊克
(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 王波波
(51)Int.Cl.
H04L 9/30(2006.01)
(56)对比文件
US 5751808 A,1998.05.12, 全文.
US 5146500 A,1992.09.08, 全文.
WO 01/01625 A1, 全文.
平昭.椭圆曲线公钥密码体制研究与应用.电子科技大学硕士论文.2003,24-31.
审查员 高静

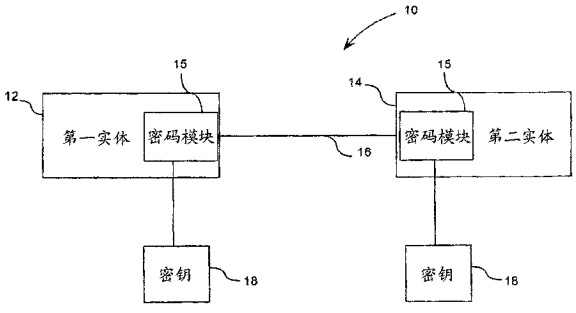
权利要求书 2 页 说明书 8 页 附图 4 页

(54)发明名称

基于椭圆曲线的新陷门单向函数及其用于较短签名和非对称加密的应用

(57)摘要

本发明提供一种新的陷门单向函数。通常,使用某二次代数整数 z。接着可以找到曲线 E 和在 E 上定义 [z] 的有理映射。该有理映射 [z] 是陷门单向函数。z 的明智选择将确保:可有效计算 [z],难以反演 [z],从由 [z] 定义的有理函数难以确定 z,以及对 z 的了解使得可以基于某组椭圆曲线点反演 [z]。每一有理映射是平移和自同态的组合,因为平移易于反演,有理映射最安全的部分是自同态。如果反演自同态从而 [z] 的问题与 E 中离散对数问题一样难,那么密码群的大小可以小于用于 RSA 陷门单向函数的群。



CN 101099329 B

1. 在 n 阶椭圆曲线 E 上运算的密码系统，所述密码系统包括对针对第二通信端的数据进行密码处理的第一通信端，所述第一通信端包括第一密码模块，所述第一密码模块：

具有与二次代数整数 z 相应的基于群的自同态 [z]，所述二次代数整数 z 满足 $z^2+uz+v = 0$，其中 u 和 v 是秘密整数，并且 v 与 n 是互质数，所述密码模块被配置为：

将所述自同态 [z] 标识为公钥运算；

确定私钥运算 [-w]([u]+[z])，其中 w 是整数，$wv = 1 \mod n$，[-w] 是对应于 -w 的自同态，[u] 是对应于 u 的自同态；

获得要进行密码处理的数据 x；

对所述数据 x 应用所述公钥运算和所述私钥运算之一，从而得到修改的数据 x′；以及

将所述修改的数据 x′ 提供给所述密码系统中的所述第二通信端，以使所述第二通信端处的第二密码模块能够使用所述公钥运算和所述私钥运算中的另一个来对所述修改的数据 x′ 进行互补密码运算。

2. 根据权利要求 1 所述的密码系统，其特征在于，所述整数 z 是具有实部和虚部的复数。

3. 根据权利要求 1 所述的密码系统，其特征在于，所述自同态 [z] 表现为有理映射。

4. 根据权利要求 1 所述的密码系统，其特征在于，所述密码数据 x 包括消息 m，所述第一密码模块进行的所述公钥运算对所述消息 m 进行加密从而得到加密消息 m′，以及所述第二密码模块应用的所述私钥运算对所述加密消息 m′ 进行解密从而得到所述消息 m。

5. 根据权利要求 1 所述的密码系统，其特征在于，所述修改的数据 x′ 包括要签名的消息 m，所述第一密码模块对所述消息 m 应用所述私钥运算从而得到签名 s，以及所述互补运算包括对所述签名 s 的所述公钥运算从而认证所述签名。

6. 根据权利要求 5 所述的密码系统，其特征在于，所述消息 m 由所述第二通信端应用于原始消息 M 的散列函数生成。

7. 根据权利要求 1 所述的密码系统，其特征在于，所述密码数据 x 包括多个消息，以便接收所述第一通信端的签名，所述第一通信端对所述多个消息的组合应用所述私钥运算从而得到所述签名，以及由所述第二通信端使用所述公钥运算，从而认证所述签名，并由此认证所述多个消息的每一个消息。

8. 用于密码系统中的第一通信端对针对第二通信端的数据进行密码处理的方法，所述密码系统在 n 阶椭圆曲线 E 上运算，所述第一通信端具有与二次代数整数 z 相应的基于群的自同态 [z]，所述二次代数整数 z 满足 $z^2+uz+v = 0$，其中 u 和 v 是秘密整数，并且 v 与 n 是互质数，所述方法包括以下步骤：

将所述自同态 [z] 标识为公钥运算；

确定私钥运算 [-w]([u]+[z])，其中 w 是整数，$wv = 1 \mod n$，[-w] 是对应于 -w 的自同态，[u] 是对应于 u 的自同态；

获得要进行密码处理的数据 x；

对所述数据 x 应用所述公钥运算和所述私钥运算之一，从而得到修改的数据 x′；以及

将所述修改的数据 x′ 提供给所述密码系统中的所述第二通信端，以使所述第二通信端能够使用所述公钥运算和所述私钥运算中的另一个来对所述修改的数据 x′ 进行互补密码运算。

9. 根据权利要求 8 所述的方法，其特征在于，所述整数 z 是具有实部和虚部的复数。

10. 根据权利要求 8 所述的方法，其特征在于，所述自同态 [z] 表现为有理映射。

11. 根据权利要求 8 所述的方法，其特征在于，所述密码数据 x 包括消息 m，应用所述公钥运算对所述消息 m 加密从而得到加密消息 m′ ，以及所述第二密码模块应用所述私钥运算从所述加密消息 m′ 中解密出所述消息 m。

12. 根据权利要求 8 所述的方法，其特征在于，所述修改的数据 x′ 包括要签名的消息 m ；所述方法包括应用所述私钥运算对所述消息 m 运算从而得到签名 s，以及所述互补运算包括对所述签名 s 的所述公钥运算从而认证所述签名 s。

13. 根据权利要求 12 所述的方法，其特征在于，所述消息 m 由所述第二通信端应用于原始消息 M 的散列函数生成。

14. 根据权利要求 8 所述的方法，其特征在于，所述密码数据 x 包括多个消息，以便接收签名，所述私钥运算对所述多个消息的组合运算从而得到所述签名，以及所述公钥运算对所述签名运算从而认证所述签名，并由此认证所述多个消息的每一个消息。

15. 根据权利要求 8 所述的方法，其特征在于，所述数据 x 包括将由多个签名者签名的消息，所述私钥运算包括对应于所述多个签名者中的每一个的多个运算，对所述消息连续应用所述多个运算从而得到签名，所述公钥运算包括对应于所述多个签名者中的每一个的多个对应运算，按相反的顺序对与所述多个签名者中的每一个相对应的所述多个运算连续应用所述多个对应运算，从而认证所述签名。

基于椭圆曲线的新陷门单向函数及其用于较短签名和非对称加密的应用

技术领域

[0001] 本发明涉及陷门单向加密函数以及利用此类函数的密码系统。

背景技术

[0002] 陷门单向函数(TOWF)是公开可计算函数,仅一个实体可对其反演(invert)。需要称为私钥的专用密码来计算TOWF的逆(inverse)。

[0003] TOWF的经典实例是基于$M^{ed} \equiv M(\mathrm{mod}\ N)$这一关系的RSA函数。公共RSA函数w计算如下:$W(x) = x^e \mod N$。数字e和N是公共值。选择数字N为两个加密的不同质数p和q的积。用私钥运算w反演RSA函数,可计算如下:$W^{-1}(y) = y^d \mod N$,其中$d = (1/e) \mod (p-1)(q-1)$并为私钥。

[0004] 无私钥而反演RSA函数被认为是难题。对于大值的N来说,对N因式分解得到质数p、q是计算上不可实行的,而因此私钥$w = (p-1)(q-1)$也保持秘密。实际中,当前所作的许多在线银行业务的安全性依赖于无私钥则难以反演的RSA函数。换句话说,人们通常认为RSA是TOWF。

[0005] 作为TOWF,RSA函数可用作执行数字签名和公钥加密的密码系统的基础。为了用陷门单向函数W对消息M数字签名,需要利用私钥运算W^{-1}和公共散列函数H计算$S = W^{-1}(H(M))$。散列函数有两个用途:将M压缩到W^{-1}可处理的摘要(digest)大小,以及防止一些潜在攻击,这些潜在攻击涉及从一条消息签名向相关的但未授权的消息的转换。为了用陷门单向函数检验消息M的签名S,需要核查$H(M) = W(S)$。

[0006] 用TOWF进行公钥加密有点与签名相反。不进行散列,而使用编码方案E。为了对消息M加密,需要计算密码$C = W(E(M))$。为了对密码C解密,需要计算$M = E^{-1}(W^{-1}(C))$。编码函数用于使M适合应用于W所需的大小,并且防止某些种类相关消息的攻击。

[0007] 一种可选的密码系统针对离散对数问题的难点而建立。将安全性建立在离散对数问题的基础上的特别牢固的密码系统利用椭圆曲线,并且与RSA TOWF密码系统相比具有减小的带宽的优势。

[0008] 尽管与RSA TOWF密码系统相比椭圆曲线密码系统减小带宽,其在保持现有系统的理想属性的同时仍需要使带宽最小化。而且TOWF不依赖随机数发生器,因此即使所需带宽较大,在某些环境下更易于执行。

[0009] 因此本发明的目的是提供一种TOWF密码系统来消除或减轻上述的缺点。

[0010] 为了便于理解本发明的基本原理,下面回顾一下这些原理的数学基础。

[0011] 椭圆曲线E是满足椭圆曲线定义方程的点(x,y)的集合。定义方程对y是二次方的和对x是三次方的,并且是非奇异的。坐标x和y是域的元素,是可被加、减、乘和除(0除外)的一组元素。域的例子包括有理数和实数。还有有限域,它们是密码系统中最常用的域。有限域的例子是以质数q为模的整数集。

[0012] 不失一般性,椭圆曲线的定义方程可为Weierstrass形式。当域F取自以质数q

> 3 为模的整数时，那么 Weierstrass 方程采取这种形式 $y^2 = x^3+ax+b$，其中 a 和 b 是域 F 的元素。

[0013] 椭圆曲线 E 包括点 (x, y) 和另一点即无穷点 (point at infinity)O，其中点 (x, y) 是定义方程的所有解。椭圆曲线 E 还有群结构，意指在曲线上的两个点 P 和 Q 可做加法而形成第三点 P+Q。点 O 是群的恒等式，意指对所有的点 P，有 P+O = O+P = P。加法是结合的，因此 P+(Q+R) = (P+Q)+R，并且是可交换的，因此对所有的点 P、Q 和 R，有 P+Q = Q+R。每一点 P 有负点 -P，使得 P+(-P) = O。当曲线方程是 $y^2 = x^3+ax+b$ 形式的 Weierstrass 方程时，P = (x, y) 的负点很容易确定为 -P = (x, -y)。根据坐标对点 P 和 Q 做加法的公式只适度复杂，只涉及少量定义 E 的域中的域运算。

[0014] 域上二变量有理函数 r(x,y) 是相同域上的两个二变量多项式的比。因此 r(x,y) = p(x,y)/q(x,y)，其中 p 和 q 是 x 和 y 的多项式。x 和 y 的多项式是 ax^my^n 形式的项的和，其中 a 是域元素 (可能取决于 m 和 n)，而 m 和 n 非负整数。例如，x^2y-3y^4+1 是 x 和 y 的多项式。对于任意有理函数 r(x,y) 和域元素 u 和 v，在点 (u,v) 有有理函数数 r(x,y) 的值。该值是域元素或无穷点，并写为 r(u,v)。仅通过用域元素 u 代换每次出现的变量 x，用 v 代换每一 y，并而后计算所有的域运算，例如乘法、加法和除法。有时候除以 0 的结果通常表示值 r(u,v) 实际上是无穷的，因为该值不在域中而认为是例外。因此对于曲线上的点 (x,y) 计算 r(x, y) 是可能的。在点 O 定义 r(x, y) 的值也是可能的，这样能够计算关于曲线的每一点的 r。

[0015] 椭圆曲线 E 上的有理映射是一对有理函数 r(x,y) 和 s(x,y)，使得如果 (u,v) 是 E 上的点，那么 (t, w) = (r(u, v), s(u, v)) 也是 E 上的点。更一般而言，如果 (u, v) 由 O 取代，而且如果 (t, w) 为 O 是可接受的，这对应于 t 和 w 都是无穷大，那么这种情况还需保持成立。

[0016] 就像曲线上的点一样，椭圆曲线上的有理映射实际上可做加法。除了不用域元素做运算，而用有理函数即用 x 和 y 的符号函数做运算之外，加法规则相同。

[0017] 作为 E 的有理函数，如果 r 等于 r′ 并且 s 等于 s′ ，则 E 上的有理映射 (r, s) 等于另一个有理映射 (r′ , s′)。

[0018] 特定类的有理映射是自同态。自同态 e 是具有加法特性的有理映射 e = (r, s)，即对于任意两个点 P 和 Q，有 e(P+Q) = e(P)+e(Q)。椭圆曲线理论中一个重要的定理表示，如果 e 是具有这种特性 e(O) = O 的有理映射，那么 e 也是自同态。这个定理大大简化了对给定有理映射是否是自同态的确定。

[0019] 自同态的重要例子是 e = [m]，由 e(P) = mP 定义，即 m 个点 P 的和。因为曲线 E 的加法法则由有理函数定义，那么 m 个 P 的迭代和 mP 也是如此，因为这些有理函数可以迭代。因而 e(P) 是有理映射。因为关于曲线 E 的加法运算是结合的，对于 e = [m]，有 e(P+Q) = m(P+Q) = m(P)+m(Q) = e(P)+e(Q)。因而，因为 e 有加法特性，所以 e 是自同态。

[0020] 如果有不同于 [m] 的自同态，那么说 E 有复数乘法。有限域上定义的椭圆曲线总有复数乘法。换句话说，对于所有的整数 m，这些椭圆曲线总有不同于 [m] 的自同态 e。

[0021] 椭圆曲线理论的有效的定理表示，任何自同态 e 相当于 (r(x),cyr′ (x)) 形式的唯一映射，其中 r(x) 是单个变量的有理函数，c 是常量域元素，而 r′ (x) 是 r(x) 导数。这个结果根本不明显，但是如果 e 是 (f(x, y), g(x, y)) 形式，那么如下所述，不难确定 r(x)。

[0022] 为了举例说明，用线性或 y 的常量多项式代换 f(x,y) 中每次出现的 y^2。例如，如果该曲线的定义方程是 $y^2 = x^3+ax+b$ 那么 y^2 可由 x^3+ax+b 代换，其为 y 的常量。按需要这样运用多次，使得分子和分母中的 y 没有任何高于 1 的幂，换句话说，它们对 y 是线性的。修改的 f(x,y) 具有 (a(x)+b(x)y)/(c(x)+d(x)y) 这个形式，其中 a、b、c 和 d 是多项式函数，不与前面使用的这些变量混淆。通过用 (c(x)-d(x)y) 乘上端和下端可从分母中消去 y，得出下端中 $c(x)^2-d(x)^2\ y^2 = c(x)^2-d(x)^2(x^3+ax+b)$。分子中的 y^2 也可消去。这样给出一种形式 g(x)+h(x)y，其中 g(x) 和 h(x) 是 x 的有理函数。因为当 e 是自同态时有 e(-P) = -e(P)，因而对于曲线上的所有 (x,y)，e(x,-y) = -e(x,y)，因此 g(x)+h(x)y = g(x)-h(x)y，可证明 h(x) = 0。因此现在我们得到 r(x) 为 g(x)。显然用这种方法得到的 r(x) 是唯一的。

[0023] 同样地，有理函数 g(x, y) 可表示为线性函数 h(x)+yk(x)，其中 h(x) 和 k(x) 是 x 的有理函数，而通过相同的理由可显示 h(x) = 0。这样意味着可确定 k(x)，其提供一种得到 (r(x), cyr′ (x)) 形式中的常量 c 方法。可选地，c 可由对 r(x) 微分得到，并而后在某点 P 计算 e 而解出 c。

[0024] 每一自同态对椭圆曲线群有一作用，该椭圆曲线群对应于二次代数整数。二次代数整数 z 是复数，使得对于某整数 u 和 v，有 $z^2+uz+v = 0$。如果 $e^2+[u]z+[v] = [0]$，那么自同态 e 对应于该代数整数，其中如上所述，此处的加法是有理映射的相加。这时，我们可写 e = [z]，其中 [] 表示对应于有理整数的有理映射。

[0025] 所有实数整数是二次代数整数，而自同态 [m] 对应于整数 m。不是实数整数的二次代数整数是复数 i，-1 的平方根，其满足二次方程 $i^2+1 = 0$。对于每一不是实数整数的二次代数整数，只有有限的具有自同态 [z] 的椭圆曲线。已知的结果给出确定这类曲线的理论程序，以及确定 [z] 为有理映射的方法。

[0026] 通常，自同态 e 的次数是点 P 的数量，使得 e(P) = 0。更确切地，这称为 e 的可分离次数。实际次数是可分次数和其他某些称为不可分次数的积。当 e 表示为其标准形式 (r(x), cyr′ (x)) 时，r(x) 的分子的次数是 e 的次数，而 r(x) 的分母的次数少 1 次。（这里我们假设 r(x) 的分子和分母是互质的）而且，对于 e = [z]，通常有 e 的次数为 $|z|^2$。例如，自同态 [m] 的次数因此为 $|m|^2 = m^2$。

[0027] 在传统椭圆曲线密码系统中，经常计算自同态 [m]。数 m 代表私钥，而 [m]P = mP 代表公钥。即使对于大 m 值，可有效计算函数 [m]，比对出现在 [m] 的 r(x) 的分子和分母的完全展开多项式形式中的 m^2 项求和快得多。此处关键的结果是可有效计算高次数的自同态。

[0028] 下面例子列出了任意椭圆曲线上的每一可能的 2 次自同态。该列表完全等效于有理映射和椭圆曲线。这些选自 Silverman 的算术椭圆曲线高等概论 (Silverman)。

[0029] 首先是 e = [z] = [1+i]，定义在曲线 E 上：

[0030] $y^2 = x^3+x$，则：$$e(x,y)=\left(\frac{x^2+1}{z^2x},\frac{y(x^2-1)}{z^3x^2}\right)$$

[0031] 注意 z 作为定义 e 的作用的有理函数出现，因此当 E 定义在含有对应于 z 的值的域 F 上时，仅定义 e。（该注解也适用下面的两个自同态 e）

[0032] 第二是 e = [z] = [√ (-2)]，定义在 E 上：

[0033] $y^2 = x^3+4x^2+2x$，则 $e(x,y)=\left(\frac{x^2+4x+2}{z^2x},\frac{y(x^2-2)}{z^3x^2}\right)$

[0034] 第三是 e = [z] = [(1+ √ (-7))/2]，定义在 E 上：

[0035] $y^2 = x^3-35x+98$，则：

[0036] $$e(x,y)=\left(\frac{x^2+x(z^2-2)-7(1-z)^4}{z^2(x+z^2-2)},\frac{y((x+z^2-2)^2+7(1-z)^4)}{z^3(x+z^2-2)^2}\right)$$

发明内容

[0037] 发明人公认可使用椭圆密码系统的属性获得 TOWF，该 TOWF 提供有着减小的宽带的牢固的密码系统。

[0038] 一方面，本发明提供一种在 n 阶椭圆曲线 E 上运算的密码系统。该密码系统具有与二次代数整数 z 相应的自同态 [z]，该二次代数整数 z 满足 $z^2+uz+v = 0$，其中 u 和 v 是秘密整数，并且 v 与 n 是互质数；公钥运算，用于对加密数据 x 应用所述自同态 [z] 从而得到修改的数据 x′；以及私钥运算，用于对修改的数据 x′ 应用 [-w]([u]+[z]) 从而得到数据 x，其中 w 是整数，而 $wv = 1 \bmod n$。

[0039] 另一方面，本发明提供用于在密码系统中执行密码运算的方法，该密码系统在 n 阶椭圆曲线 E 上运算。该方法包括以下步骤：导出对应于二次代数整数 z 的自同态 [z]，该二次代数整数 z 满足 $z^2+uz+v = 0$，其中 u 和 v 是秘密整数，并且 v 与 n 是互质数；利用自同态 [z] 对加密数据 x 应用公钥运算以便得到修改的数据 x′；以及利用 [-w][u]+[z] 对修改的数据 x′ 应用私钥运算以便得到数据 x，其中 w 是整数，而 $wv = 1 \bmod n$。

附图说明

[0040] 现在将仅通过实例参照附图描述本发明的实施例，其中：

[0041] 图 1 是密码交换方案的图示；

[0042] 图 2 是显示了陷门单向函数的应用系统的图示；

[0043] 图 3 是显示了图 2 中陷门单向函数用于加密的应用系统的图示；

[0044] 图 4 是显示了图 2 中陷门单向函数用于数字签名的应用系统的图示；

[0045] 图 5 是显示了图 2 中陷门单向函数用于聚合签名的应用系统的图示；

[0046] 图 6 是一图示，示出了图 2 中陷门单向函数用于具有单个消息的聚合签名以及多个签名者的多重陷门单向函数的应用系统。

具体实施方式

[0047] 因而参照图 1，密码系统 10 具有经信道 16 通信的第一实体 12 和第二实体 14。第一实体 12 和第二实体 14 各具有密码模块 15，该密码模块将可用的公钥函数或私钥函数 18 应用于两个实体 12、14。各实体 12、14 将利用带有 TOWF 的密钥函数 18 实现如上所述的加密 / 解密或签名 / 认证。

[0048] 为了实现这种系统，必须确定具有对应的公钥函数和私钥函数的合适的 TOWF。发

明人已认识到利用二次代数整数 z 可得到合适的 TOWF。然后找到曲线 E 和在 E 上定义 [z] 的有理映射。该有理映射 [z] 是 TOWF。Z 的明智选择将确保其有必要的密码属性，即：

[0049] (a) 可有效计算 [z]；

[0050] (b) 难以反演 [z]；

[0051] (c) 从定义 [z] 的有理函数难以确定 z；以及

[0052] (d) 对 z 的了解使得可以基于某组椭圆曲线点反演 [z]。

[0053] 更一般而言，某人可以使用两个不同曲线 E 和 E′ 之间的有理映射 r。该有理映射可用作 TOWF。然而，为了易于执行，使用 E = E′ 更方便。优选执行从 E 到 E 的有理映射。

[0054] 因为每一有理映射（即从 E 到 E）是平移和自同态的组合，其中平移易于确定和反演，有理映射最安全的部分是自同态。因而执行有理映射时优选自同态。

[0055] 发明人已认识到，为了反演 z 计算陷门的逆的一种潜在方法是使用 z 的二次方程：$z^2+uz+v = 0$，其中 u 和 v 是整数。该方程除以 vz 得出 (z+u)/v+(1/z) = 0。从而 (1/z) = -(z+u)/v。此时，(1/z) 通常不是二次代数整数。更准确地，如果 z 的次数大于 1，那么 (1/z) 不是二次代数整数。因而，没有反演 [z] 的自同态。反而，有双重自同态 (dual endomorphism)[z′] = [-(z+u)]，其满足 [z][z′] = [v]。在特定域 F 中，椭圆曲线 E 的阶 n 有时可与 v 互质数，这意味着有一整数 w 使得 wv = 1 mod n。这意味着对于定义在 F 上的 E 的点来说 [w] 用作 [v] 的逆。

[0056] 这时，E(F) 上 [z] 的作用 (action) 是通过自同态 [w][z′] = [-w(z+u)] 可逆的。如果可有效找到 [z]，那么 [-w(z+u)] 也是可能找到的。其可选表达式为 [-w]([u]+[z])。

[0057] 从而，可利用自同态 [z] 作为公钥运算以及关系 [-w]([u]+[z]) 作为私钥运算。

[0058] 整数 u，v 保持加密并且只对执行私用函数的实体可用。

[0059] 应该了解这对域 F 是特定的并且对于定义在另一个域 F′ 上的 E 是不正确的。定义在 F 上的 E 的点有时表示为 E(F) 以强调坐标在 F 之外的点不在考虑之中。

[0060] 对于 [z] 为了是陷门单向函数，从 [z] 的公共定义确定 u 和 v 应该是计算上不可行的，否则其 E(F) 上的逆被有效计算为 [-w]([u]+[z])。因而，需要给出不允许容易确定 u 和 v 的 [z] 的形式。

[0061] 通过将 [z] 设为一对有理函数，认为不易确定 u 和 v。典型地，第一坐标仅是 x 的函数，因此 [z] 有点为规范形式 (r(x)，g(x，y))，然后计算 r(x) 的说明可潜在地暴露 r(x) 的分子的次数，尽管因大量的项而作为两个多项式的比的 r(x) 的完全展开可能是不可实行的。由于 [z] 的次数是 v，[z] 的说明有可能将暴露 v。因而，为了确保 [z] 是单向陷门，重要的是确保也不暴露 u，否则可如上所述将 [z] 反演。

[0062] 根据 Silverman，确定通用椭圆曲线的自同态环是非平凡问题。由于 v 和 u 本质上确定自同态环，基于 (up to) 整数因子，仅从椭圆曲线的说明确定 v 和 u 通常不可行。因而，根据单个复数自同态的说明，确定自同态环仍是非平凡问题，这似乎可信。尤其，这意味着根据作为一对有理函数的 [z] 的说明来确定 u 是非平凡问题，也似乎可信。

[0063] 因而，应该选择 z 的次数使得其有适当大的阶。这样有助于确保利用关系 $u^2 < 4v$ 不会耗尽所有的可能 u 值。这是从上面得出的，因为 z 必须为虚数复数。

[0064] [z] 的一个可能构造基于下面结论。如上所述，如果 e = [z] = (r(x)，cyr′ (x)) 为 m 次，那么 r(x) = p(x)/q(x)，其中 p 和 q 分别是 m 和 m-1 次的多项式。e 的核是 m 个点

的集合，椭圆 $0 = Zi, Z_2, \ldots, Z_m$，使得对于 j 从 1 到 m 有 $e(Z_j) = 0$。如果对于 j 从 2 到 m，有 $Z_j = (z_j, y_j)$，那么可假定 $q(x) = (x-z_2)(x-z_3)\ldots(x-z_m)$。而且，由于 $[z']\,[z] = [m]$，所以 $mZ_j = 0$，其中当如上确定为 $mZ_j = [m]Z_j = [z']\,[z]Z_j = [z']\,0 = 0$ 时，z′ 是 z 的共轭。此外，e 的核是椭圆曲线 E 中的阶 m 的子群，尽管不必须为 E(F) 的一部分。总体上，该椭圆曲线通常至少有 m+1 个此类子群。

[0065] 接着，考虑含有点 $B = (0, \sqrt{b})$ 的椭圆曲线。假定有某点 W，使得 $[z]W = B$。对于 j 从 1 到 m，让 $W_j = W+Z_j$。（注意 $W_1 = W+Z_1 = W+0 = W$）。假定对于 j 从 1 到 m，有 $W_j = (wj, uj)$。那么对于某常量 d，有 $p(x) = d(x-w_1)(x-w_2)\ldots(x-w_m)$。

[0066] 注意 $p(x) = d(x-w_1)u(x)$，u(x) 的根实质为 q(x) 的根的有理函数。当两个多项式的根具有像这种简单关系时，有多项式系数变换。例如，如果 u(x) 的根是 q(x) 的根的平方，那么 $u(x) = q(\sqrt{x})q(-\sqrt{x})(-1)^{\deg q(x)}$。这样，可看到计算 q(x) 能够提供计算 u(x) 的方法。

[0067] 应用上面结论，可以搜索某椭圆曲线 E 中的阶 m 的子群，其有限 x 坐标是低汉明权多项式 q(x) 的零点。最好具有低汉明权多项式 q(x)，因为它们对计算有效。然后将找到如上所述的点 W，如上概述，其允许人们有效计算分子 p(x)。一旦算出 p(x) 和 q(x)，那么可算出 r(x)。

[0068] 如下说明如何找到这种多项式 p(x)、q(x)。注意如果 Z_j 在 [z] 的核中，那么 $-Z_j$ 也在其中，并因此 z_j 可作为 q(x) 的二重根出现。假定 q(x) 有 m 次，m 为质数。进一步假定 m 是 Elkies 质数，其确切含义不涉及下面讨论。这意味着对 s(x) 的 (m-1)/2 次多项式 $q(x) = s(x)^2$，其为 m 次除法多项式 (division polynomial) 的因子。对椭圆曲线 E(F) 上的点计数的 Schoof-Elkies-Atkin(SEA) 算法包括找到 s(x) 形式多项式的步骤。通过递推方程找到多项式 v(x) 的系数。从而，构造这种多项式的方法是众所周知的。在 SEA 算法中，找到针对较小 m 值的这种 s(x)，但对于本发明的目的，使 m 值增大有利。

[0069] 另一种可能的方法是选择低汉明权的不可约分多项式 s(x)。使 z 为其一个根，其中 z 是椭圆曲线 E 上某点的 x 坐标。该点可以具有有限阶 m。通过应用 Galois 自同构，该有限阶将对 s(x) 的任何根 z 有效 (hold)。如果这时来自 s(x) 的根的这些点是之内有界的，即它们形成 E 的子群，那么 s(x) 具有理想的形式。为此 (For this to happen)，我们基本需要 Galois 自同构 g 和 E 上的点 P 使得 $g(P) = 2P$。通过搜索 g、P 以及 E，使得能够找到理想形式的多项式 s(x)。实际中，因为只采用两个值之一，所以可忽略 y 坐标。

[0070] 如果自同态的核只在点 0 与群 E(F) 相交，那么群 E(F) 上自同态 e 的作用是可逆的。这种情况下，自同态 e 是群 E(F) 的自同构。通常群 E(F) 是循环的，并在下面讨论中，我们假定群 E(F) 是循环的。如果 e 是 n 阶循环群的自同构，那么由发明人实现的算法确定整数 d，使得 $e(G) = dG$，其中对于该群使用加号 (additive notation)。该算法的代价取决于 n-1 的因式分解。公知 n 的随机值通常具有约为 $n^{1/3}$ 的因子 f。给定这个大小的因子，该算法可用 f 的常量多倍的方式确定 d。这样比给出 dG 找 d 的通用算法快得多。通用算法采用 $n^{1/2}$ 方式。

[0071] 因而，最好群 E(F) 有 n 阶使得 n-1 没有接近 $n^{1/3}$ 的因子。用这种方法选择 n 的可选方法是仅选择较大的 n，以便攻击 $n^{1/3}$ 的代价是考虑中的对手所无法达到的。例如，在 80 位安全级别，可选择这种较大的 n 以便使得 n 约为 2^{240}，并且在 128 位安全级别，可选择 n 使

得 n 约为 2^{384}。然而，出于效率的理由，优选使用较小的 n，而因此推测将采取必要的额外工作，以确保 n-1 的大小近似于 $n^{1/3}$。

[0072] 在图 2 中主要示出了使用自同态 e 的方式。第一实体 12 取一 x 值。其可从两个相应 y 值中任意选择一个。然后将应用公钥函数 [z] 作为有理映射 e = (r(x),g(x,y)) 并计算 e(x,y) 从而得到某值 (x′ ,y′)。这将是基本公钥运算。第二实体 14 接收消息 (x′ ,y′) 并接着应用 e^{-1} 从而得到值 (x,y)。这将是基本私钥运算 [-w]([u]+[z])。注意如果 y 改为 -y，y′ 改为 -y′ ，但不影响 x′ 和 x。因而实际上差不多可以忽略 y。

[0073] 如图 3 中所示将此方法用于加密，第一实体 12 通过应用公钥函数 [z] 设定 x 为明码以及 x′ 为密码。公钥加密的公知复杂方法通常对明码 x 进行一些随机化填充，以便尤其对相同明码的重复加密给出不同密码。第二实体 14 利用私钥函数对密码 x′ 解密从而得到明码 x。

[0074] 如图 4 中所示将此方法用于签名，第二实体将 x′ 设定为有待签名的消息，并且通过应用私钥函数计算作为签名的 x。通常使用一定的散列来创建来自较长消息的 x′ ，这是数字签名的标准方法。第一实体 12 使用公钥运算 e 来确认 e(x,y) = (x′ ,y′)。散列函数是单向的，因此第一实体不能从 (x,y) 开始伪造签名以及应用 e 得到 (x′ ,y′)，因为下一步将找到消息 M，使得 x′ = Hash(M)，对于单向散列函数这被认为不可实行。

[0075] 如果反演 [z] 的问题与 E 中离散对数问题一样难，那么密码群的大小可以小于用于 RSA TOWF 的群。例如，粗略认为 3072 位 RSA 系数与定义在 256 位域上的椭圆曲线一样安全。认为两种目标的安全级别都是 128 位，这是目前经互联网使用最广泛的商业级安全级别，例如网上银行业务。椭圆曲线陷门单向函数 [z]，签名 x 或基本密码 x′ 的大小是 256 位，但对于 RSA 大小为 3072 位。

[0076] 与传统椭圆曲线密码编码系统 (ECC) 相比，256 位椭圆曲线的签名大约长 512 位，其为椭圆曲线 TOWF 的签名大小的两倍。对于加密可能有类似的节省。

[0077] 在另一个实施例和本发明的应用中，TOWF 应用于签名或密码的聚合。下面将解释签名，但应该了解密码的细节完全类似。

[0078] 签名聚合意指单个签名表示由单个签名者签名的多个消息，或由多个签名者签名的单个消息，或由多个签名者签名的多个消息。

[0079] 现在参照图 5，为了对 t 个消息 m_1、m_2、...、m_t 签名，签名者 (例如，第一实体 12) 对每个消息进行散列并且将每个散列转换为椭圆曲线点，产生 (yield)t 个点 P_1、...、P_t，而后加起来从而产生一点 $P = P_1+...+P_t$。而后签名者应用反函数 e^{-1} 从而得到签名 $S = e^{-1}(P)$，其为对于多个消息的单个消息。而后另一个实体 (例如，第二实体 14) 的认证包括对消息进行散列、将每个散列转换为一点、求和得到整个 P，而接着通过检验是否 e(S) = P 将公钥 18 运算 e 应用于 S。这样做相比于仅并联这些消息的做法的优势在于，因为签名是加性的，为希望改变部分消息的签名者实现较大的灵活性。

[0080] 上述程序不强制对个体消息部分签名的顺序，即签名认证和由相同实体签名的一组 (无序) 签名有关。然而应该注意，假如通过认证实体可取回或导出个体纯量倍数 (scalar multiples)(“权”)，该程序可易于概括为个体签名的加权和，而非个体签名部分 S_1、...、S_t 的和。这将允许在这 t 个消息的签名过程中规定顺序，通过使权数依赖于可应用的顺序。

[0081] 现在参照图 6，如果 t 个不同的签名者（例如，集体第一实体 12）使用相同的椭圆曲线群，并且具有不同的 TOWF e_1、...、e_t，那么它们可以如下形成单个消息的聚合签名。为了签名消息 m，第一实体 12 的第一个签名者计算消息的散列并且将该散列转换为椭圆曲线点 P。接着它们（即第一实体 12 的所有签名者）通过每个应用其私钥运算共同计算 $e^t(e_{t-1}^{-1}(...(e_1^{-1}(P))))$，其中由实体 1、2、...、t 按顺序进行签名。认证（例如，由第二实体 14）包括按相反的顺序应用各相应的公钥 18 操作，并检验合成点 P(resulting point) 是否对应于被签名消息 m 的散列值。

[0082] 通常，椭圆曲线自同态交换 (commut)，因此由多个实体对单个消息签名的顺序好像不相关。然而应该注意，该程序易于一般化使得在签名过程中强制顺序。如下所述可实现这一点，例如，通过使每个签名实体向被计算的签名施加一个偏移。

[0083] 假定由实体 i 在点 P 的个体签名是 $e_i^{-1}(P+A_i)$，其中椭圆曲线点 A_i 对实体 i 是唯一的。那么通过对 m 进行散列和将该散列转换为椭圆曲线点 P（如前），可得到实体 1、2、...、t 对消息 m 的有序聚合签名，并随后使各签名实体在合成值上应用其自己的签名操作。这样导致 $S_1 = e_1^{-1}(P+A_1)$，$S_2 = e_2^{-1}(S_1+A_2)$，...，$S_t = e_t^{-1}(S_{t-1}+A_t)$，其中 S_t 是合成聚合签名。假如个体偏移 (individual offsets)A_1、...、A_t 可通过认证实体取回或导出，并且取决于计算顺序 $S_{t-1} = e_t(S_t)-A_t$，$S_{t-2} = e_t(S_{t-1})-A_{t-1}$，...，$S_1 = e_2(S_2)-A_2$，$P = e_1(S_1)-A_1$ 以及检验椭圆曲线点 P 是否对应于被签名的消息 m 的散列值，现在签名认证是上述程序的细微修正 (trivial modification)，。

[0084] 上面描述了原始方案的修正，从而利用偏移 A_i 强制签名过程的顺序，其中每个偏移 A_i 对各签名实体是唯一的。应明白在此其可以有变化，例如定义 $S_i = e_i^{-1}(f(P, i))$ 而非 $S_i = e_i^{-1}(P+A_i)$，其中 f 是 E 上的映射，属性为可从 f(P, i) 以及与签名实体 i 相关的公共信息有效重新计算 P。多个实体对单个消息的有序签名对签定 (signing off) 例如大机构中的项目有用，其中要求多个签名并且项目需要由所涉及的授权方以特别分级顺序（例如，颠倒）签定。

[0085] 尽管参照一定的特定实施例描述了本发明，对本领域技术人员来说其多种修改是显然的，而不脱离如其所附权利要求概括的本发明实质和范围。通过引用将上面所引用的所有参考文献的整个公开内容并入此处。

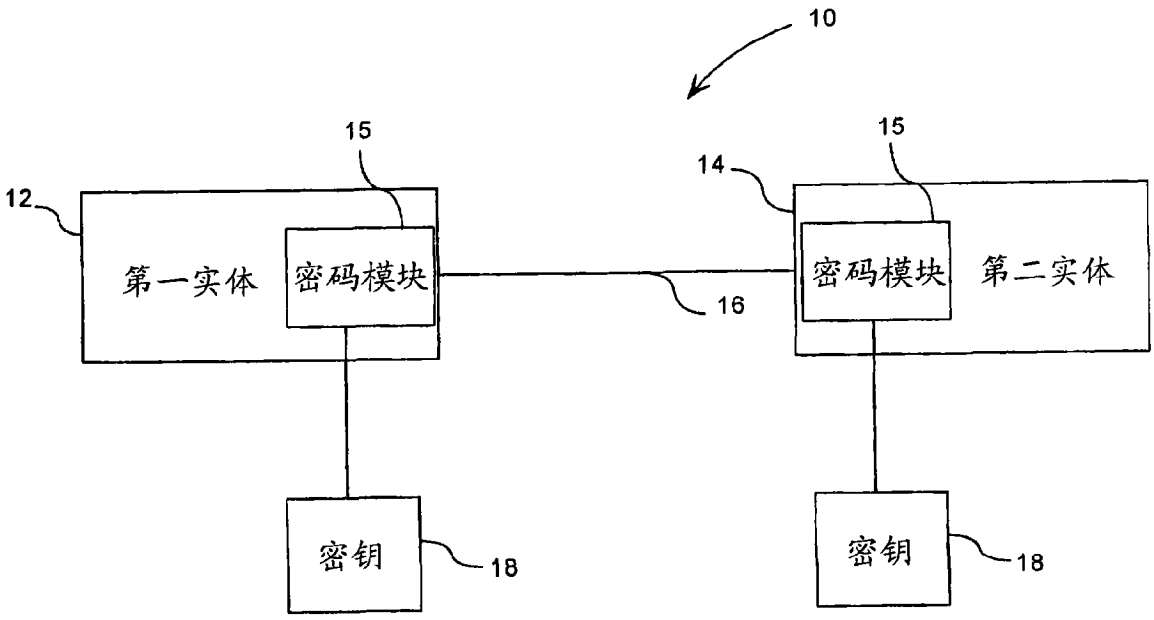

10
15
15
14
12
第一实体
密码模块
密码模块
第二实体
16
密钥
18
密钥
18

图 1

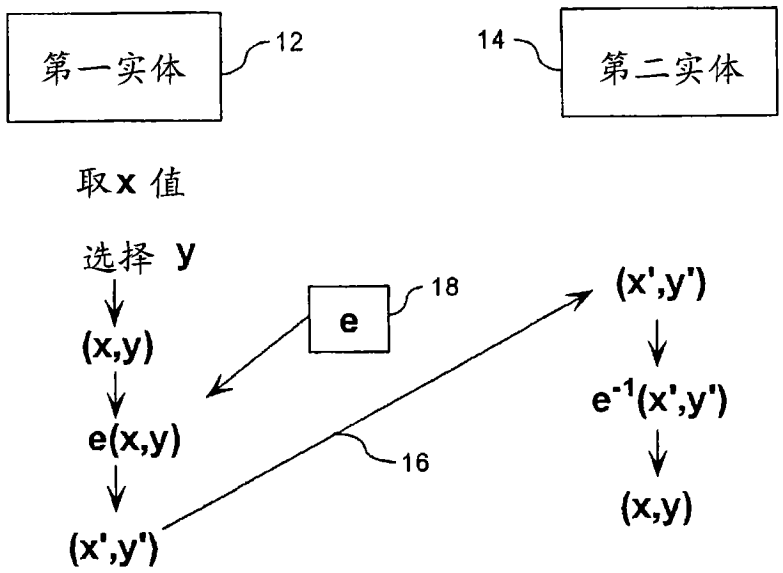

第一实体
12
14
第二实体
取x 值
选择 y
(x,y)
e(x,y)
(x',y')
e
18
16
(x',y')
e-1(x',y')
(x,y)

图 2

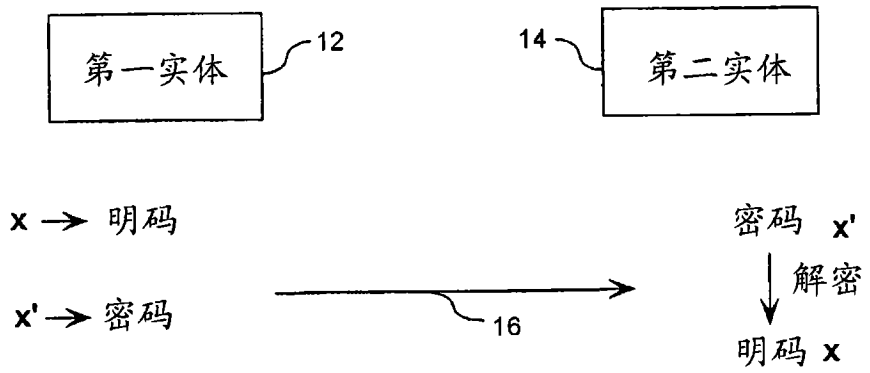

第一实体
12
14
第二实体
x → 明码
x' → 密码
16
密码 x'
解密
明码 x

图 3

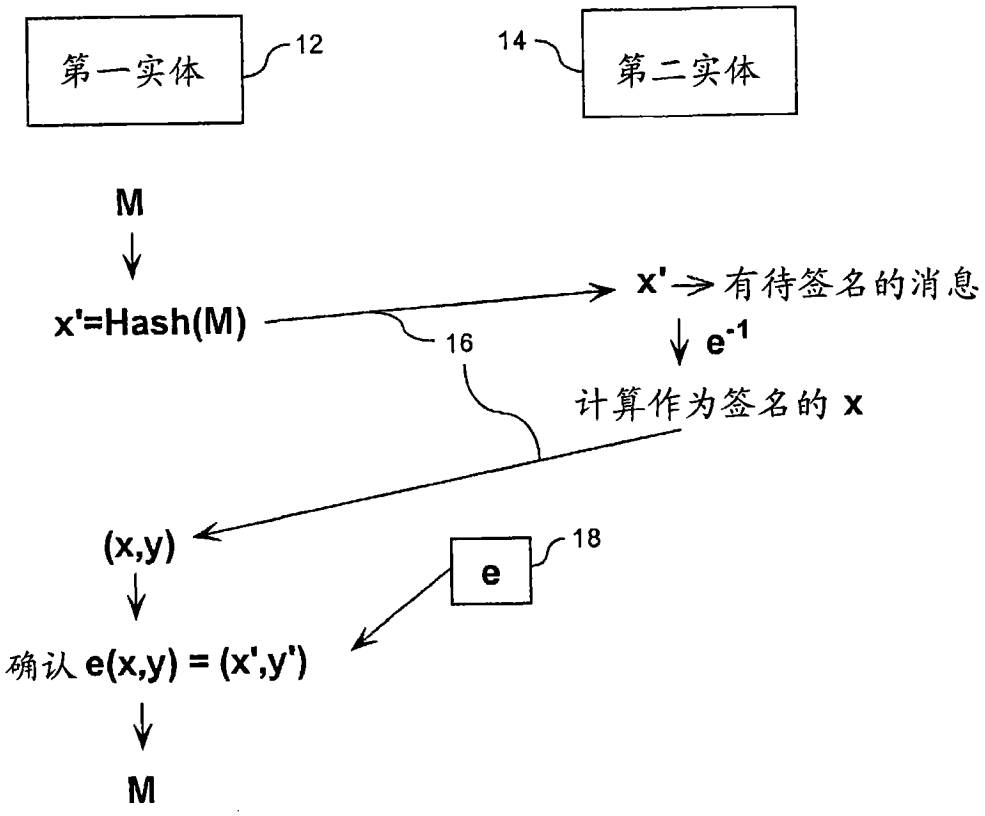

第一实体
12
14
第二实体
M
x'=Hash(M)
16
x' → 有待签名的消息
e-1
计算作为签名的 x
(x,y)
e
18
确认 e(x,y) = (x',y')
M

图 4

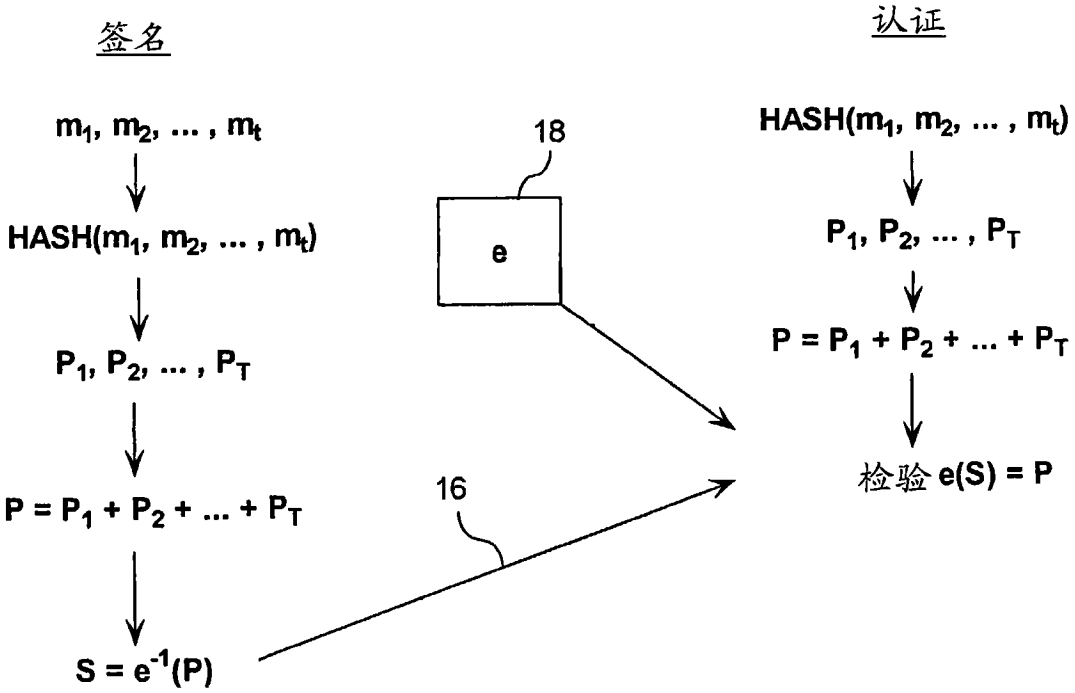

签名
认证
$m_1, m_2, \ldots, m_t$
$HASH(m_1, m_2, \ldots, m_t)$
$P_1, P_2, \ldots, P_T$
$P = P_1 + P_2 + \ldots + P_T$
$S = e^{-1}(P)$
18
e
16
$HASH(m_1, m_2, \ldots, m_t)$
$P_1, P_2, \ldots, P_T$
$P = P_1 + P_2 + \ldots + P_T$
检验 e(S) = P

图 5

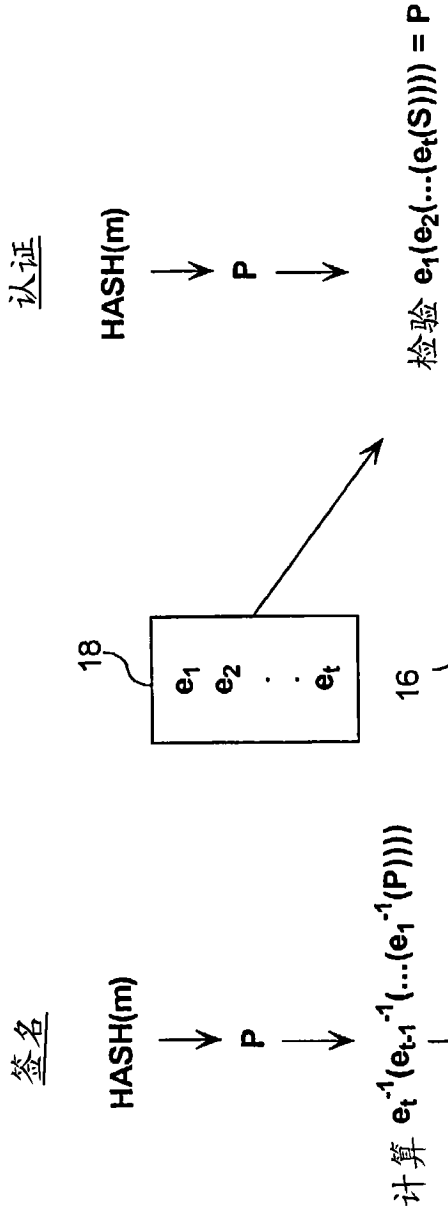

签名
HASH(m)
P
计算 $e_t^{-1}(e_{t-1}^{-1}(\ldots(e_1^{-1}(P))))$
S
16
18
e_1 e_2 . . e_t
认证
HASH(m)
P
检验 $e_1(e_2(\ldots(e_t(S)))) = P$

图 6