

1. 一种加密的方法,

5 a) 具有包含模的取幂 E 的至少一个计算步骤 $E=x^d \pmod{p \cdot q}$, 其中具有第一素数因数 p , 第二素数因数 q , 指数 d 和底数 x , 以此

b) 为进行模的取幂, 选择两个自然数 r 和 s , 条件是, d 对于 $\text{kgV}(r, s)$ 相对地是一个素数, 并以此执行以下的计算步骤:

$$x_1 = x \pmod{p \cdot r}$$

$$x_2 = x \pmod{q \cdot s}$$

10 $d_1 = d \pmod{\phi(p \cdot r)}$

$$d_2 = d \pmod{\phi(q \cdot s)}$$

$$z_1 = x_1^{d_1} \pmod{p \cdot r}$$

$$z_2 = x_2^{d_2} \pmod{q \cdot s}$$

其中 $(\phi \cdot)$ 是欧拉函数, $\text{kgV}(r, s)$ 是 r 和 s 的最小公倍数,

15 c) 然后按照中国余数定理由 z_1 和 z_2 计算数 z : $z = z_1 \pmod{p \cdot r}$; $z = z_2 \pmod{q \cdot s}$;

d) 通过还原 Z 模 $p \cdot q$, 计算取幂的结果 E ,

e) 在一个检查步骤中检查先前计算的数 z 因而检查结果 E 的计算错误,

20 f) 所述检查步骤包括下面的计算操作:

f1) 借助于扩展的欧拉算法, 计算具有特性 $e \cdot d=1$ 的最小的可能的自然数 e ,

$$f2) \text{ 计算值 } C = z^e \pmod{\text{kgV}(r, s)},$$

25 f3) 比较值 x 和 C 模 $\text{kgV}(r, s)$, 以此如果 $x \neq C \pmod{\text{kgV}(r, s)}$, 则模的取幂 E 的结果作为错误的被丢弃。

2. 一种加密方法

a) 具有包含模的取幂 E 的至少一个计算步骤 $E=x^d \pmod{p \cdot q}$, 其中具有第一素数因数 p , 第二素数因数 q , 指数 d 和底数 x , 以此

30 b) 为进行模的取幂, 在间隔 $[1, \dots, r-1]$ 和 $[1, \dots, s-1]$ 内分别选择两个自然数 r 和 s , 以及两个数 b_1 和 b_2 , 所述 b_1 和 b_2 对于 r 和 s 相对地是素数, 并且以此使 b_1 和 b_2 满足条件 $b_1 = b_2 \pmod{\text{ggT}(r, s)}$, 其中 $\text{ggT}(r, s)$ 代表 r 和 s

的最大公约数,

c) 利用两个数 b_1 和 b_2 按照中国余数定理计算满足下式的 x_1, x_2 :

$$x_1 = x \pmod{p}, \quad x_1 = b_1 \pmod{r}$$

$$x_2 = x \pmod{q}, \quad x_2 = b_2 \pmod{s}$$

5 并进行以下计算步骤:

$$d_1 = d \pmod{\phi(p)}$$

$$d_2 = d \pmod{\phi(q)}$$

$$z_1 = x_1^{d_1} \pmod{p \cdot r}$$

$$z_2 = x_2^{d_2} \pmod{q \cdot s}$$

10 其中 (ϕ) 是欧拉函数, $\text{kgV}(r, s)$ 是 r 和 s 的最小公倍数,

d) 然后按照中国余数定理由 z_1 和 z_2 计算数 z : $z = z_1 \pmod{p \cdot r}$; $z = z_2 \pmod{q \cdot s}$;

e) 通过还原 z 模 $p \cdot q$, 计算取幂的结果 E ,

f) 在一个检查步骤中检查先前计算的数 z (因而自动地也是结果 E) 的

15 计算错误,

g) 所述检查步骤包括下面的计算操作:

g1) 计算数

$$C_1 = b_1^{d_1} \pmod{r}$$

$$C_2 = b_2^{d_2} \pmod{s}$$

20 其中 d_1, d_2 在进行以 $\phi(r)$ 和 $\phi(s)$ 对模的取幂之前分别被还原,

g2) 比较 z_1 和 C_1 模 r 以及 z_2 和 C_2 模 s , 以此如果保持 $C_1 \neq z_1 \pmod{r}$, 或者 $C_2 \neq z_2 \pmod{s}$, 则模的取幂 E 的结果作为错误的被丢弃。

3. 如权利要求 2 所述的加密方法, 其特征在于, 所述数 r 和 s 是奇数。

4. 如权利要求 1-3 中的任何一个所述的加密方法, 其特征在于, 其中
25 的数 r 和 s 在 $[0, 2^k-1]$ 的范围内选择, 其中 $16 \leq k \leq 32$ 。

5. 如权利要求 1-4 中的任何一个所述的加密方法, 其特征在于, 其中所述的数 r 和 s 中的至少一个这样选择, 使得乘积 $p \cdot r$ 或 $q \cdot s$ 的二进制表示含有尽可能多的前置的数 (leading ones)。

6. 如权利要求 1-5 中的任何一个所述的加密方法, 其特征在于, 其中
30 所述的两个数 r 和 s 这样选择, 使得乘积 $p \cdot r$ 或 $q \cdot s$ 的二进制表示含有尽可能多的前置的数。



[12] 发明专利申请公开说明书

[21] 申请号 01809690.5

[43] 公开日 2003 年 7 月 9 日

[11] 公开号 CN 1429360A

[22] 申请日 2001.5.15 [21] 申请号 01809690.5
[30] 优先权
[32] 2000. 5.17 [33] DE [31] 10024325.8
[86] 国际申请 PCT/EP01/05532 2001.5.15
[87] 国际公布 WO01/88693 德 2001.11.22
[85] 进入国家阶段日期 2002.11.18
[71] 申请人 德国捷德有限公司
地址 德国慕尼黑
[72] 发明人 马丁·塞森

[74] 专利代理机构 北京市柳沈律师事务所
代理人 王志森 黄小临

权利要求书 6 页 说明书 7 页

[54] 发明名称 加密的方法和装置

[57] 摘要

本发明涉及一种加密方法，具有包含模的取幂 E 的至少一个计算步骤 $E = x^d \pmod{p \cdot q}$ ，其中具有第一素数因数 p，第二素数因数 q，指数 d 和底数 x，以此按照中国余数定理计算模的取幂 E。

ISSN 1008-4274

7. 如权利要求 5 和 6 之一所述的加密方法, 其特征在于,

a) 在第一个分步骤, 不受 d 对于 $\phi(kgV(r, s))$ 相对地是素数这个条件的限制, 对于数 r 和 s 中的至少一个分别首先选择相应的最佳数 r_{opt} 和 s_{opt} , 以及

5 b) 在第二个分步骤中, 选择相邻的值 $r=r_{opt}-i$ 和 $s=s_{opt}-i$, $i=0, 1, \dots, k$, 使得 d 对于 $\phi(kgV(r, s))$ 相对地是素数。

8. 如权利要求 5 和 6 之一所述的加密方法, 其特征在于,

a) 在第一个分步骤, 不受 d 对于 $\phi(kgV(r, s))$ 相对地是素数这个条件的限制, 对于数 r 和 s 中的每一个分别选择相应的最佳数 r_{opt} 和 s_{opt} , 以及

10 b) 在第二个分步骤中, 选择值 $r=2^l$, $r_{opt}s=2^l s_{opt}$, $l=0, 1, \dots, j$, 使得 d 对于 $\phi(kgV(r, s))$ 相对地是素数。

9. 如权利要求 5 和 6 之一所述的加密方法, 其特征在于,

a) 在第一个分步骤, 不受 d 对于 $\phi(kgV(r, s))$ 相对地是素数这个条件的限制, 首先选择数 r_{opt} 和 s_{opt} 中的至少一个,

15 在第二个分步骤中, 选择相邻的值 $r=r_{opt}-i$ 和 $s=s_{opt}-i$, $i=0, 1, \dots, k$, 使得如果对于 $i=0, 1, \dots, k$ 这种值存在, 则 d 对于 $\phi(kgV(r, s))$ 相对地是素数, 以及

c) 在第三分步骤, 这样选择值 $r=2^l r_{opt}$, $s=2^l s_{opt}$, $l=0, 1, \dots, j$, 使得如果在第二个分步骤中未选择所述的值, 则 d 对于 $\phi(kgV(r, s))$ 相对地是素数。

20 10. 如上述任何一个权利要求所述的加密方法, 其特征在于, 其包括 RSA 方法。

11. 如上述任何一个权利要求所述的加密方法, 其特征在于, 其包括拉比特特征方法。

25 12. 如上述任何一个权利要求所述的加密方法, 其特征在于, 其包括 Fiat-Shamir 识别方法。

13. 一种加密装置,

a) 具有至少一个取幂装置, 用于执行一个包含模的取幂 E 的计算步骤,

$$E=x^d \pmod{p \cdot q}$$

30 其中具有第一素数因数 p , 第二素数因数 q , 指数 d 和底数 x , 以此

b) 为进行模的取幂, 选择两个自然数 r 和 s , 条件是, d 对于 $\phi(kgV(r, s))$

相对地是一个素数，并以此执行以下的计算步骤：

$$x_1 = x \pmod{p \cdot r}$$

$$x_2 = x \pmod{q \cdot s}$$

$$d_1 = d \pmod{\phi(p \cdot r)}$$

$$5 \quad d_2 = d \pmod{\phi(q \cdot s)}$$

$$z_1 = x_1^{d_1} \pmod{p \cdot r}$$

$$z_2 = x_2^{d_2} \pmod{q \cdot s}$$

其中 $(\phi \cdot)$ 是欧拉函数， $\text{kgV}(r, s)$ 是 r 和 s 的最小公倍数，

c) 然后按照中国余数定理由 z_1 和 z_2 计算数 z ： $z = z_1 \pmod{p \cdot r}$ ； $z = z_2$
10 $\pmod{q \cdot s}$ ；

d) 通过还原 z 模 $p \cdot q$ ，计算取幂的结果 E ，

e) 在一个检查步骤中检查先前计算的数 z （因而也自动地是结果 E ）的计算错误，

f) 所述检查步骤包括下面的计算操作：

15 f1) 借助于扩展的欧拉算法，计算具有特性 $e \cdot d = 1 \pmod{\text{kgV}(r, s)}$ 的最小的可能的自然数 e ，

f2) 计算值 $C = z^e \pmod{\text{kgV}(r, s)}$ ，

f3) 比较值 x 和 C 模 $\text{kgV}(r, s)$ ，以此如果 $x \neq C \pmod{\text{kgV}(r, s)}$ ，则模的取幂 E 的结果作为错误的被丢弃。

20 14. 一种加密装置

a) 具有至少一个取幂装置，用于执行包含模的取幂 E 的至少一个计算步骤 $E = x^d \pmod{p \cdot q}$ ，其中具有第一素数因数 p ，第二素数因数 q ，指数 d 和底数 x ，以此

b) 为进行模的取幂，在间隔 $[1, \dots, r-1]$ 和 $[1, \dots, s-1]$ 内分别选择两个
25 自然数 r 和 s ，以及两个数 b_1 和 b_2 ，所述 b_1 和 b_2 对于 r 和 s 相对地是素数，并且以此使 b_1 和 b_2 满足条件 $b_1 = b_2 \pmod{\text{ggT}(r, s)}$ ，其中 $\text{ggT}(r, s)$ 代表 r 和 s 的最大公约数，

c) 利用两个数 b_1 和 b_2 按照中国余数定理计算满足下式的 x_1, x_2 ：

$$x_1 = x \pmod{p} \quad , \quad x_1 = b_1 \pmod{r}$$

$$30 \quad x_2 = x \pmod{q} \quad , \quad x_2 = b_2 \pmod{s}$$

并进行以下计算步骤：

$$d_1 = d \pmod{\phi(p)}$$

$$d_2 = d \pmod{\phi(q)}$$

$$z_1 = x_1^{d_1} \pmod{p \cdot r}$$

$$z_2 = x_2^{d_2} \pmod{q \cdot s}$$

5 其中 (ϕ) 是欧拉函数, $\text{kgV}(r, s)$ 是 r 和 s 的最小公倍数,

d) 然后按照中国余数定理由 z_1 和 z_2 计算数 z : $z = z_1 \pmod{p \cdot r}$; $z = z_2 \pmod{q \cdot s}$;

e) 通过还原 z 模 $p \cdot q$, 计算取幂的结果 E ,

f) 在一个检查步骤中检查先前计算的数 z (因而自动地也是结果 E) 的
10 计算错误,

h) 所述检查步骤包括下面的计算操作:

g1) 计算数

$$C_1 = b_1^{d_1} \pmod{r}$$

$$C_2 = b_1^{d_2} \pmod{s}$$

15 其中 d_1, d_2 在进行以 $\phi(r) \phi(s)$ 对模的取幂之前分别被还原,

g2) 比较值 z_1 和 C_1 模 r 以及 z_2 和 C_2 模 s , 以此如果保持 $C_1 \neq z_1 \pmod{r}$, 或者 $C_2 \neq z_2 \pmod{s}$, 则模的取幂 E 的结果作为错误的被丢弃。

15. 如权利要求 14 所述的加密装置, 其特征在于, 所述数 r 和 s 是奇数。

16. 如权利要求 13 - 15 中的任何一个所述的加密装置, 其特征在于, 其
20 中的数 r 和 s 在 $[0, 2^k - 1]$ 的范围内选择, 其中 $16 \leq k \leq 32$ 。

17. 如权利要求 13 - 16 中的任何一个所述的加密装置, 其特征在于, 其中所述的数 r 和 s 中的至少一个这样选择, 使得乘积 $p \cdot r$ 或 $q \cdot s$ 的二进制表示含有尽可能多的前置的数。

18. 如权利要求 13 - 17 中的任何一个所述的加密装置, 其特征在于, 其
25 中所述的两个数 r 和 s 这样选择, 使得乘积 $p \cdot r$ 或 $q \cdot s$ 的二进制表示含有尽可能多的前置的数。

19. 如权利要求 17 和 18 之一所述的加密装置, 其特征在于,

a) 在第一个分步骤, 不受 d 对于 $\phi(\text{kgV}(r, s))$ 相对地是素数这个条件的限制, 对于数 r 和 s 中的至少一个分别首先选择相应的最佳数 r_{opt} 和 s_{opt} , 以
30 及

b) 在第二个分步骤中, 选择相邻的值 $r = r_{\text{opt}} - i$ 和 $s = s_{\text{opt}} - i$, $i = 0, 1, \dots, k$,

使得 d 对于 $\phi(kgV(r, s))$ 相对地是素数。

20. 如权利要求 17 和 18 之一所述的加密装置，其特征在于，

a) 在第一个分步骤，对于数 r 和 s 中的每一个分别选择相应的最佳数 r_{opt} 和 s_{opt} ，不受 d 对于 $\phi(kgV(r, s))$ 相对地是素数这个条件的限制，以及

5 b) 在第二个分步骤中，选择值 $r=2^l r_{opt}$ $s=2^l s_{opt}$, $l=0, 1, \dots, j$, 使得 d 对于 $\phi(kgV(r, s))$ 相对地是素数。

21. 如权利要求 17 和 18 之一所述的加密装置，其特征在于，

a) 在第一个分步骤，不受 d 对于 $\phi(kgV(r, s))$ 相对地是素数这个条件的限制，首先选择数 r_{opt} 和 s_{opt} 中的至少一个，

10 b) 在第二个分步骤中，选择相邻的值 $r=r_{opt}-i$ 和 $s=s_{opt}-i$, $i=0, 1, \dots, k$, 使得如果对于 $i=0, 1, \dots, k$ 这种值存在，则 d 对于 $\phi(kgV(r, s))$ 相对地是素数，以及

c) 在第三分步骤，这样选择值 $r=2^l r_{opt}$, $s=2^l s_{opt}$, $l=0, 1, \dots, j$, 使得如果在第二个分步骤中未选择所述的值，则 d 对于 $\phi(kgV(r, s))$ 相对地是素数。

15 22. 如上述任何一个权利要求所述的加密装置，其特征在于，其包括 RSA 方法。

23. 如上述任何一个权利要求所述的加密装置，其特征在于，其包括拉比特征方法。

20 24. 如上述任何一个权利要求所述的加密装置，其特征在于，其包括 Fiat-Shamir 识别方法。

加密的方法和装置

5 技术领域

本发明涉及一种加密的方法和装置。

背景技术

由于电子商务的不断增加的重要性，以加密和特征方案(signature
10 scheme)形式的加密方法开始广泛流行。这些方法一般借助于电子装置来实现，所述电子装置可以包括例如可编程的通用微型控制器，或者是专用的电子电路，例如 ASIC 形式的电子电路。一种加密装置的特别感兴趣的加密形式是智能卡，因为如果在技术上设计得当，其可以保护密钥数据防止进行未被允许的访问。一直努力致力于改善加密方法的执行速度，以及
15 保护它们免遭各种可能的攻击方案。本发明尤其适用于和智能卡结合使用，但是并不限于此。本发明可以和各种加密装置结合来实施。

在许多已知的加密方法中，需要按照下式进行模的取幂(modular exponentiation):

$$E=x^d \pmod{N}=x^d \pmod{p,q} \quad (1)$$

20 其中 p 和 q 是素数(prime number)。一种包括模的取幂步骤的特别重要的加密方法是 RSA 方法，该方法例如可以由 Alfred J. Menezes, Paul C. van Oorschot 和 Scott A. Vanstone, "Handbook of Applied Cryptography" Boca Raton: CRC Press, 1997, pages 285-291 得知。不过，模的取幂的使用不限于 RSA 方法，还包括例如从 Menezes et al., ibid., pages 438-442 得知的 Rabin
25 特征，以及从 Menezes et al. ibid., pages 408-410 得知的 Fiat-Shamir 识别方案。

包括模的取幂的加密方法的安全性经常取决于由公式(1)把数 N 因子分解成其素数因数(prime factor)p 和 q 的难度。这个问题只有对大的值 N 才具有足够的复杂性，因此，在一方面，应当选择尽可能大的数 N。在另一
30 方面，借助于按照公式(1)的模的取幂计算所述的值的计算工作随着 N 的数量的增大而单调地增加，因此，从实际应用的观点看来，尽管 N 取大的值，

但是同时希望把所需的计算时间限制在可接受的值。

已知为了应用被称为“中国余数定理”来4倍提高计算速度，该定理例如使得在相等的计算时间内能够有较大的值N。直接代替公式(1)，按照下式进行变换：

$$5 \quad E = x^d \pmod{p \cdot q} = aE_1 + bE_2 \pmod{N} \quad (2)$$

其中

$$E_1 = x^d \pmod{p} \quad (3)$$

$$E_2 = x^d \pmod{q} \quad (4)$$

应用中国余数定理的一个结果是，所述模的取幂不再对模N进行计算，
10 即不再以对模(modulo)该隐藏其自身的素数的因子分解的数进行计算，而是在这种计算规则中预先假定连续地第一步计算模p和第二步计算模q，即对素因子分解的认识 $n=p \cdot q$ ，以便保持秘密，并导致把总的计算过程分解成第一计算步骤(3)，其主要涉及第一素数因数，和第二计算步骤(4)，其主要涉及第二素数因数。其优点在于，必须对模 $\phi(p \cdot q)$ 规定在公式(1)中的指数d，而必须只对模 $\phi(p)$ 或 $\phi(q)$ 规定在公式(2)中的指数，其中 ϕ 表示欧拉函数。
15

感兴趣的是，对这种使用模的取幂的加密方法的一种攻击(attack)方案最近已经成为已知的，通过所述方案，只要具体的执行利用按照公式(2)到(4)所示的中国余数定理，借助于在未扰乱的计算序列中的合适的人工指令，关于N的素因子因子分解的信息可以从扰乱的模的取幂的有缺陷的结果恢复。这种被称为“贝利克攻击”的试图例如在 Dan Boneh, Richard A. DeMillo 和 Richard J. Lipton: “On the importance of checking cryptographic protocols for faults , ” Advances in Cryptology-EUROCRYPT, 97, Lecture Notes in Computer Science
20 1233, Berlin: Springer, 1997 中描述了。一种加密装置由物理指令操纵，例如增加时钟速度、操作电压或照射，使得在按照中国余数定理执行模的取幂时以某个不是太大的几率发生计算错误。如果只在公式(2)中的两项中的一项发生计算错误，则两个素数因数p和q可以由错误的取幂结果重构。

由所述利用中国余数定理执行的模的取幂的弱点得出的结果是，在其被
30 进一步处理之前，尤其是在以某种形式例如以特征(signature)的形式输出之前，首先检查计算操作结果的正确性。

对于“贝利克攻击”的一种价值不大的对策是借助于至少一次重复所述计算操作来实现这种正确性检查。在随机计算错误的情况下，可以假定，第一计算操作的结果偏离检查计算操作的结果。这种方法的主要缺点在于，通过一次检查计算，计算时间已经被加倍。

- 5 文件 W0 - A - 98/52319 具体地披露了一种方法，用于保护按照中国余数定理执行的模的取幂的计算操作防止“贝利克攻击。例如从 $[0, 2^k-1]$ 的范围内选择一个秘密的整数 j ，其中 $16 \leq k \leq 32$ 。然后计算下式：

$$v_1 = x \pmod{j \cdot q} \quad (5)$$

$$v_2 = x \pmod{j \cdot q} \quad (6)$$

10 $d_1 = d \pmod{\varphi(j \cdot p)} \quad (7)$

$$d_2 = d \pmod{\varphi(j \cdot p)} \quad (8)$$

$$w_1 = v_1^{d_1} \pmod{j \cdot q} \quad (9)$$

$$w_2 = v_1^{d_2} \pmod{j \cdot q} \quad (10)$$

然后检查是否其保持：

15 $w_1 = w_2 \pmod{j} \quad (11)$

如果式 (11) 可以被证实，则用已知的方法计算下式：

$$y_1 = w_1 \pmod{p} \quad (12)$$

$$y_2 = w_2 \pmod{q} \quad (13)$$

由此借助于中国余数定理便可以确定

20 $E = x^d \pmod{N} \quad (14)$

这种已知的方法和简单的检查计算操作相比的优点在于，所需的附加的计算时间被大大降低了。

在这种方法中，两个素数 p 和 q 必须乘以同一因数 c 。文件 W0 - A1-98/52319 披露了第二种方法，其允许素数 p 和 q 乘以不同的因数 r 和 s 。

- 25 不过，对于检查计算，两个另外的取幂是可能的。

发明内容

本发明的问题在于提供一种加密方法和装置，所述方法和装置节省计算操作或计算时间，同时保持或者增加安全性。

- 30 这个问题通过具有按照权利要求 1 或 2 所述的特征的一种加密方法并通过具有权利要求 13 或 14 所述的特征的一种加密装置解决了。

从属权利要求 3 到 12 以及 15 到 24 表示一些有利的发展。

具体实施方式

如上所述，如果在模的取幂中的模数具有许多前置的(leading)二进制模数，使得不同的因数 r 和 s 表示其中的某个优点，则对于某些算术和逻辑单元是有利的。此外，具有一些对于模的取幂优化的算术和逻辑单元，但是从中央处理单元向只有用于取幂的优化的算术和逻辑单元的数据传递引起可观的额外开销。本发明和上述的利用不同的因数 r 和 s 的方法相比，省去了一次取幂。

按照本发明，例如从范围 $[0, 2^k-1]$ 的范围内选择 2 个整数 r 和 s ，其中 $16 \leq k \leq 32$ ，使得 d 对于 $\phi(\text{kgV}(r, s))$ 相对地是一个素数，其中 $\text{kgV}(r, s)$ 是 r 和 s 的最小公倍数， s 和 $\phi()$ 是欧拉函数。此时，计算下式：

$$x_1 = x \pmod{p \cdot r} \quad (15)$$

$$x_2 = x \pmod{q \cdot s} \quad (16)$$

$$d_1 = d \pmod{\phi(p \cdot r)} \quad (15)$$

$$d_2 = d \pmod{\phi(q \cdot s)} \quad (16)$$

$$z_1 = x_1^{d_1} \pmod{p \cdot r} \quad (15)$$

$$z_2 = x_2^{d_2} \pmod{q \cdot s} \quad (16)$$

现在，保持 $z_1 = x_1^d \pmod{p \cdot r}$ ， $z_2 = x_2^d \pmod{q \cdot s}$ 。按照中国余数定理，利用下式可以容易地由 z_1 和 z_2 计算出一个数 z ：

$$z = z_1 \pmod{p \cdot r}; z = z_2 \pmod{q \cdot s}; z = x^d \pmod{p \cdot q \cdot \text{kgV}(r, s)} \quad (17)$$

按照本发明，数 r 和 s 必须这样选择，使得 d 对于 $\phi(\text{kgV}(r, s))$ 相对地是一个素数。在这些情况下，可以使用扩展的欧拉算法，从而利用下式容易地求出一个自然数 e ：

$$e \cdot d = 1 \pmod{\phi(\text{kgV}(r, s))} \quad (18)$$

借助于 Z 和 e ，按照下式计算数 C ：

$$C = z^e \pmod{\text{kgV}(r, s)} \quad (19)$$

按照欧拉定理，有：

$$C = z^{d \cdot e} = x \pmod{\text{kgV}(r, s)} \quad (20)$$

通过比较两个值 C 和 x 模 $\text{kg}(r, s)$ ，可以以高的概率确定错误。如果确定 $C \neq x \pmod{\text{kgV}(r, s)}$ ，则模的取幂的结果便被认为是错误的并被丢弃。

在RSA方法（像在拉比特征方案中一样）中，要进行模的取幂，以便产生数字特征或进行解密，以此使模 p, q 和指数 d 只依赖于私人密钥。其结果是，数 d, e, r 和 s 可以在所述私人密钥积分时被计算一次，并被存储，以供再用。

- 5 在本发明的改型中，例如在 $[0, 2^k-1]$ 的范围内选择 2 个整数 r 和 s ，其中 $16 \leq k \leq 32$ 。在二进制的算术和逻辑单元的情况下，建议数 r 和 s 是奇数。此外，在间隔 $[1, \dots, r-1]$ 和 $[1, \dots, s-1]$ 内选择两个固定的数 b_1 和 b_2 ，其不依赖于 x ，并分别相对于 r 和 s 是素数。如果 r 和 s 相对地不是素数，则 b_1 和 b_2 必须满足附加的条件 $b_1 = b_2 \pmod{\text{ggT}(r, s)}$ ，其中 $\text{ggT}(r, s)$ 代表 r 和 s 的最大公约数。

按照中国余数定理，首先利用下式计算数 x_1 ：

$$X_1 = x \pmod{p}, x_1 = b_1 \pmod{r} \quad (21)$$

同样按照下式计算 x_2 ：

$$X_2 = x \pmod{q}, x_2 = b_2 \pmod{s} \quad (22)$$

- 15 然后，计算下式：

$$d_1 = d \pmod{\phi(p)} \quad (23)$$

$$d_2 = d \pmod{\phi(q)} \quad (24)$$

$$z_1 = x_1^{d_1} \pmod{p, r} \quad (25)$$

$$z_1 = x_1^{d_1} \pmod{q, s} \quad (26)$$

- 20 $C_1 = b_1^{d_1} \pmod{r} \quad (27)$

$$C_2 = b_2^{d_2} \pmod{s} \quad (28)$$

为了节省计算时间，在分别进行以 $\phi(r)$ 和 $\phi(s)$ 对模的取幂之前，可以还原式 (27) 和 (28) 中的指数 d_1 和 d_2 。

从式 (23) 和 (25) 有：

- 25 $z_1 = x^{d_1} \pmod{p} \quad (29)$

从 (24) 和 (26) 有：

$$z_2 = x^{d_2} \pmod{q} \quad (30)$$

按照中国余数定理，由 z_1 和 z_2 可以容易地计算数 z ：

$$z = z_1 \pmod{p, r}; z = z_2 \pmod{q, s}; \quad (31)$$

- 30 即使 r 和 s 相对地不是素数，所述数 z 也是存在的，这是因为 $z_1 = C_1 = b_1^{d_1} = b_2^{d_2} = C_2 = z_2 \pmod{\text{ggAT}(r, s)}$ 。因为 p 和 q 相对地是素数，由式 (29)、

(30) 和 (31) 有:

$$z = x^d \pmod{p \cdot q} \quad (32)$$

因此, 由上述计算的值可以容易地确定所求的数 z 。

由式 (21)、(25) 和 (27) 有:

5 $z_1 = C_1 \pmod{r} \quad (33)$

由式 (22)、(26) 和 (28) 有:

$$z_2 = C_2 \pmod{s} \quad (34)$$

通过检查条件 (33) 和 (34), 可以以高的几率确定错误。如果条件 (33) 或 (34) 中的一个被破坏, 则模的取幂的结果被认为是错误的, 因而被丢弃。

10 按照文件 W0-A1-98/52319 的权利要求 8 所述的方法, 数 b_1 和 b_2 不依赖于其中所述的方法的改型中的底数 x 。当应用 RSA 方法或拉比特征方法时, 私人密钥一般被集中在曾经被使用过若干次的加密装置例如智能卡中。在这些方法中应用的模的取幂中, 指数 d 和模数 $p \cdot q$ 是私人密钥的固定元素。因而, 值 C_1 和 C_2 在加密装置中进行密钥积分时必须只计算一次, 并且然后可
15 以被存储在所述装置中。和文件 W0-A1-98/52319 所述的方法相比, 存储这些值使得节省两次模的取幂运算。

在通常的实施例中, 一种具有用于加快模的算法的附加的硬件的加密装置, 例如智能卡, 含有快速的加法与/或乘法单元, 同时通常的标准的方法必须进行在模的还原中所需的由一个长的数的除法, 例如由 Donald Knuth:

20 “The Art of Computer Programming,” Volume 2: Seminumerical Algorithms, 2nd Ed., Addison-Wesley, 1981 得知的。用于简化除法操作的若干已知的方法之一是在取幂之前由数 r 乘模数 p , 使得乘积 $p \cdot r$ 的二进制表示包含尽可能多的数, 例如见 Menezes et al., *ibid.*, pages 598-599。由一个尽可能多超前的数去除比由一般的数去除简单得多。

25 按照本发明, 选择乘数 r , 使得 d 对于 $\phi(r)$ 相对地是素数。在上述的本发明的改型中, 不需要这种相对的素数性。对于每个模数 p , 具有一个取决于除法的特定技术实现的最佳的乘数 r_{opt} 。如果 r 的选择的值略小于优化的值, 则乘积 $p \cdot r$ 仍然含有足够超前的数, 从而使得除法能够简单地进行。按高的机率, 数 d 对于至少一个值 $\phi(r_{opt}-i)$ 相对地是素数, 其中 $i=1, \dots, k$,
30 其中 k 是依赖于实施的一个小的数。

如果不是这种情况, 则使 r 被 $2^i \cdot r$ 代替, 其中 2^i 根据实施是一个 2 的

合适的幂。

因而，对于第二个素数因数 q 可以应用同样的代替。因为可以选择乘数 r （对于 p ），和 s （对于 q ）彼此独立，对于乘数 s 可以同样进行相应的选择。