

[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 00817730.9

[45] 授权公告日 2008 年 4 月 9 日

[11] 授权公告号 CN 100380862C

[22] 申请日 2000.9.29 [21] 申请号 00817730.9  
[30] 优先权

[32] 1999.10.1 [33] FR [31] 99/12465  
[32] 1999.10.1 [33] FR [31] 99/12467  
[32] 1999.10.1 [33] FR [31] 99/12468  
[32] 2000.7.21 [33] FR [31] 00/09644

[86] 国际申请 PCT/FR2000/002717 2000.9.29

[87] 国际公布 WO2001/026279 法 2001.4.12

[85] 进入国家阶段日期 2002.5.16

[73] 专利权人 法国电信公司

地址 法国巴黎

共同专利权人 法国电视传播公司

马思·里兹克

[72] 发明人 路易斯·吉卢 让-雅克·吉斯卡特

[56] 参考文献

WO9633567A 1996.10.24

EP0792044A 1997.8.27

EP0381523A 1990.8.8

审查员 王桂霞

[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 赵科

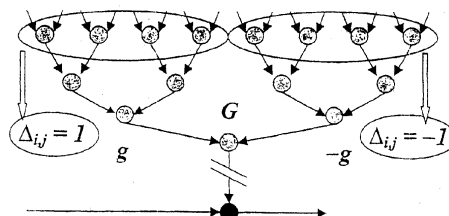
权利要求书 8 页 说明书 52 页 附图 3 页

[54] 发明名称

验证实体真实性或消息完整性的方法、系统、设备

[57] 摘要

本发明涉及一个通过以下数值进行证明的方法： $m(\geq 1)$  对私有数值  $Q_i$  和公开数值  $G_i = g_i^2$ ；一个由  $f(\geq 2)$  个素数的乘积构成的公开模数  $n$ ；一个满足以下类型关系的指数  $v = 2^k (k > 1)$ ： $G_j \cdot Q_i^v \equiv 1 \pmod n$  或  $G_j \equiv Q_i^v \pmod n$ 。在通过把  $Q_i$  或其反置模数  $n$  提高成以  $n$  为模以  $k-1$  为秩的乘方获得的  $m$  个数值中有至少一个不同于  $\pm g_i$ 。在  $2m$  个等式中： $x^2 \equiv g_i \pmod n$ ， $x^2 \equiv -g_i \pmod n$ ，其中至少有一个在以  $n$  为模的整数环中有  $x$  的解。



1.一种用于利用非对称密钥提供真实性或完整性的计算机实现方法, 包括:

获取一个或多个私有数值  $Q_1, Q_2, \dots, Q_m$  和相应的公开数值  $G_1, G_2, \dots, G_m$  的集合, 每对密钥  $(Q_i, G_i)$  验证等式  $G_i \cdot Q_i^v \equiv 1 \pmod n$  或等式  $G_i \equiv Q_i^v \pmod n$ , 其中  $m$  是大于或等于1的整数,  $i$  是1和 $m$ 之间的整数, 其中 $n$ 是等于由  $p_1, \dots, p_f$  所指定的 $f$ 个私有素数的乘积的公开整数, 这些素数中的至少两个相互不同, 其中 $f$ 是大于1的整数,  $v$ 是公开指数, 使得  $v=2^k$ , 其中 $k$ 是具有大于1的整数值的参数; 其中每个公开数值  $G_i$  (对于  $i=1, \dots, m$ ) 使得  $G_i \equiv g_i^2 \pmod n$ , 其中  $g_i$  (对于  $i=1, \dots, m$ ) 是具有大于1且小于每个素数  $p_1, \dots, p_f$  的整数值的基数; 其中对于1和 $m$ 之间的至少一个整数值  $l$ ,  $g_l$  或  $(-g_l)$  是以  $n$  为模的整数环的二次余数, 其中对于1和 $m$ 之间的至少一个整数值  $s$ ,  $q_s$  不与  $g_s \pmod n$  同余, 也不与  $(-g_s) \pmod n$  同余, 其中对于  $i=1, \dots, m$ , 如果  $G_i \times Q_i^v = 1 \pmod n$ , 则  $q_i \equiv Q_i^{-v/2} \pmod n$ , 而如果  $G_i = Q_i^v \pmod n$ , 则  $q_i \equiv Q_i^{v/2} \pmod n$ ;

从证明者接收确认  $R$ , 确认  $R$  具有的计算值使得  $R = r^v \pmod n$ , 其中  $r$  是证明者随机选择的整数且  $0 < r < n$ ;

随机地选择  $m$  个质问  $d_1, d_2, \dots, d_m$ ;

将质问  $d_1, d_2, \dots, d_m$  发送到证明者;

从证明者接收应答  $D$ , 应答  $D$  具有的计算值使得:  $D = r \times Q_1^{d_1} \times Q_2^{d_2} \times \dots \times Q_m^{d_m} \pmod n$ ; 以及

如果应答  $D$  具有的值使得  $D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times \dots \times G_m^{\varepsilon_m d_m} \pmod n$  等于确认  $R$ , 则确定证明者是可信的, 其中对于  $i=1, \dots, m$ , 如果  $G_i \times Q_i^v = 1 \pmod n$ , 则  $\varepsilon_i = +1$ , 而如果  $G_i = Q_i^v \pmod n$ , 则  $\varepsilon_i = -1$ 。

2. 一种用于利用非对称密钥提供真实性或完整性的计算机实现方法, 包括:

获取一个或多个私有数值  $Q_1, Q_2, \dots, Q_m$  和相应的公开数值  $G_1, G_2, \dots, G_m$  的集合, 每对密钥  $(Q_i, G_i)$  验证等式  $G_i \cdot Q_i^v \equiv 1 \pmod n$  或

等式  $G_i \equiv Q_i^v \pmod{n}$ , 其中  $m$  是大于或等于1的整数,  $i$  是1和  $m$  之间的整数, 其中  $n$  是等于由  $p_1, \dots, p_f$  所指定的  $f$  个私有素数的乘积的公开整数, 这些素数中的至少两个相互不同, 其中  $f$  是大于1的整数,  $v$  是公开指数, 使得  $v=2^k$ , 其中  $k$  是具有大于1的整数值的的安全参数; 其中每个公开数值  $G_i$  (对于  $i=1, \dots, m$ ) 使得  $G_i \equiv g_i^2 \pmod{n}$ , 其中  $g_i$  (对于  $i=1, \dots, m$ ) 是具有大于1且小于每个素数  $p_1, \dots, p_f$  的整数值的基数; 其中对于1和  $m$  之间的至少一个整数值  $l$ ,  $g_l$  或  $(-g_l)$  是以  $n$  为模的整数环的二次余数, 其中对于1和  $m$  之间的至少一个整数值  $s$ ,  $q_s$  不与  $g_s \pmod{n}$  同余, 也不与  $(-g_s) \pmod{n}$  同余, 其中对于  $i=1, \dots, m$ , 如果  $G_i \times Q_i^v = 1 \pmod{n}$ , 则  $q_i \equiv Q_i^{-v/2} \pmod{n}$ , 而如果  $G_i = Q_i^v \pmod{n}$ , 则  $q_i = Q_i^{v/2} \pmod{n}$ ;

从证明者接收确认  $R$ , 确认  $R$  具有利用中国余数方法由一组确认分量  $R_j$  而计算的值, 其中  $j=1, \dots, f$ , 每个确认分量  $R_j$  具有的值使得  $R_j = r_j^v \pmod{p_j}$ , 其中  $r_j$  是证明者随机选择的整数使得  $0 < r_j < p_j$ ;

随机地选择  $m$  个质问  $d_1, d_2, \dots, d_m$ ;

将质问  $d_1, d_2, \dots, d_m$  发送到证明者;

从证明者接收应答  $D$ , 其中利用中国余数方法由一组应答分量  $D_j$  计算应答  $D$ , 应答分量  $D_j$  具有的值使得: 对于  $j=1, \dots, f$ ,  $D_j = r_j \times Q_{1,j}^{d_1} \times Q_{2,j}^{d_2} \times \dots \times Q_{m,j}^{d_m} \pmod{p_j}$ , 其中对于  $i=1, \dots, m$  和  $j=1, \dots, f$ ,  $Q_{i,j} = Q_i \pmod{p_j}$ , 以及

如果应答  $D$  具有的值使得  $D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times \dots \times G_m^{\varepsilon_m d_m} \pmod{n}$  等于确认  $R$ , 则确定证明者是可信的, 其中对于  $i=1, \dots, m$ , 如果  $G_i \times Q_i^v = 1 \pmod{n}$ , 则  $\varepsilon_i = +1$ , 而如果  $G_i = Q_i^v \pmod{n}$ , 则  $\varepsilon_i = -1$ 。

3. 一种用于利用非对称密钥提供真实性或完整性的计算机实现方法, 包括:

获取一个或多个私有数值  $Q_1, Q_2, \dots, Q_m$  和相应的公开数值  $G_1, G_2, \dots, G_m$  的集合, 每对密钥  $(Q_i, G_i)$  验证等式  $G_i \cdot Q_i^v \equiv 1 \pmod{n}$  或等式  $G_i \equiv Q_i^v \pmod{n}$ , 其中  $m$  是大于或等于1的整数,  $i$  是1和  $m$  之间的整数, 其中  $n$  是等于由  $p_1, \dots, p_f$  所指定的  $f$  个私有素数的乘积的公开整数, 这些素数中的至少两个相互不同, 其中  $f$  是大于1的整数,  $v$  是公开指数,

使得 $v=2^k$ , 其中 $k$ 是具有大于1的整数值的安全参数; 其中每个公开数值 $G_i$  (对于 $i=1, \dots, m$ ) 使得 $G_i \equiv g_i^2 \pmod n$ , 其中 $g_i$  (对于 $i=1, \dots, m$ ) 是具有大于1且小于每个素数 $p_1, \dots, p_r$ 的整数值的基数; 其中对于1和 $m$ 之间的至少一个整数 $l$ ,  $g_l$ 或 $(-g_l)$ 是以 $n$ 为模的整数环的二次余数, 其中对于1和 $m$ 之间的至少一个整数 $s$ ,  $q_s$ 不与 $g_s \pmod n$ 同余, 也不与 $(-g_s) \pmod n$ 同余, 其中对于 $i=1, \dots, m$ , 如果 $G_i \times Q_i^v = 1 \pmod n$ , 则 $q_i \equiv Q_i^{-v/2} \pmod n$ , 而如果 $G_i = Q_i^v \pmod n$ , 则 $q_i = Q_i^{v/2} \pmod n$ ;

从证明者接收令牌 $T$ , 其中令牌 $T$ 具有的值使得 $T=h(M, R)$ , 其中 $h$ 是散列函数,  $M$ 是从证明者所接收的消息,  $R$ 是这样的确认, 其具有的计算值使得:  $R=r^v \pmod n$ , 其中 $r$ 是证明者随机选择的整数, 使得 $0 < r < n$ ;

随机地选择 $m$ 个质问 $d_1, d_2, \dots, d_m$ ;

将质问 $d_1, d_2, \dots, d_m$ 发送到证明者;

从证明者接收应答 $D$ , 其中应答 $D$ 具有的值使得:  $D = r \times Q_1^{d_1} \times Q_2^{d_2} \times \dots \times Q_m^{d_m} \pmod n$ ; 以及

如果应答 $D$ 具有的值使得 $h(M, D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times \dots \times G_m^{\varepsilon_m d_m} \pmod n)$ 等于令牌 $T$ , 则确定消息 $M$ 是可信的, 其中对于 $i=1, \dots, m$ , 如果 $G_i \times Q_i^v = 1 \pmod n$ , 则 $\varepsilon_i = +1$ , 而如果 $G_i = Q_i^v \pmod n$ , 则 $\varepsilon_i = -1$ 。

4. 一种用于利用非对称密钥提供真实性或完整性的计算机实现方法, 包括:

获取一个或多个私有数值 $Q_1, Q_2, \dots, Q_m$ 和相应的公开数值 $G_1, G_2, \dots, G_m$ 的集合, 每对密钥 $(Q_i, G_i)$ 验证等式 $G_i \cdot Q_i^v \equiv 1 \pmod n$ 或等式 $G_i \equiv Q_i^v \pmod n$ , 其中 $m$ 是大于或等于1的整数,  $i$ 是1和 $m$ 之间的整数, 其中 $n$ 是等于由 $p_1, \dots, p_r$ 所指定的 $f$ 个私有素数的乘积的公开整数, 这些素数中的至少两个相互不同, 其中 $f$ 是大于1的整数,  $v$ 是公开指数, 使得 $v=2^k$ , 其中 $k$ 是具有大于1的整数值的安全参数; 其中每个公开数值 $G_i$  (对于 $i=1, \dots, m$ ) 使得 $G_i \equiv g_i^2 \pmod n$ , 其中 $g_i$  (对于 $i=1, \dots, m$ ) 是具有大于1且小于每个素数 $p_1, \dots, p_r$ 的整数值的基数; 其中对于1和 $m$ 之间的至少一个整数 $l$ ,  $g_l$ 或 $(-g_l)$ 是以 $n$ 为模的整数环的二次余数, 其中

对于1和m之间的至少一个整数值s,  $q_s$ 不与 $g_s \bmod n$ 同余, 也不与 $(-g_s) \bmod n$ 同余, 其中对于 $i=1, \dots, m$ , 如果 $G_i \times Q_i^v = 1 \bmod n$ , 则 $q_i \equiv Q_i^{-v/2} \bmod n$ , 而如果 $G_i = Q_i^v \bmod n$ , 则 $q_i = Q_i^{v/2} \bmod n$ ;

从证明者接收令牌T, 其中令牌T具有的值使得 $T=h(M, R)$ , 其中h是散列函数, M是从证明者所接收的消息, R是具有利用中国余数方法由一组确认分量 $R_j$ 所计算的值的确认, 其中 $j=1, \dots, f$ , 每个确认分量 $R_j$ 具有的值使得 $R_j = r_j^v \bmod p_j$ , 其中 $r_j$ 是证明者随机选择的整数使得 $0 < r_j < p_j$ ;

随机地选择m个质问 $d_1, d_2, \dots, d_m$ ;

将质问 $d_1, d_2, \dots, d_m$ 发送到证明者;

从证明者接收应答D, 其中利用中国余数方法由一组应答分量 $D_j$ 计算应答D, 应答分量 $D_j$ 具有的值使得: 对于 $j=1, \dots, f$ ,  $D_j = r_j \times Q_{1j}^{d_1} \times Q_{2j}^{d_2} \times \dots \times Q_{mj}^{d_m} \bmod p_j$ , 其中对于 $i=1, \dots, m$ 和 $j=1, \dots, f$ ,  $Q_{ij} = Q_i \bmod p_j$ , 以及

如果应答D具有的值使得 $h(M, D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times \dots \times G_m^{\varepsilon_m d_m} \bmod n)$ 等于令牌T, 则确定消息M是可信的, 其中对于 $i=1, \dots, m$ , 如果 $G_i \times Q_i^v = 1 \bmod n$ , 则 $\varepsilon_i = +1$ , 而如果 $G_i = Q_i^v \bmod n$ , 则 $\varepsilon_i = -1$ 。

5.如权利要求1至4中任一项所述的计算机实现方法, 其中每个质问 $d_i$  (对于 $i=1, \dots, m$ ) 取从0到 $(2^k-1)$ 的值。

6.一种用于利用非对称密钥提供真实性或完整性的计算机系统, 包括:

用于获取一个或多个私有数值 $Q_1, Q_2, \dots, Q_m$ 和相应的公开数值 $G_1, G_2, \dots, G_m$ 的集合的装置, 每对密钥 $(Q_i, G_i)$ 验证等式 $G_i \cdot Q_i^v \equiv 1 \bmod n$ 或等式 $G_i \equiv Q_i^v \bmod n$ , 其中m是大于或等于1的整数, i是1和m之间的整数, 其中n是等于由 $p_1, \dots, p_f$ 所指定的f个素数的乘积的公开整数, 这些素数中的至少两个相互不同, 其中f是大于1的整数, 其中v是公开指数, 使得 $v=2^k$ , 其中k是具有大于1的整数值的安全参数; 其中每个公开数值 $G_i$  (对于 $i=1, \dots, m$ ) 使得 $G_i \equiv g_i^2 \bmod n$ , 其中 $g_i$  (对于 $i=1, \dots, m$ ) 是具有大于1且小于每个素数 $p_1, \dots, p_f$ 的整数值的基数; 其中对于1和m

之间的至少一个整数值 $l$ ,  $g_i$ 或 $(-g_i)$ 是以 $n$ 为模的整数环的二次余数, 其中对于 $1$ 和 $m$ 之间的至少一个整数值 $s$ ,  $q_s$ 不与 $g_s \bmod n$ 同余, 也不与 $(-g_s) \bmod n$ 同余, 其中对于 $i=1, \dots, m$ , 如果 $G_i \times Q_i^v = 1 \bmod n$ , 则 $q_i \equiv Q_i^{-v/2} \bmod n$ , 而如果 $G_i = Q_i^v \bmod n$ , 则 $q_i \equiv Q_i^{v/2} \bmod n$ ;

用于从证明者接收确认 $R$ 的装置, 确认 $R$ 具有的计算值使得 $R = r^v \bmod n$ , 其中  $r$ 是证明者随机选择的整数且 $0 < r < n$ ;

用于随机地选择 $m$ 个质问 $d_1, d_2, \dots, d_m$ 的装置;

用于将质问 $d_1, d_2, \dots, d_m$ 发送到证明者的装置;

用于从证明者接收应答 $D$ 的装置, 应答 $D$ 具有的计算值使得:  $D = r \times Q_1^{d_1} \times Q_2^{d_2} \times \dots \times Q_m^{d_m} \bmod n$ ; 以及

用于如果应答 $D$ 具有的值使得  $D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times \dots \times G_m^{\varepsilon_m d_m} \bmod n$  等于确认 $R$ , 则确定证明者是可信的装置, 其中对于 $i=1, \dots, m$ , 如果 $G_i \times Q_i^v = 1 \bmod n$ , 则 $\varepsilon_i = +1$ , 而如果 $G_i = Q_i^v \bmod n$ , 则 $\varepsilon_i = -1$ 。

7. 一种用于利用非对称密钥提供真实性或完整性的计算机系统, 包括:

用于获取一个或多个私有数值 $Q_1, Q_2, \dots, Q_m$ 和相应的公开数值 $G_1, G_2, \dots, G_m$  的集合的装置, 每对密钥 $(Q_i, G_i)$ 验证等式 $G_i \cdot Q_i^v \equiv 1 \bmod n$ 或等式 $G_i \equiv Q_i^v \bmod n$ , 其中 $m$ 是大于或等于 $1$ 的整数,  $i$ 是 $1$ 和 $m$ 之间的整数, 其中 $n$ 是等于由 $p_1, \dots, p_f$ 所指定的 $f$ 个私有素数的乘积的公开整数, 这些素数中的至少两个相互不同, 其中 $f$ 是大于 $1$ 的整数,  $v$ 是公开指数, 使得 $v=2^k$ , 其中 $k$ 是具有大于 $1$ 的整数值的的安全参数; 其中每个公开数值 $G_i$  (对于 $i=1, \dots, m$ )使得 $G_i \equiv g_i^2 \bmod n$ , 其中 $g_i$  (对于 $i=1, \dots, m$ )是具有大于 $1$ 且小于每个素数 $p_1, \dots, p_f$ 的整数值的基数; 其中对于 $1$ 和 $m$ 之间的至少一个整数值 $l$ ,  $g_l$ 或 $(-g_l)$ 是以 $n$ 为模的整数环的二次余数, 其中对于 $1$ 和 $m$ 之间的至少一个整数值 $s$ ,  $q_s$ 不与 $g_s \bmod n$ 同余, 也不与 $(-g_s) \bmod n$ 同余, 其中对于 $i=1, \dots, m$ , 如果 $G_i \times Q_i^v = 1 \bmod n$ , 则 $q_i \equiv Q_i^{-v/2} \bmod n$ , 而如果 $G_i = Q_i^v \bmod n$ , 则 $q_i \equiv Q_i^{v/2} \bmod n$ ;

用于从证明者接收确认 $R$ 的装置, 确认 $R$ 具有利用中国余数方法由一组确认分量 $R_j$ 而计算的值, 其中 $j=1, \dots, f$ , 每个确认分量 $R_j$ 具有的值

使得  $R_j = r_j^v \bmod p_j$ , 其中  $r_j$  是证明者随机选择的整数使得  $0 < r_j < p_j$ ;

用于随机地选择  $m$  个质问  $d_1, d_2, \dots, d_m$  的装置;

用于将质问  $d_1, d_2, \dots, d_m$  发送到证明者的装置;

用于从证明者接收应答  $D$  的装置, 其中利用中国余数方法由一组应答分量  $D_j$  计算应答  $D$ , 应答分量  $D_j$  具有的值使得: 对于  $j=1, \dots, f$ ,  $D_j = r_j \times Q_{1,j}^{d_1} \times Q_{2,j}^{d_2} \times \dots \times Q_{m,j}^{d_m} \bmod p_j$ , 其中对于  $i=1, \dots, m$  和  $j=1, \dots, f$ ,  $Q_{i,j} = Q_i \bmod p_j$ , 以及

用于如果应答  $D$  具有的值使得  $D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times \dots \times G_m^{\varepsilon_m d_m} \bmod n$  等于确认  $R$ , 则确定证明者是可信的装置, 其中对于  $i=1, \dots, m$ , 如果  $G_i \times Q_i^v = 1 \bmod n$ , 则  $\varepsilon_i = +1$ , 而如果  $G_i = Q_i^v \bmod n$ , 则  $\varepsilon_i = -1$ .

8. 一种用于利用非对称密钥提供真实性或完整性的计算机系统, 包括:

用于获取一个或多个私有数值  $Q_1, Q_2, \dots, Q_m$  和相应的公开数值  $G_1, G_2, \dots, G_m$  的集合的装置, 每对密钥  $(Q_i, G_i)$  验证等式  $G_i \cdot Q_i^v \equiv 1 \bmod n$  或等式  $G_i \equiv Q_i^v \bmod n$ , 其中  $m$  是大于或等于1的整数,  $i$  是1和  $m$  之间的整数, 其中  $n$  是等于由  $p_1, \dots, p_f$  所指定的  $f$  个私有素数的乘积的公开整数, 这些素数中的至少两个相互不同, 其中  $f$  是大于1的整数,  $v$  是公开指数, 使得  $v=2^k$ , 其中  $k$  是具有大于1的整数值的安全参数; 其中每个公开数值  $G_i$  (对于  $i=1, \dots, m$ ) 使得  $G_i \equiv g_i^2 \bmod n$ , 其中  $g_i$  (对于  $i=1, \dots, m$ ) 是具有大于1且小于每个素数  $p_1, \dots, p_f$  的整数值的基数; 其中对于1和  $m$  之间的至少一个整数值  $l$ ,  $g_l$  或  $(-g_l)$  是以  $n$  为模的整数环的二次余数, 其中对于1和  $m$  之间的至少一个整数值  $s, q_s$  不与  $g_s \bmod n$  同余, 也不与  $(-g_s) \bmod n$  同余, 其中对于  $i=1, \dots, m$ , 如果  $G_i \times Q_i^v = 1 \bmod n$ , 则  $q_i \equiv Q_i^{-v/2} \bmod n$ , 而如果  $G_i = Q_i^v \bmod n$ , 则  $q_i = Q_i^{v/2} \bmod n$ ;

用于从证明者接收令牌  $T$  的装置, 其中令牌  $T$  具有的值使得  $T = h(M, R)$ , 其中  $h$  是散列函数,  $M$  是从证明者所接收的消息,  $R$  是这样的确认, 其具有的计算值使得:  $R = r^v \bmod n$ , 其中  $r$  是证明者随机选择的整数, 使得  $0 < r < n$ ;

用于随机地选择  $m$  个质问  $d_1, d_2, \dots, d_m$  的装置;

用于将质问 $d_1, d_2, \dots, d_m$ 发送到证明者的装置;

用于从证明者接收应答D的装置, 其中应答D具有的值使得:  $D = r \times Q_1^{d_1} \times Q_2^{d_2} \times \dots \times Q_m^{d_m} \bmod n$ ; 以及

用于如果应答D具有的值使得  $h(M, D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times \dots \times G_m^{\varepsilon_m d_m} \bmod n)$  等于令牌T, 则确定消息M是可信的装置, 其中对于 $i=1, \dots, m$ , 如果  $G_i \times Q_i^v = 1 \bmod n$ , 则  $\varepsilon_i = +1$ , 而如果  $G_i = Q_i^v \bmod n$ , 则  $\varepsilon_i = -1$ 。

9. 一种用于利用非对称密钥提供真实性或完整性的计算机系统, 包括:

用于获取一个或多个私有数值 $Q_1, Q_2, \dots, Q_m$ 和相应的公开数值 $G_1, G_2, \dots, G_m$ 的集合的装置, 每对密钥 $(Q_i, G_i)$ 验证等式 $G_i \cdot Q_i^v \equiv 1 \bmod n$ 或等式 $G_i \equiv Q_i^v \bmod n$ , 其中 $m$ 是大于或等于1的整数,  $i$ 是1和 $m$ 之间的整数, 其中 $n$ 是等于由 $p_1, \dots, p_r$ 所指定的 $f$ 个私有素数的乘积的公开整数, 这些素数中的至少两个相互不同, 其中 $f$ 是大于1的整数,  $v$ 是公开指数, 使得 $v=2^k$ , 其中 $k$ 是具有大于1的整数值的的安全参数; 其中每个公开数值 $G_i$  (对于 $i=1, \dots, m$ ) 使得 $G_i \equiv g_i^2 \bmod n$ , 其中 $g_i$  (对于 $i=1, \dots, m$ ) 是具有大于1且小于每个素数 $p_1, \dots, p_r$ 的整数值的基数; 其中对于1和 $m$ 之间的至少一个整数值 $l$ ,  $g_l$ 或 $(-g_l)$ 是以 $n$ 为模的整数环的二次余数, 其中对于1和 $m$ 之间的至少一个整数值 $s, q_s$ 不与 $g_s \bmod n$ 同余, 也不与 $(-g_s) \bmod n$ 同余, 其中对于 $i=1, \dots, m$ , 如果  $G_i \times Q_i^v = 1 \bmod n$ , 则  $q_i \equiv Q_i^{-v/2} \bmod n$ , 而如果  $G_i = Q_i^v \bmod n$ , 则  $q_i = Q_i^{v/2} \bmod n$ ;

用于从证明者接收令牌T的装置, 其中令牌T具有的值使得 $T=h(M, R)$ , 其中 $h$ 是散列函数,  $M$ 是从证明者所接收的消息,  $R$ 是具有利用中国余数方法由一组确认分量 $R_j$ 所计算的值的确认, 其中 $j=1, \dots, f$ , 每个确认分量 $R_j$ 具有的值使得 $R_j = r_j^v \bmod p_j$ , 其中 $r_j$ 是证明者随机选择的整数使得 $0 < r_j < p_j$ ;

用于随机地选择 $m$ 个质问 $d_1, d_2, \dots, d_m$ 的装置;

用于将质问 $d_1, d_2, \dots, d_m$ 发送到证明者的装置;

用于从证明者接收应答D的装置, 其中利用中国余数方法由一组应答分量 $D_j$ 计算应答D, 应答分量 $D_j$ 具有的值使得: 对于 $j=1, \dots, f$ ,  $D_j =$

$r_j \times Q_{1,j}^{d_1} \times Q_{2,j}^{d_2} \times \dots \times Q_{m,j}^{d_m} \bmod p_j$ , 其中对于  $i=1, \dots, m$  和  $j=1, \dots, f$ ,  $Q_{i,j} = Q_i \bmod p_j$ , 以及

用于如果应答D具有的值使得  $h(M, D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times \dots \times G_m^{\varepsilon_m d_m} \bmod n)$  等于令牌T, 则确定消息M是可信的装置, 其中对于  $i=1, \dots, m$ , 如果  $G_i \times Q_i^v = 1 \bmod n$ , 则  $\varepsilon_i = +1$ , 而如果  $G_i = Q_i^v \bmod n$ , 则  $\varepsilon_i = -1$ 。

10. 如权利要求 6 至 9 中任一项所述的计算机系统, 其中每个质问  $d_i$  (对于  $i=1, \dots, m$ ) 取从 0 到  $(2^k-1)$  的值。

11. 一种用于生成非对称加密密钥的计算机实现方法, 其中所属密钥包括  $m \geq 1$  个私有数值  $Q_1, Q_2, \dots, Q_m$  和  $m$  个相应的公开数值  $G_1, G_2, \dots, G_m$ , 所述计算机实现方法包括:

选择安全参数  $k$ , 其中  $k$  是大于 1 的整数;

确定模数  $n$ , 其中  $n$  是等于至少两个素数  $p_1, \dots, p_r$  的乘积的公开整数;

选择  $m$  个基数  $g_1, g_2, \dots, g_m$ , 其中每个基数  $g_i$  (对于  $i=1, \dots, m$ ) 具有大于 1 且小于每个素数  $p_1, \dots, p_r$  的整数值, 并且其中对于 1 和  $m$  之间的至少一个整数值  $l$ ,  $g_l$  或  $(-g_l)$  是以  $n$  为模的整数环的二次余数;

对于  $i=1, \dots, m$ , 通过  $G_i \equiv g_i^2 \bmod n$ , 计算公开数值  $G_i$ ; 以及

对于  $i=1, \dots, m$ , 通过求解等式  $G_i \times Q_i^v = 1 \bmod n$  或等式  $G_i = Q_i^v \bmod n$ , 计算私有数值  $Q_i$ , 其中公开指数  $v$  使得  $v=2^k$ , 使得对于 1 和  $m$  之间的至少一个整数值  $s$ ,  $q_s$  不与  $g_s \bmod n$  同余, 也不与  $(-g_s) \bmod n$  同余, 其中对于  $i=1, \dots, m$ , 如果  $G_i \times Q_i^v = 1 \bmod n$ , 则  $q_i \equiv Q_i^{-v/2} \bmod n$ , 而如果  $G_i = Q_i^v \bmod n$ , 则  $q_i \equiv Q_i^{v/2} \bmod n$ 。

## 验证实体真实性或消息 完整性的方法、系统、设备

### 技术领域

本发明涉及密码领域，更具体地说，本发明涉及验证实体真实性和/或消息的完整性和/或真实性的方法，系统，和设备。

### 背景技术

发明人为Louis Guillou和JeanJacques Quisquater的专利EP 0 311 470 B1描述了这种方法。此后将通过术语"GQ专利"或"GQ方法"表示他们的专利成果。此后术语"GQ2"，或"GQ2发明"或"GQ2技术"将被用来描述本发明。

根据GQ方法，一个被称为"委托机构"的实体为各个被称为"见证者"的实体分配一个身份并且计算其RSA签名。在定制过程中，委托机构为见证者指定一个身份和签名。其后，见证者声明："这是我的身份；我知道该身份的RSA签名"。见证者在不出示这个签名的情况下证明他知道其身份的RSA签名。通过委托机构分配的RSA公开鉴别密钥，一个被称为"控制者"的实体在没有获得其中的知识的情况下确定RSA签名对应于所声明的身份。使用GQ方法的机制在"不传送知识"的情况下运行。根据GQ方法，见证者不知道委托机构为大量身份签署的RSA私有密钥。

上述GQ技术利用了RSA技术。然而虽然RSA技术严重依赖模数 $n$ 的因数分解，但正如在针对实现RSA技术的各种数字签名标准的所谓"乘法攻击"中可以看到，这种依赖的不具等效性，并且实际上差别很大。

GQ2技术有双重目标：一方面，是改进RSA技术的性能特性，另一方面是避免RSA技术的固有问题。有关GQ2私有密钥的知识相当

于有关模数 $n$ 的因数分解的知识。任何对三元组GQ2的攻击均导致对模数 $n$ 的因数分解：此时存在等效性。使用 GQ2技术减少了签名或自认证实体以及控制者实体的工作负载。通过在安全和性能方面对因数分解问题的良好使用，GQ2技术避免了 RSA技术的缺点。

GQ方法实现了包括 512位或更多位数的数值取模计算。这些计算涉及具有基本相同的长度、高到以 $2^{16}+1$ 为指数的幂的数值。但是尤其是在银行卡领域中，现有的微电子基础设施均使用没有算术协处理器的可自编程单片微处理器。涉及诸如 GQ方法的方法中产生的多个算术应用的工作负载所需要的计算时间在某些情况下为使用银行卡支付其购买的客户带来不便。回顾以往，当试图增加支付卡的安全性时，银行机构提出了一个特别难以解决的问题。事实上，必须研究两个明显矛盾的问题：一方面，通过使用更加冗长和独特的密钥增加安全性，另一方面，防止工作负载为用户带来过长的计算时间。由于还有必要考虑到现有基础设施和现有微处理器部件，这个问题变得尤其尖锐。

GQ2技术的目标是提供一个能够解决这个问题并且仍然增加了安全性的解决方案。

## 发明内容

### 方法

更具体地，本发明涉及一个为控制者实体验证下列内容的方法：

- 一个实体的真实性和/或
- 与这个实体相关的消息 $M$ 的完整性。

通过所有或部分下列参数或这些参数的派生参数完成这个证明：

- $m$ 对私有数值 $Q_1, Q_2, \dots, Q_m$ 和公开数值 $G_1, G_2, \dots, G_m$  ( $m$ 大于或等于1)，

-由上述 $f$ 个素数 $p_1, p_2, \dots, p_f$  ( $f$ 大于或等于2)的乘积构成的一个公开模数 $n$ ，

上述模数，上述私有和公开数值有以下类型的关系：

$$G_i \cdot Q_i^V \equiv 1 \pmod{n} \text{ 或 } G_i \equiv Q_i^V \pmod{n}$$

其中  $v$  表示一个上述类型的公开指数

$$v = 2^k$$

其中  $k$  是大于1的安全参数,

上述  $m$  个公开数值  $G_i$  是少于  $f$  个素数  $p_1, p_2, \dots, p_f$  的  $m$  个基数  $g_1, g_2, \dots, g_m$  的平方  $g_i^2$ ; 通过满足下面的条件产生上述  $f$  个素数  $p_1, p_2, \dots, p_f$  和/或上述  $m$  个基数  $g_1, g_2, \dots, g_m$ 。

第一条条件

根据第一条条件, 各个等式

$$x^v \equiv g_i^2 \pmod{n}$$

在以  $n$  为模的整数环中有  $x$  的解。

第二条条件

根据第二条条件, 在  $G_i \equiv Q_i^v \pmod{n}$  成立的情况下, 在通过把  $Q_i$  提高成以  $n$  为模以  $k-1$  为秩的乘方获得的  $m$  个数值  $q_i$  中有一个  $q_i$  不同于  $\pm g_i$  (即有一个非无效解)。

根据第二条条件, 在  $G_i \cdot Q_i^v \equiv 1 \pmod{n}$  成立的情况下, 在通过把  $Q_i$  模  $n$  的反置提高成以  $n$  为模以  $k-1$  为秩的乘方获得的  $m$  个数值  $q_i$  中有一个  $q_i$  不同于  $\pm g_i$  (即有一个非无效解)。

这里应当注意, 根据当前的符号表示,  $\pm g_i$  表示数量  $g_i$  和  $n-g_i$ 。

第三条条件

根据第三条条件, 在  $2m$  个等式中间:

$$x^2 \equiv g_i \pmod{n} \quad (2)$$

$$x^2 \equiv -g_i \pmod{n} \quad (3)$$

其中至少有一个在以  $n$  为模的整数环中有  $x$  的解。

上述方法在下面定义的步骤中实现了被称作见证者的实体。上述见证者实体具有  $f$  个素数  $p_i$  和/或  $m$  个基数  $g_i$  和/或素数的中国余数的参数和/或公开模数  $n$  和/或  $m$  个私有数值  $Q_i$  和/或私有数值  $Q_i$  与公开指数  $v$  的  $f \cdot m$  个分量  $Q_{i,j}$  ( $Q_{i,j} \in \{Q_i \pmod{p_j}\}$ )。

见证者计算以  $n$  为模数的整数环中的质问 (commitment)  $R$ 。通过以下操作计算各个质问:

-执行下列类型的运算

$$R \equiv r^v \bmod n$$

其中  $r$  是一个随机数值并且  $0 < r < n$ ,

-或

\*\*通过执行下列类型的运算

$$R_i \equiv r_i^v \bmod p_i$$

其中  $r_i$  是一个与素数  $p_i$  相关的随机数值, 其中  $0 < r_i < p_i$ , 各个  $r_i$  属于一个随机数值集合  $\{r_1, r_2, \dots, r_t\}$ ,

\*\*接着使用中国余数方法。

见证者接收一或多个质问(challenge) $d$ 。每个质问 $d$ 包括 $m$ 个被称作基本质问的整数  $d_i$ 。根据各个质问 $d$ , 见证者通过执行以下类型的运算计算一个应答 $D$ ,

-或者通过执行下列类型的运算:

$$D \equiv r \cdot Q_1^{d_1} \cdot Q_2^{d_2} \cdot \dots \cdot Q_m^{d_m} \bmod n$$

-或者

\*\*通过执行下列类型的运算:

$$D_i \equiv r_i \cdot Q_{i,1}^{d_1} \cdot Q_{i,2}^{d_2} \cdot \dots \cdot Q_{i,m}^{d_m} \bmod p_i$$

\*\*接着使用中国余数方法。

该方法使得应答 $D$ 的数量与质问 $d$ 和确认 $R$ 一样多。 每给数值 $R$ ,  $d$ ,  $D$ 均构成一个被表示成 $\{R, d, D\}$ 的三元组。

证明一个实体的真实性的实例

在一个实施例的第一变型中, 基于本发明的方法被用来向一个被称为控制者的实体证明一个被称为证明者的实体的真实性。上述证明者实体包括见证者。 上述证明者和控制者实体执行下列步骤:

- 步骤1: 涉及确认 $R$ 的操作

每次见证者使用上述过程计算各个确认 $R$ 。 证明者向控制者发送所有或部分确认 $R$ 。

- 步骤2: 涉及质问 $d$ 的操作

在接收所有或部分确认R之后,控制者产生数量等于确认R的数量的质问d并且向证明者发送质问d。

- 步骤3: 涉及应答D的操作

见证者使用上述过程根据质问d计算应答D。

- 步骤4: 涉及检查的操作

证明者向控制者发送各个应答D。

**第一种情况: 证明者已经发送一部分确认R**

如果证明者已经发送一部分确认R,则控制者在具有m个公开数值 $G_1, G_2, \dots, G_m$ 的情况下根据各个质问d和各个应答D计算一个重构确认R',这个重构确认R'满足以下类型的关系

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \pmod{n}$$

或以下类型的关系

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \pmod{n}.$$

控制者确定各个重构的确认R'还原出已经发送过来的所有或部分确认R。

**第二种情况: 证明者已经全部发送确认R**

如果证明者已经发送全部确认R,则控制者在具有m个公开数值 $G_1, G_2, \dots, G_m$ 的情况下确定各个确认R满足以下类型的关系

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \pmod{n}$$

或以下类型的关系

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \pmod{n}.$$

**证明消息的完整性的案例**

在一个实施例的能够与其第一变型配合使用的第二变型中,基于本发明的方法被用来为被称为控制者实体的实体证明与被称为证明者实体的实体相关的消息M的完整性。上述证明者实体包括见证者。

上述证明者和控制者实体执行下列步骤:

- 步骤1: 涉及确认R的操作

每次见证者使用上述过程计算各个确认R。

- 步骤2: 涉及质问d的操作

证明者使用一个散列函数h计算至少一个令牌T, 其中散列函数的参数包括消息M和所有或部分确认R。证明者向控制者发送令牌T。在接收令牌T之后, 控制者产生数量等于确认R的数量的质问d并且向证明者发送质问d。

- 步骤3: 涉及应答D的操作

见证者使用上述过程根据质问d计算应答D。

- 步骤4: 涉及检查的操作

证明者向控制者发送各个应答D。控制者在具有m个公开数值 $G_1, G_2, \dots, G_m$ 的情况下根据各个质问d和各个应答D计算一个重构确认R', 这个重构确认R'满足以下类型的关系:

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \pmod{n}$$

或以下类型的关系

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \pmod{n}.$$

接着控制者使用一个散列函数h重构令牌T', 其中散列函数的参数包括消息M和所有或部分重构确认R'。接着控制者确定令牌T'与发送的令牌T相同。

## 消息的数字签名及其真实性证明

在基于本发明的一个实施例的能够与前面两个实施例配合使用的第三变型中, 基于本发明的方法被用来通过一个被称为签名实体的实体产生消息M的数字签名。上述签名实体包含见证者。

## 签名运算

上述签名实体执行签名运算以便获得包括以下内容的已签名消息:

-消息M,

-质问d和/或确认R,

-应答D。

上述签名实体通过实现下列步骤执行签名运算:

步骤1: 涉及确认R的操作

每次见证者使用上述过程计算各个确认R。

步骤2: 涉及质问d的操作

签名实体使用一个散列函数h获得一个二进制序列, 上述散列函数的参数包括消息M和各个确认R。签名实体从这个二进制序列中提取其数量等于确认R的数量的质问d。

\*步骤3: 涉及应答D的操作

见证者使用上述过程根据质问d计算应答D。

## 检查运算

为了验证消息M的真实性, 一个被称作控制者的实体检查已签名消息。具有已签名消息的上述控制者实体通过执行如下步骤来完成检查运算,

在控制者具有确认R, 质问d, 应答D的情况下

如果控制者具有确认R, 质问d, 应答D, 则控制者确定确认R, 质问d和应答D满足以下类型的关系:

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \bmod n$$

或以下类型的关系:

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \bmod n.$$

接着控制者确定消息M, 质问d和确认R满足散列函数:

$$d = h(\text{消息}, R)$$

在控制者具有质问d和应答D的情况下

如果控制者具有质问d和应答D, 控制者根据各个质问d和各个应答D重构满足以下类型的关系的确认R':

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \bmod n$$

或以下类型的关系:

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n.$$

接着控制者确定消息M和质问d满足散列函数:

$$d = h(\text{消息}, R')$$

在控制者具有确认R和应答D的情况下

如果控制者具有确认R和应答D, 则控制者使用散列函数并且重构d'

$$d' = h(\text{消息}, R).$$

接着控制者设备确定确认R, 质问d'和应答D满足以下类型的关系:

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

或以下类型的关系:

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n.$$

## 系统

本发明还涉及被用来向控制者服务器验证下列内容的系统:

- 一个实体的真实性和/或
- 与这个实体相关的消息M的完整性。

通过所有或部分下列参数或这些参数的派生参数完成这个证明:

-m对私有数值 $Q_1, Q_2, \dots, Q_m$ 和公开数值 $G_1, G_2, \dots, G_m$  (m大于或等于1),

-由上述f个素数 $p_1, p_2, \dots, p_f$  (f大于或等于2)的乘积构成的一个公开模数n,

上述模数, 上述私有和公开数值有以下类型的关系:

$$G_i \cdot Q_i^v \equiv 1 \text{ mod } n \text{ 或 } G_i \{ Q_i^v \text{ mod } n$$

其中 v表示一个下述类型的公开指数:

$$v=2^k$$

其中k是大于1的安全参数,

上述 m个公开数值 $G_i$ 是少于f个素数 $p_1, p_2, \dots, p_f$ 的 m个不同基数 $g_1, g_2, \dots, g_m$ 的平方 $g_i^2$ ; 产生上述 f个素数 $p_1, p_2, \dots, p_f$ 和/或上述 m个基数 $g_1, g_2, \dots, g_m$ 以满足下面的条件。

### 第一条件

根据第一条件, 各个等式:

$$x^v \equiv g_i^2 \pmod{n} \quad (1)$$

可以被以 $n$ 为模的整数环中的 $x$ 求解。

### 第二条件

根据第二条件, 在  $G_i \equiv Q_i^v \pmod{n}$  成立的情况下, 在通过把  $Q_i$  提高成以 $n$ 为模以 $k-1$ 为秩的乘方获得的  $m$ 个数值  $q_i$ 中有一个  $q_i$ 不同于  $\pm g_i$  (即有一个非无效解)。

根据第二条件, 在  $G_i \cdot Q_i^v \equiv 1 \pmod{n}$  成立的情况下, 在通过把  $Q_i$  模 $n$ 的反置提高成以 $n$ 为模以 $k-1$ 为秩的乘方获得的  $m$ 个数值  $q_i$ 中有一个  $q_i$ 不同于  $\pm g_i$  (即有一个非无效解)。

这里应当指出, 根据当前的符号表示,  $\pm g_i$ 表示数量  $g_i$ 和 $n-g_i$ 。

### 第三条件

根据第三条件, 在  $2m$ 个等式中间:

$$x^2 \equiv g_i \pmod{n} \quad (2)$$

$$x^2 \equiv -g_i \pmod{n} \quad (3)$$

其中至少有一个可以被以 $n$ 为模的整数环中的 $x$ 求解。

上述系统包括一个见证者设备, 尤其是被包含在诸如基于微处理器的银行卡形式的漫游对象中的设备。见证者设备包括一个存储器区段, 上述存储器区段包含 $f$ 个素数  $p_i$ 和/或素数的中国余数的参数和/或公开模数 $n$ 和/或 $m$ 个私有数值  $Q_i$ 和/或私有数值  $Q_i$ 与公开指数 $v$ 的 $f \cdot m$ 个分量 $Q_{i,j}$  ( $Q_{i,j} \equiv Q_i \pmod{p_j}$ )。见证者设备还包括:

-随机数值产品装置, 此后被称作见证者设备的随机数值产生装置,

-计算装置, 此后被称作见证者设备计算确认 $R$ 的装置。

计算装置使得能够计算以 $n$ 为模数的整数环中的确认 $R$ 。通过以

下方式计算各个确认

执行下列类型的运算:

$$R \equiv r^v \bmod n$$

其中  $r$  是随机数产生装置产生的随机数值, 并且  $0 < r < n$ ; 或者  
执行下列类型的运算

$$R_i \equiv r_i^v \bmod p_i$$

其中  $r_i$  是一个与素数  $p_i$  相关的随机数值, 其中  $0 < r_i < p_i$ , 各个  $r_i$  属于一个由随机数值产生装置产生的随机数值集合  $\{r_1, r_2, \dots, r_t\}$ , 并且接着使用中国余数方法。

见证者设备还包括:

-接收装置, 此后被称作接收见证者设备的质问  $d$  的装置, 上述接收装置接收一或多个质问  $d$ ; 每个质问  $d$  均包括  $m$  个此后被称作基本质问的整数  $d_i$ 。

-计算装置, 此后被称作计算见证者设备的应答  $D$  的装置, 上述计算根据各个质问  $d$  计算以下类型的应答  $D$ :

完成下列类型的运算:

$$D \equiv r \cdot Q_1^{d_1} \cdot Q_2^{d_2} \cdot \dots \cdot Q_m^{d_m} \bmod n$$

或者, 完成下列类型的运算:

$$D_i \equiv r_i \cdot Q_{i,1}^{d_1} \cdot Q_{i,2}^{d_2} \cdot \dots \cdot Q_{i,m}^{d_m} \bmod p_i$$

并且接着使用中国余数方法。

见证者设备还包括发送一或多个确认  $R$  和一或多个应答  $D$  的发送装置。应答  $D$  的数量与质问  $d$  和确认  $R$  一样多, 其中每组数值  $R, d, D$  构成一个被表示成  $\{R, d, D\}$  的三元组。

证明一个实体的真实性的实例

在实施例的第一变型中, 基于本发明的系统被用来向一个被称为控制者的实体证明一个被称为证明者的实体的真实性。

上述系统包括一个与证明者实体相关的证明者设备。上述证明者设备通过互连装置与见证者设备互连。尤其可以采取漫游对象中的逻

辑微电路的形式，例如基于微处理器的银行卡中的微处理器的形式。

上述系统还包括一个与控制者实体相关的控制者设备。上述控制者设备尤其可以采取终端或远程服务器的形式。上述控制者设备包括连接装置以便通过电子、电磁、光学或声学方式，尤其是通过计算机通信网络连接至证明者设备。

上述系统被用来执行下列步骤：

#### 步骤1：涉及确认R的操作

每次见证者设备的计算确认R的装置使用上述过程计算各个确认R。见证者设备包括通过互连装置向证明者设备发送所有或部分确认R的发送装置，此后被称作见证者设备的发送装置。证明者设备还包括通过连接装置向控制者设备发送所有或部分确认R的发送装置，此后被称作证明者的发送装置。

#### 步骤2：涉及质问d的操作

控制者设备包括质问产生装置，该装置在接收所有或部分确认R之后产生数量等于确认R的数量的质问d。控制者设备还包括通过连接装置向证明者发送所有或部分质问d的发送装置，此后被称作控制者的发送装置。

#### \*步骤3：涉及应答D的操作

接收见证者设备的质问的装置通过互连装置接收来自证明者设备的各个质问d。见证者设备计算应答D的装置使用上述过程根据质问d计算应答D。

#### \*步骤4：涉及检查的操作

证明者的发送装置向控制者发送各个应答D。控制者设备还包括：

- 计算装置，此后被称作控制者设备的计算装置，
- 比较装置，此后被称作控制者设备的比较装置。

### 第一种情况：证明者已经发送一部分确认R

如果证明者的发送装置已经发送一部分确认R，则控制者的计算装置在具有m个公开数值 $G_1, G_2, \dots, G_m$ 的情况下根据各个质问d和各个应答D计算一个重构确认R'，这个重构确认R'满足以下类型的关系：

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \bmod n$$

或以下类型的关系：

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \bmod n.$$

控制者设备的比较装置将各个重构确认R'与接收的所有或部分确认R进行比较。

### 第二种情况：证明者已经全部发送确认R

如果证明者的发送计算装置已经发送全部确认R，则控制者设备的计算装置和比较装置在具有m个公开数值 $G_1, G_2, \dots, G_m$ 的情况下确定各个确认R满足以下类型的关系：

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \bmod n$$

或以下类型的关系：

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \bmod n.$$

### 证明消息的完整性的实例

在一个能够与第一变型实施例配合使用的第二变型实施例中，基于本发明的系统被用来向一个被称为控制者的实体证明与一个被称为证明者的实体相关的消息M的完整性。上述系统包括与证明者实体相关的证明者设备。上述证明者设备通过互连装置与见证者设备互连。尤其可以采取漫游对象中的逻辑微电路的形式，例如采取基于微处理器的银行卡中的微处理器的形式。上述系统还包括一个与控制者实体相关的控制者设备。上述控制者设备尤其可以采取终端或远程服务器的形式。上述控制者设备包括连接装置以便通过电子、电磁、光学或声学方式，尤其是通过数据处理通信网络连接到证明者设备。

上述系统被用来执行下列步骤:

**步骤1: 涉及确认R的操作**

每次见证者设备的计算确认R的装置使用上述过程计算各个确认R。见证者设备具有通过互连装置向证明者设备发送所有或部分确认R的发送装置, 此后被称作见证者设备的发送装置。

**步骤2: 涉及质问d的操作**

证明者设备包括计算装置, 此后被称作证明者的计算装置, 计算装置使用一个散列函数h计算至少一个令牌T, 其中散列函数的参数包括消息M和所有或部分确认R。证明者设备还包括通过连接装置向控制者设备发送各个令牌T的发送装置, 此后被称为证明者设备的发送装置。控制者设备还具有质问产生装置, 该装置在接收令牌T之后产生数量等于确认R的数量的质问d。控制者设备还具有通过连接装置向证明者发送所有或部分质问d的发送装置, 此后被称作控制者的发送装置。

**\*步骤3: 涉及应答D的操作**

接收见证者设备的质问的装置通过互连装置接收来自证明者设备的各个质问d。见证者设备计算应答D的装置使用上述过程根据质问d计算应答D。

**\*步骤4: 涉及检查的操作**

证明者的发送装置向控制者发送各个应答D。控制者设备还包括计算装置, 此后被称作控制者设备的计算装置, 上述计算装置在具有m个公开数值 $G_1, G_2, \dots, G_m$ 的情况下首先根据各个质问d和各个应答D计算一个重构确认R', 这个重构确认R'满足以下类型的关系:

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \pmod{n}$$

或以下类型的关系:

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \pmod{n}.$$

接着使用一个散列函数h计算一个令牌T', 其中散列函数的参数包括消息M和所有或部分重构确认R',

控制者设备还具有将计算的令牌T'与接收的令牌T相比较的比较

装置，此后被称为控制者设备的比较装置。

### 消息的数字签名及其真实性证明

在一个基于本发明的实施例的能够与前两个实施例中的一个和/或另一个配合使用的第三变型中，基于本发明的系统被用来证明一个被称作签名实体的实体对一个此后被称为签名消息的消息M实施的数字签名。

已签名消息包括：

- 消息M，
- 质问d和/或确认R，
- 应答D。

### 签名运算

上述系统包括与签名实体相关的签名设备。上述签名设备通过互连装置与见证者设备互连，并且尤其可以具有漫游对象中逻辑微电路的形式，例如具有基于微处理器的银行卡中微处理器的形式。

上述系统被用来执行下列步骤：

#### 步骤1：涉及确认R的操作

每次见证者设备的计算确认R的装置使用上述过程计算各个确认R。见证者设备包括通过互连装置向签名设备发送所有或部分确认R的发送装置，此后被称作见证者设备的发送装置。

#### 步骤2：涉及质问d的操作

签名设备包括计算装置，此后被称作签名设备的计算装置，上述计算装置使用一个散列函数h计算一个二进制序列并且从这个二进制序列中提取出数量等于确认R的数量的质问d，其中散列函数的参数包括消息M和所有或部分确认R。

#### \*步骤3：涉及应答D的操作

见证者设备接收质问d的装置通过互连装置接收来自签名设备的各个质问d。见证者设备计算应答D的装置使用上述过程根据质问d计

算应答D。见证者设备包括通过互连装置向签名设备发送应答D的发送装置，此后被称作见证者设备的发送装置。

## 检查运算

为了验证消息M的真实性，一个被称作控制者的实体检查已签名消息。

上述系统还包括一个与控制者实体相关的控制者设备。上述控制者设备尤其可以采取终端或远程服务器的形式。上述控制者设备包括连接装置以便通过电子、电磁、光学或声学方式，尤其是通过计算机通信网络连接到签名设备。

上述与签名实体相关的签名设备包括通过连接装置向控制者设备发送已签名消息的发送装置，此后被称为签名设备的发送装置。因而控制者设备具有一个包括以下内容的已签名消息：

- 消息M，
- 质问d和/或确认R，
- 应答D。

控制者设备包括：

- 计算装置，此后被称作控制者设备的计算装置，
- 比较装置，此后被称作控制者设备的比较装置。

在控制者设备具有确认R，质问d，应答D的情况下

如果控制者设备具有确认R，质问d，应答D，则控制者设备的计算和比较装置确定确认R，质问d和应答D满足以下类型的关系

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \pmod n$$

或以下类型的关系：

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \pmod n.$$

接着控制者设备的计算和比较装置确定消息M，质问d和确认R满足散列函数：

$$d = h(\text{消息}, R)$$

在控制者设备具有质问d和应答D的情况下

如果控制者重构具有质问d和应答D, 控制者的计算装置根据各个质问d和各个应答D重构满足以下类型的关系的确认R'

$$R' \equiv G_1^{d^1} \cdot G_2^{d^2} \cdot \dots \cdot G_m^{d^m} \cdot D^v \bmod n$$

或以下类型的关系:

$$R' \equiv D^v / G_1^{d^1} \cdot G_2^{d^2} \cdot \dots \cdot G_m^{d^m} \cdot \bmod n.$$

接着控制者设备的计算和比较装置确定消息M和质问d满足散列函数:

$$d = h(\text{消息}, R')$$

在控制者具有确认R和应答D的情况下

如果控制者设备具有确认R和应答D, 则控制者设备的计算装置使用散列函数并且以下面方式计算出d':

$$d' = h(\text{消息}, R)$$

接着控制者设备的计算和比较装置确定消息M, 质问d'和确认R满足以下关系:

$$R \equiv G_1^{d'^1} \cdot G_2^{d'^2} \cdot \dots \cdot G_m^{d'^m} \cdot D^v \bmod n$$

或以下类型的关系:

$$R \equiv D^v / G_1^{d'^1} \cdot G_2^{d'^2} \cdot \dots \cdot G_m^{d'^m} \cdot \bmod n.$$

终端设备

本发明还涉及与一个实体相关的终端设备。终端设备尤其可以采取漫游对象的形式, 例如基于微处理器的银行卡中的微处理器的形式, 终端设备被用来为控制者设备验证下列内容:

- 一个实体的真实性和/或
- 与这个实体相关的消息M的完整性。

通过所有或部分下列参数或这些参数的派生参数完成这个证明:

- m对私有数值 $Q_1, Q_2, \dots, Q_m$ 和公开数值 $G_1, G_2, \dots, G_m$  (m大于或等

于1),

-由上述f个素数 $p_1, p_2, \dots, p_r$  (f大于或等于2)的乘积构成的一个公开模数n。

上述模数, 上述私有和公开数值有以下类型的关系

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ 或 } G_i \equiv Q_i^v \pmod{n}$$

其中 v表示一个下述类型的公开指数

$$v=2^k$$

其中k是大于1的安全参数。

上述 m个公开数值 $G_i$ 是少于f个素数 $p_1, p_2, \dots, p_r$ 的 m个不同基数 $g_1, g_2, \dots, g_m$ 的平方 $g_i^2$ ; 产生上述 f个素数 $p_1, p_2, \dots, p_r$ 和/或上述 m个基数 $g_1, g_2, \dots, g_m$ 以满足下面的条件。

### 第一条件

根据第一条件, 各个等式:

$$x^v \equiv g_i^2 \pmod{n} \quad (1)$$

可以被以n为模的整数环中的x求解。

### 第二条件

根据第二条件, 在  $G_i \cdot Q_i^v \equiv 1 \pmod{n}$ 成立的情况下, 在通过把  $Q_i$  提高成以n为模以k-1为秩的乘方获得的 m个数值  $q_i$ 中有一个  $q_i$ 不同于  $\pm g_i$  (即有一个非无效解)。

根据第二条件, 在  $G_i \cdot Q_i^v \equiv 1 \pmod{n}$ 成立的情况下, 在通过把  $Q_i$  模n的反置提高成以n为模以k-1为秩的乘方获得的 m个数值  $Q_{iv}$ 中有一个  $Q_{iv}$ 不同于  $\pm g_i$  (即有一个非无效解)。

这里应当指出, 根据当前的符号表示,  $\pm g_i$ 表示数量  $g_i$ 和 $n-g_i$ 。

### 第三条件

根据第三条件, 在 2m个等式中间:

$$x^2 \equiv g_i \pmod{n} \quad (2)$$

$$x^2 \equiv -g_i \pmod{n} \quad (3)$$

其中至少有一个可以被以 $n$ 为模的整数环中的 $x$ 求解。

上述终端设备包括一个见证者设备，上述见证者设备包括一个存储器区段，上述存储器区段包含 $f$ 个素数  $p_i$ 和/或素数的中国余数的参数和/或公开模数 $n$ 和/或 $m$ 个私有数值  $Q_i$ 和/或私有数值  $Q_i$ 与公开指数 $v$ 的 $f, m$ 个分量 $Q_{i,j}$  ( $Q_{i,j} \equiv Q_i \pmod{p_j}$ )。

见证者设备还包括：

-随机数值产生装置，此后被称作见证者设备的随机数值产生装置，

-计算装置，此后被称作计算见证者设备的确认 $R$ 的装置，上述计算装置计算见证者设备在以 $n$ 为模的整数环中的确认 $R$ 。

通过以下方式计算各个确认

执行下列类型的运算：

$$R \equiv r^v \pmod{n}$$

其中  $r$ 是随机数值产生装置产生的随机数值，并且 $0 < r < n$ 。

或者，执行下列类型的运算：

$$R_i \equiv r_i^v \pmod{p_i}$$

其中  $r_i$ 是一个与素数  $p_i$ 相关的随机数值，其中 $0 < r_i < p_i$ ，各个  $r_i$ 属于一个由随机数值产生装置产生的随机数值集合 $\{r_1, r_2, \dots, r_f\}$ ，并且接着使用中国余数方法。

见证者设备还包括：

-接收装置，此后被称作接收见证者设备的质问 $d$ 的装置，上述接收装置接收一或多个质问 $d$ ，每个质问 $d$ 均包括 $m$ 个此后被称作基本质问的整数 $d_i$ 。

-计算装置，此后被称作计算见证者设备的应答 $D$ 的装置，上述计算根据各个质问 $d$ 计算一个应答 $D$ ，

或者通过执行下列类型的运算：

$$D \equiv r \cdot Q_1^{d_1} \cdot Q_2^{d_2} \cdot \dots \cdot Q_m^{d_m} \pmod{n}$$

或者通过执行下列类型的运算：

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \dots \cdot Q_{i,m}^{dm} \bmod p_i$$

并且接着使用中国余数方法。

上述见证者设备还包括发送一或多个确认R和一或多个应答D的发送装置。应答D的数量与质问d和确认R一样多,其中每组数值R,d,D构成一个被表示成{R,d,D}的三元组。

### 证明一个实体的真实性的实例

在一个第一实施例变型中,基于本发明的终端设备被用来向一个被称作控制者的实体证明一个被称作证明者的实体的真实性。

上述终端设备包括与证明者实体相关的证明者设备。上述证明者设备通过互连装置与见证者设备互连。尤其可以采取漫游对象中的逻辑微电路的形式,例如基于微处理器的银行卡中的微处理器的形式。

上述证明者设备还包括连接装置以便通过电子、电磁、光学或声学方式,尤其是通过数据处理通信网络连接到与控制者实体相关的控制者设备。上述控制者设备尤其可以采取终端或远程服务器的形式。

上述终端设备被用来执行下列步骤:

#### \*步骤1: 涉及确认R的操作

每次见证者设备的计算确认R的装置使用上述过程计算各个确认R。

见证者设备具有通过互连装置向证明者设备发送所有或部分确认R的发送装置,此后被称作见证者设备的发送装置。证明者设备还具有通过连接装置向控制者设备发送所有或部分确认R的发送装置,此后被称作证明者的发送装置

#### \*步骤2和3: 涉及质问d的操作, 涉及应答D的操作

见证者设备接收质问d的装置通过控制者设备和证明者设备之间的连接装置和证明者设备与见证者设备之间的互连装置接收来自控制者设备的各个质问d。见证者设备计算应答D的装置使用上述过程根据质问d计算应答D。

#### \*步骤4: 涉及检查的操作

证明者的发送装置向执行检查的控制者设备发送各个应答D。

### 证明消息的完整性的实例

在一个能够与第一实施例配合使用的第二实施例变型中，基于本发明的终端设备被用来向一个被称为控制者的实体证明与一个被称为证明者的实体相关的消息M的完整性。使上述终端设备包括一个与证明者实体相关的证明者设备，上述证明者设备通过互连装置与见证者设备连接。尤其可以采取漫游对象中的逻辑微电路的形式，例如基于微处理器的银行卡中的微处理器的形式。上述证明者设备包括连接装置以便通过电子、电磁、光学或声学方式，尤其是通过数据处理通信网络连接到与控制者实体相关的控制者设备。上述控制者设备尤其可以采取终端或远程服务器的形式。

上述终端设备被用来执行下列步骤：

步骤1：涉及确认R的操作

每次见证者设备的计算确认R的装置使用上述过程计算各个确认R。见证者设备具有通过互连装置向证明者设备发送所有或部分确认R的发送装置，此后被称作见证者设备的发送装置。

步骤2和3：涉及质问d的操作，涉及应答D的操作

证明者设备包括计算装置，此后被称作证明者的计算装置，计算装置使用一个散列函数h计算至少一个令牌T，其中散列函数的参数包括消息M和所有或部分确认R。证明者设备还具有通过连接装置向控制者设备发送各个令牌T的发送装置，此后被称为证明者设备的发送装置。

上述控制者设备在接收令牌T之后产生数量等于确认R的数量的质问d

见证者设备接收质问d的装置通过控制者设备和证明者设备之间的连接装置和证明者设备与见证者设备之间的互连装置接收来自控制者设备的各个质问d。见证者设备计算应答D的装置使用上述过程根据质问d计算应答D。

### **\*步骤4: 涉及检查的操作**

证明者的发送装置向进行检查的控制者发送各个应答D。

### **消息的数字签名及其真实性证明**

在一个能够与前两个实施例中的任意一个配合使用的第三实施例变型中, 基于本发明的终端设备被用来通过一个被称作签名实体的实体产生对一个此后被称为签名消息的消息M的数字签名。

已签名消息包括:

- 消息M,
- 质问d和/或确认R,
- 应答D。

上述终端设备包括与签名实体相关的签名设备。上述签名设备通过互连装置与见证者设备互连。尤其可以采取漫游对象中的逻辑微电路的形式, 例如基于微处理器的银行卡中的微处理器的形式。上述签名设备包括连接装置以便通过电子、电磁、光学或声学方式, 尤其是通过数据处理通信网络连接与与控制者实体相关的控制者设备。上述控制者设备尤其可以采取终端或远程服务器的形式。

### **签名运算**

上述终端设备被用来执行下列步骤:

#### **\*步骤1: 涉及确认R的操作**

每次见证者设备的计算确认R的装置使用上述过程计算各个确认R。见证者设备包括通过互连装置向签名设备发送所有或部分确认R的发送装置, 此后被称作见证者设备的发送装置。

#### **\*步骤2: 涉及质问d的操作**

签名设备包括计算装置。此后被称作签名设备的计算装置。上述计算装置使用一个散列函数h计算一个二进制序列并且从这个二进制序列中提取出数量等于确认R的数量的质问d, 其中散列函数的参数包括消息M和所有或部分确认R。

### \*步骤3: 涉及应答D的操作

接收质问d的装置通过互连装置接收来自签名设备的各个质问d。见证者设备计算应答D的装置使用上述过程根据质问d计算应答D。见证者设备包括通过互连装置向签名设备发送应答D的发送装置, 此后被称作见证者设备的发送装置。

### 控制者设备

本发明也涉及一个控制者设备。控制者设备尤其可以采取与控制者实体相关的终端或远程服务器的形式。控制者设备被用来检查以下内容:

-一个实体的真实性和/或

-与这个实体相关的消息M的完整性。

通过所有或部分下列参数或这些参数的派生参数完成这个证明:

-m对公开数值 $G_1, G_2, \dots, G_m$  (m大于或等于1),

-由上述f个素数 $p_1, p_2, \dots, p_f$  (f大于或等于2)的乘积构成的一个对于控制者设备和相关控制者实体是未知数的公开模数n。

上述模数, 上述私有和公开数值有以下类型的关系

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ 或 } G_i \equiv Q_i^v \pmod{n}$$

其中 v表示一个下述类型的公开指数:

$$v=2^k$$

其中k是大于1的安全参数。

上述 m个公开数值 $G_i$ 是少于f个素数 $p_1, p_2, \dots, p_f$ 的 m个不同基数 $g_1, g_2, \dots, g_m$ 的平方 $g_i^2$ ; 产生上述 f个素数 $p_1, p_2, \dots, p_f$ 和/或上述 m个基数 $g_1, g_2, \dots, g_m$ 以满足下面的条件。

### 第一条件

根据第一条件, 各个等式:

$$x^v \equiv g_i^2 \pmod{n} \quad (1)$$

可以被以n为模的整数环中的x求解。

## 第二条件

根据第二条件, 在  $G_i \equiv Q_i^V \pmod n$  成立的情况下, 在通过把  $Q_i$  提高成以  $n$  为模以  $k-1$  为秩的乘方获得的  $m$  个数值  $q_i$  中有一个  $q_i$  不同于  $\pm g_i$  (即有一个非无效解)。

根据第二条件, 在  $G_i \cdot Q_i^V \equiv 1 \pmod n$  成立的情况下, 在通过把  $Q_i$  模  $n$  的反置提高成以  $n$  为模以  $k-1$  为秩的乘方获得的  $m$  个数值  $q_i$  中有一个  $q_i$  不同于  $\pm g_i$  (即有一个非无效解)。

这里应当指出, 根据当前的符号表示,  $\pm g_i$  表示数量  $g_i$  和  $n-g_i$ 。

## 第三条件

根据第三条件, 在  $2m$  个等式中间:

$$x^2 \equiv g_i \pmod n \quad (2)$$

$$x^2 \equiv -g_i \pmod n \quad (3)$$

其中至少有一个可以被以  $n$  为模的整数环中的  $x$  求解。

## 证明一个实体的真实性的实例

在一个第一实施例变型中, 基于本发明的控制者设备被用来证明一个被称作证明者的实体和一个被称作控制者的实体的真实性。

上述证明者设备包括连接装置以便通过电子、电磁、光学或声学方式, 尤其是通过数据处理通信网络连接到与证明者实体相关的证明者设备。

上述控制者设备被用来执行下列步骤:

步骤1和2: 涉及确认  $R$  的操作, 涉及质问  $d$  的操作

上述控制者设备还具有通过连接装置接收所有或部分来自证明者设备的确认  $R$  的装置。

控制者设备包括质问产生装置, 该装置在接收所有或部分确认  $R$  之后产生数量等于确认  $R$  各个数量的各个质问  $d$ , 其中各个质问  $d$  均包括  $m$  个此后被称作基本质问的整数  $d_i$ 。

控制者设备还包括通过连接装置向证明者发送所有或部分质问d的发送装置，此后被称作控制者的发送装置。

\*步骤3和4：涉及应答D的操作，涉及检查的操作

控制者设备还包括：

- 通过连接装置接收来自证明者设备的应答D的装置，
- 计算装置，此后被称作控制者设备的计算装置，
- 比较装置，此后被称作控制者设备的比较装置。

第一种情况：证明者已经发送一部分确认R

如果证明者的接收装置已经接收一部分确认R，则控制者设备的计算装置在具有m个公开数值 $G_1, G_2, \dots, G_m$ 的情况下根据各个质问d和各个应答D计算一个重构确认R'，这个重构确认R'满足以下类型的关系：

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \pmod{n}$$

或以下类型的关系：

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \pmod{n}.$$

控制者设备的比较装置将各个重构确认R'与接收的所有或部分确认R进行比较。

第二种情况：证明者已经全部发送确认R

如果证明者的发送计算装置已经接收全部确认R，则控制者设备的计算装置和比较装置在具有m个公开数值 $G_1, G_2, \dots, G_m$ 的情况下确定各个确认R满足以下类型的关系：

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \pmod{n}$$

或以下类型的关系：

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \pmod{n}.$$

证明消息的完整性的实例

在一个能够与第一实施例配合使用的第二实施例变型中，基于本

发明的控制者设备被用来证明与一个被称为证明者的实体相关的消息M的完整性。

上述证明者设备包括连接装置以便通过电子、电磁、光学或声学方式，尤其是通过数据处理通信网络连接到与证明者实体相关的证明者设备。

上述控制者设备被用来执行下列步骤：

\*步骤1和2：涉及确认R的操作，涉及质问d的操作

上述控制者设备具有通过连接装置接收来自证明者设备的令牌T的装置。控制者设备具有质问产生装置，该装置在接收令牌T之后产生数量等于确认R的数量的质问d，其中各个质问d均包括m个此后被称作基本质问的整数 $d_i$ 。控制者设备还具有通过连接装置向证明者发送所有或部分质问d的发送装置，此后被称作控制者的发送装置。

\*步骤3和4：涉及应答D的操作，涉及检查的操作

上述控制者设备还包括通过连接装置接收来自证明者设备的应答D的装置。上述控制者设备还包括计算装置，此后被称作控制者设备的计算装置，上述计算装置在具有m个公开数值 $G_1, G_2, \dots, G_m$ 的情况下首先根据各个质问d和各个应答D计算一个重构确认R'，这个重构确认R'满足以下类型的关系：

$$R' \equiv G_1^{d_1} \cdot G_2^{d_2} \cdot \dots \cdot G_m^{d_m} \cdot D^v \pmod{n}$$

或以下类型的关系：

$$R' \equiv D^v / G_1^{d_1} \cdot G_2^{d_2} \cdot \dots \cdot G_m^{d_m} \pmod{n}.$$

接着使用一个散列函数h计算一个令牌T'，其中散列函数的参数包括消息M和所有或部分重构确认R'。

控制者设备还具有将计算的令牌T'与接收的令牌T相比较的比较装置，此后被称作控制者设备的比较装置。

## 消息的数字签名及其真实性证明

在一个能够与前两个实施例中的一个或另一个配合使用的第三实施例变型中，通过利用一个被称作控制者的实体检查一个签名消息，

基于本发明的控制者设备被用来证明消息M的真实性。

通过一个与具有散列函数 $h$ (消息, R)的签名实体相关的签名设备发送的签名消息包括:

- 消息M,
- 质问d和/或确认R,
- 应答D.

### 检查运算

上述签名设备包括连接装置以便通过电子, 电磁, 光学或声学方式, 尤其是通过数据处理通信网络连接到与签名实体相关的签名设备。上述控制者设备通过连接装置从签名设备接收签名消息。

控制者设备包括:

- 计算装置, 此后被称作控制者设备的计算装置,
- 比较装置, 此后被称作控制者设备的比较装置。

\*在控制者设备具有确认R, 质问d, 应答D的情况下

如果控制者设备具有确认R, 质问d, 应答D, 则控制者设备的计算和比较装置确定确认R, 质问d和应答D满足以下类型的关系

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \pmod{n}$$

或以下类型的关系:

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \pmod{n}.$$

接着控制者设备的计算和比较装置确定消息M, 质问d和确认R满足散列函数:

$$d = h(\text{消息}, R)$$

\*在控制者设备具有质问d和应答D的情况下

如果控制者设备具有质问d和应答D, 控制者设备的计算装置可以根据各个质问d和各个应答D计算出满足以下类型的关系的确认R':

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \pmod{n}$$

或以下类型的关系:

$$R' \equiv D^v / G_1^{d^1} \cdot G_2^{d^2} \cdot \dots \cdot G_m^{d^m} \cdot \text{mod } n.$$

接着控制者设备的计算和比较装置确定消息M和质问d满足散列函数

$$d = h(\text{消息}, R')$$

在控制者设备具有确认R和应答D的情况下:

如果控制者设备具有确认R和应答D, 则控制者设备的计算装置使用散列函数并且以下面方式计算出d':

$$d' = h(\text{消息}, R)$$

接着控制者设备的计算和比较装置确定消息M, 质问d'和确认R满足以下关系

$$R \equiv G_1^{d'^1} \cdot G_2^{d'^2} \cdot \dots \cdot G_m^{d'^m} \cdot D^v \text{ mod } n$$

或以下类型的关系:

$$R \equiv D^v / G_1^{d'^1} \cdot G_2^{d'^2} \cdot \dots \cdot G_m^{d'^m} \cdot \text{mod } n.$$

#### 附图说明

在阅读完本申请的以下描述和附图之后, 本发明的其它特征在优点将更加清楚。

图 1A-1D 分别描述了表示  $GG(p)$  中“求乘方”函数的图的一个片断;

图 2A 和 2B 分别描述了  $G$  在圆圈中和在分支的一个适当位置时图的片断;

图 3A 和 3B 分别描述了用于一给定参数  $k$  的图的一个片断。

#### 具体实施方式

GQ方法的目标是对实体、消息和消息的数字签名一起进行动态认证。这些都属于“不传送知识”的方法。一个实体证明其知道一个或若干个私有数值。另一个实体进行检查; 该实体知道对应的公开数值。证明实体希望在不出示私有数值的情况下得到检查实体的信任以便根据

需要以任意多次使用上述私有数值。

各个 GQ方法均依赖于一个由秘密的大素数组成的公开模数。一个公开指数 $v$ 和一个公开模数 $n$ 共同构成一个验证密钥 $\langle v, n \rangle$ ，即"提高到模数 $n$ 的 $v$ 次幂"，并且通过一个或若干个类型相同的通用等式直接实现： $G_i \equiv Q_i^v \pmod n$ 或反置 $G_i \times Q_i^v \equiv 1 \pmod n$ 。该类型对检查实体而不是证明实体内部的计算操作有影响；事实上安全分析混淆了两个类型。与一个公开数值 $G$ 和一个私有数值 $Q$ 关联的各个通用等式共同构成一对数值  $\{G, Q\}$ 。总之，各个 GQ方法针对相同密钥  $\langle v, n \rangle$  实现了一或若干对数值  $\{G, Q\}$ 。

GQ方法的一个被称作 GQ1的经典版本使用了 RSA数字签名机制。验证密钥 $\langle v, n \rangle$ 是一个 RSA公开密钥，其中奇指数 $v$ 最好是一个素数。各个 GQ1方法通常使用单独一对数值  $\{G, Q\}$ ：根据一个属于 RSA数字签名技术不可分割的部分的格式机制通过鉴别数据推断出公开数值 $G$ 。私有数值 $Q$ 或其反置模数 $n$ 是鉴别数据的一个RSA签名。证明实体出示有关其自身鉴别数据的 RSA签名的知识并且无论使用多少次这个证明不会暴露签名，从而保守了秘密。

GQ1方法通常实现两个级别的密钥：为一个对实体进行授权的机构保留 RSA私有签名密钥，其中上述实体通过鉴别数据区分彼此。这种机制被称作"基于身份"的机制。因而，芯片卡的一个发射器使用其用于各个卡的发射的 RSA私有密钥计算一个被记录成卡中的各种私有密钥的私有数值 $Q$ ；或者一个计算机网络上的客户端在进入各个会话时使用其RSA私有密钥计算一个在会话期间会被当成客户端的短期私有密钥的私有数值 $Q$ 。证明实体，芯片卡或客户端在会话期间知道其鉴别数据的 RSA签名；它们不知道在密钥层次上处于更高一级的 RSA私有密钥。但是，在一个机构的层次上使用一个 768位模数通过 GQ1方法对实体进行动态认证所需的工作负载与在各个实体的层次上使用一个512位模数和三个素数通过RSA对实体进行动态认证的工作负载几乎相同，这允许证明实体在计算各个素数乘积的取模结果之前通过计算各个素数的取模结果来使用中国余数技术。

然而，一个机构和受信实体之间的密钥层次并不是必须的。可以通过一个属于证明实体的模数使用 GQ1方法，这使得能够使用中国余数技术减少证明实体的工作负载，并且不根本改变检查实体的工作负载，另外一个证明实体层次上的模数可以比一个机构层次上的模数更短，例如512位比768位。

当实体知道其自身模数的素数时，为何要使用 RSA数字签名机制？

GQ方法的另一个被称作基本 GQ2的版本直接处理模数 $n$ 的因数分解问题。在这种情况下"直接"意味着"不需要 RSA签名"。GQ2的目标是减少证明实体和检查实体的工作负载。证明实体出示有关其自身模数的分解的知识并且这个证明不暴露分解，从而保守了秘密，所以能够根据需要被经常使用。GQ2协议的安全性等价于模数的因数分解的安全性。

各个证明实体具有其自身的模数 $n$ 。各个GQ2机制实现了一个参数 $k$ ，即一个大于1的较小数值，从而固定一个公开指数 $v = 2^k$ 和一或若干对数值 $\{G_i, Q_i\}$ 到 $\{G_m, Q_m\}$ 。各个公开数值 $G_i$ 是一个大于1并且被称作"基数"的较小数值 $g_i$ 的平方。所有证明实体均可以使用相同的公开数值 $G_i$ 到 $G_m$ 。模数 $n$ 的因数分解和私有数值 $Q_i$ 到 $Q_m$ ， $n$ 则在密钥层次中处于相同的层次上。通过两个必要和充分条件定义各组基本GQ2密钥：

-对于各个基数，两个等式 $x^2 \equiv \pm g_i \pmod n$ 在以 $n$ 为模的整数环中均不具有 $x$ 的解，即数值 $\pm g_i$ 是两个 $n$ 为模的非二次余数。

-对于各个基数，等式 $x^v \equiv g_i^2 \pmod n$ 在以 $n$ 为模的整数环中具有 $x$ 的解，其中 $v = 2^k$ 。私有数值 $Q_i$ 或其反置模数 $n$ 是这些解中的任意一个。

考虑第二条件，为了使数值 $\pm g_i$ 是两个以 $n$ 为模的非二次余数，模数 $n$ 必须包括至少两个恒等于3 (mod 4)的素数，但 $g_i$ 的勒让德符号则不同于此。因此，由其中最多仅有一个恒等于3 (mod 4)的素数组成的任意模数不允许建立一组基本GQ2密钥，这特许素数恒等于3 (mod 4)。因而通过随机取出大素数，显然只有一半恒等于3 (mod 4)并且另一半恒等于1 (mod 4)。结果，许多在使用的RSA模型不能建立一组基

本GQ2密钥。

我们这里介绍克服这种限制以便能够针对任意模数，尤其是任意RSA模数使用GQ2技术的通用化GQ2密钥集合：它们取决于两个必要充分原则。

第一原则还原了第二基本GQ2条件：

-对于各个基数 $g_1$ 到 $g_m$ ，等式 $x^V \equiv g_i^2 \pmod n$ 在以 $n$ 为模的整数环中具有 $x$ 的解，其中 $V = 2^k$ 。

由于私有数值 $Q$ 或其反置模数 $n$ 是等式的一个解，以 $n$ 为模的连续 $k-1$ 次乘方将其转换成一个数值 $q_i$ ，数值 $q_i$ 是以 $n$ 为模的整数环中的 $G_i$ 的平方根。根据数值 $q_i$ 是等于两个数值 $g_i$ 或 $n-g_i$ 中的一个，还是不同于两个数值 $g_i$ 和 $n-g_i$ ，可以确定其是否无效解。当数值 $q_i$ 是非无效解时，整除 $q_i^2 - g_i^2$ 的 $n$ 不整除 $q_i - g_i$ 或 $q_i + g_i$ 。因而任意非无效数值 $q$ 均暴露了模数 $n$ 的一个分解。

$$n = \text{pgcd}(n, q_i - g_i) \times \text{pgcd}(n, q_i + g_i)$$

第二原则加宽了第一基本GQ2条件：

-在数值 $q_1$ 至 $q_m$ 中至少有一个数值 $q_i$ 是非无效解。

应当注意，如果存在一个数值 $q_i$ 并且数值 $\pm g_i$ 是以 $n$ 为模的整数环中的两个非二次余数，则数值 $q_i$ 肯定是非无效解。因而基本GQ2密钥集合肯定是通用化GQ2密钥集合的一部分，这使得能够使用任意的模数，即对于任意的大素数成分，无论是恒等于 $3 \pmod{4}$ 还是恒等于 $1 \pmod{4}$ ，其中至少有两个是不同的。另一方面，许多通用化GQ2密钥集合不是基本GQ2密钥集合。各个通用化GQ2密钥集合基于下面情况中的一种：

-当 $2 \times m$ 个数值 $\pm g_1$ 到 $\pm g_m$ 全部是非二次余数时，这是一个基本GQ2密钥集合。

-当在 $2 \times m$ 个数值 $\pm g_1$ 到 $\pm g_m$ 中至少有一个二次余数时，这不是一个补充GQ2密钥集合，所知的是一个补充GQ2密钥集合。

本发明涉及补充GQ2密钥集合，根据定义这些通用化GQ2密钥集合不是基本GQ2密钥集合。除了前面两个原则之外，这种集合必须满

足第三个原则。

-在 $2 \times m$ 个数值 $\pm g_1$ 到 $\pm g_m$ 中有至少一个二次余数。

为了评估问题和理解我们提供的解决方案，即本发明，我们首先分析一个非无效数值 $q$ 暴露的模数 $n$ 的分解，并且接着回顾中国余数技术，和伽罗瓦域 $CG(p)$ 中有关秩的概念；并且接着研究 $CG(p)$ 中的"开方"函数和 $CG(p)$ 中对二次余数"求平方根"的函数；最后分析上述三个原则的适用性。

### 对模数分解的分析

就象模数 $n$ 被分解成 $f$ 个素数 $p_1$ 到 $p_f$ 那样，以 $n$ 为模的整数环被分解成 $f$ 个伽罗瓦域 $CG(p_1)$ 到 $CG(p_f)$ 。在每个域中有两个单平方根，即 $\pm 1$ 。在整数环中，有 $2f$ 个单平方根。各个私有数值 $Q_1$ 到 $Q_m$ 均定义了一个数值 $\Delta_i = q_i/g_i \pmod{n}$ ，该数值是整数环的 $2f$ 个单平方根中的一个；即 $n$ 分割 $\Delta_i^2 - 1$ 。

当 $q_i$ 是无效数值时，即当 $\Delta_i = \pm 1$ 时， $n$ 分割 $\Delta_i - 1$ 或 $\Delta_i + 1$ 并且 $\Delta_i$ 不暴露模数 $n$ 的分解。

当 $q_i$ 是非无效数值时，即当 $\Delta_i \neq \pm 1$ 时， $n$ 不分割 $\Delta_i - 1$ 或 $\Delta_i + 1$ 并且暴露了一个通过各个域中的 $\Delta_i$ 值得到的分解， $n = \text{pgcd}(n, \Delta_i - 1) \times \text{pgcd}(n, \Delta_i + 1)$ ：一方面是分割 $\Delta_i - 1$ 的素数，另一方面是分割 $\Delta_i + 1$ 的素数。

数值 $q$ 的乘法合成的规则检查。两个数值 $\{q_1, q_2\}$ 给出了一个复合数 $q_1 \times q_2 \pmod{n}$ 。

-当 $q_1$ 是非无效数值并且 $q_2$ 是无效数值时，复合数 $q_1 \times q_2 \pmod{n}$ 是非无效数值；它暴露了与 $q_1$ 相同的分解。

-当 $q_1$ 和 $q_2$ 是非无效数值并且 $\Delta_1 = \pm \Delta_2$ 时，复合数 $q_1 \times q_2 \pmod{n}$ 是无效数值；它不暴露任何分解。

-当 $q_1$ 和 $q_2$ 是非无效数值并且 $\Delta_1 \neq \pm \Delta_2$ 时，复合数 $q_1 \times q_2 \pmod{n}$ 是非无效数值；它暴露了一个第三分解。

三个数值 $\{q_1, q_2, q_3\}$ 提供了四个复合数 $\{q_1 \times q_2, q_1 \times q_3, q_2 \times q_3, q_1 \times q_2 \times q_3 \pmod{n}\}$ ，总共有7个数值；因而 $m$ 个数

值提供 $2^m-m-1$ 个复合数并且总共有 $2^m-1$ 个数。

现在我们考虑一个通用化 GQ2 密钥集合，其中包括  $i$  个基数  $g_1$  到  $g_i$  和  $i$  个私有数值  $Q_1$  到  $Q_i$ ，从而提供  $i$  个数值  $q_1$  到  $q_i$  和  $i$  个均属于单根的数值  $\Delta_1$  到  $\Delta_i$ 。我们通过一个提供数值  $q_{i+1}$  和根  $\Delta_{i+1}$  的私有数值  $Q_{i+1}$  尝试考虑另一个基数  $g_{i+1}$ 。

\*总共  $2^{i+1}-1$  个数值包括下面各个情况下的所有非无效数值。

-根  $\Delta_{i+1}$  是无效数值并且至少一个根  $\Delta_1$  至  $\Delta_i$  是非无效数值。

-根  $\Delta_{i+1}$  是非无效数值并且在  $2 \times i$  个根  $\pm \Delta_1$  至  $\pm \Delta_i$  中出现。

\*如果根  $\Delta_{i+1}$  是非无效数值并且没有在  $2 \times i$  个根  $\pm \Delta_1$  到  $\pm \Delta_i$  中出现，则出现  $q_{i+1}$  的各个复合数均是非无效数值。

因此，当在  $m$  个数值  $q_1$  到  $q_m$  中至少有一个是非无效数值，则总共  $2^m-1$  个数值中有超过一半的数值是非无效数值。

根据定义，当  $2^l-1-1$  个对应的复合数均是非无效数值时，称  $l < f$  个非无效数值  $\{q_1, q_2, \dots, q_l\}$  相对于模数  $n$  是独立的，即总共  $2^l-1$  个数值均是非无效数值。因而这  $2^l-1$  个数值中的每一个数值均暴露了模数  $n$  的一个不同分解。

-当  $f$  个素数不同时，模数  $n$  有  $2^{f-1}-1$  个分解。因而如果  $f-1$  个数值  $q$  是独立的，则在  $2^{f-1}-1$  个分解和总共  $2^{f-1}-1$  个包括  $f-1$  个独立数值和  $2^{f-1}-f$  个对应复合数的数值之间存在一个双-单义 (bi-univocal) 对应关系。

### \*中国余数

对于两个数值  $a$  和  $b$ ， $0 < a < b$ ，其间的素数，和两个从  $0$  到  $a-1$  的数值  $X_a$  和从  $0$  到  $b-1$  的数值  $X_b$ ；涉及确定  $0$  到  $a \times b-1$  中的唯一数值使得  $X_a \equiv X \pmod{a}$  并且  $X_b \equiv X \pmod{b}$ 。数值  $\alpha \equiv \{b \pmod{a}\}^{-1} \pmod{a}$  是中国余数参数。以下是基本中国余数操作：

$$x \equiv X_b \pmod{a}$$

$$y = X_a - x; \text{如果 } y \text{ 为负数, 用 } y+a \text{ 替代 } y$$

$$z \equiv a \times y \pmod{a}$$

$$X = z \times b + X_b$$

最初:  $X = \text{中国余数}(X_a, X_b)$

当按照升序从最小的  $p_1$  到最大的  $p_f$  排列  $f$  个素数时, 中国余数参数如下所示(比素数少 1, 即  $f-1$ ):

- 第一个参数是  $\alpha \equiv (p_2(\bmod p_1))^{-1}(\bmod p_1)$ .
- 第二个参数是  $\beta \equiv (p_1 \times p_2(\bmod p_3))^{-1}(\bmod p_3)$ .
- 第  $i$  个参数是  $\lambda \equiv (p_1 \times \dots \times p_{i-1}(\bmod p_i))^{-1}(\bmod p_i)$ .
- 依此类推

在  $f-1$  个基本操作中, 根据  $f$  个分量  $X_1$  到  $X_f$ ,  $X_j$  从 0 到  $p_j-1$  构成的任意集合产生一个从 0 到  $n-1$  的数值:

- 一个具有第一参数的第一结果  $(\bmod p_1 \times p_2)$ ,
- 一个具有第二参数的第二结果  $(\bmod p_1 \times p_2 \times p_3)$ ,
- 一个具有最后参数的最后结果  $(\bmod n = p_1 \times p_2 \times \dots \times p_f)$ .

最初指定素数  $p_1$  到  $p_f$ , 以  $n$  为模的整数环中的各个元素具有两个等价的表示:

- $f$  个数值  $X_1$  到  $X_f$ , 一个素数分量:  $X_j \equiv X(\bmod p_j)$ ,
- 一个从 0 到  $n-1$  的数值  $X$ ,  $X = \text{中国余数}(X_1, X_2, \dots, X_f)$ .

**CG(p)中数值的秩** - 令  $p$  为一个奇素数并且  $a$  是一个小于  $p$  的数值, 即  $0 < a < p$ . 根据定义,  $a$  相对于  $p$  的秩是由  $\{x_i = a; \text{则对于 } i \geq 1, x_{i+1} \equiv a \times x_i(\bmod p)\}$  定义的序列  $\{X\}$  的周期。通过应用费马定理, 我们得到:  $x_{i+p} \equiv a^p \times x_i \equiv a \times x_i \equiv x_{i+1}(\bmod p)$ . 因而数值  $a$  相对于素数  $p$  的秩是  $p-1$  或  $p-1$  的一个除数。

例如, 当  $(p-1)/2$  是一个奇素数  $p'$  时, 伽罗瓦域  $CG(p)$  包含秩为 1 的数值: 即 1, 一个秩为 2 的数值: 即 -1,  $p'-1$  个秩为  $p'$  的数值和  $p'-1$  个秩为  $2 \times p' = p-1$  的数值。在  $CG(p)$  中, 任何秩为  $p-1$  的数值均是一个“生成器”。如此称呼的原因是,  $CG(p)$  中一个生成器的连续次幂, 即序列  $\{X\}$  中下标为 1 到  $p'-1$  的项值构成  $CG(p)$  的所有非零元素的一个排列。

令  $y$  是  $CG(p)$  的一个生成器。根据  $i$  和  $p-1$  求数值  $y^i(\bmod y)$  的秩。

当  $i$  与  $p-1$  互素时, 这个秩为  $p-1$ 。当  $i$  整除  $p-1$  时, 秩为  $(p-1)/i$ 。总之, 秩为  $(p-1)/\text{pgcd}(p-1,i)$  ( $\text{pgcd}$ =最大公约数)。

根据定义, 欧拉函数  $\varphi(n)$  是小于  $n$  并且与  $n$  互素的数的数量。在  $\text{CG}(p)$  中, 有  $\varphi(p-1)$  个生成器。

为了说明, 秩有助于理解 RSA 的基础。模数  $n$  是  $f$  个素数  $p_1$  到  $p_f$  的乘积, 其中  $f \geq 2$ 。对于从  $p_1$  到  $p_f$  的各个素数  $p_j$ , 公共指数  $e$  应当与  $p_j-1$  互素。现在, 密钥  $\langle e, p_j \rangle$  观察  $\text{CG}(p_j)$  的元素的秩: 它排列  $\text{CG}(p_j)$  的元素; 存在一个尽可能小的数值  $d_j$ , 使得  $p_j-1$  整除  $e \times d_j - 1$ 。密钥  $\langle d_j, p_j \rangle$  反置  $\text{CG}(p_j)$  的元素的排列。这  $f$  个分别处于各个域  $\text{CG}(p_1)$  到  $\text{CG}(p_f)$  中的排列被公开密钥  $\langle e, n \rangle$  概括出的 RSA 排列表示成以  $n$  为模的整数环。存在一个通常尽可能小的数值  $d$ , 使得  $\text{ppcm}(p_1-1, p_2-1, \dots, p_f-1)$  的最小公倍数整除  $d \times e - 1$ 。对于从  $p_1$  到  $p_f$  的各个素数  $p_j$ , 存在  $d_j \equiv d \pmod{p_j-1}$ 。被公开密钥  $\langle e, n \rangle$  概括的 RSA 排列被私有密钥  $\langle d, n \rangle$  反置。

**CG(p)中的乘方** - 定义一个数值  $t$  使得  $p-1$  可被  $2^t$  整除但不可被  $2^{t+1}$  整除。各个大素数均出现在一个并且唯一一个类目中:  $t=1, t=2, t=3, t=4$ , 等等。如果考虑足够多的连续素数, 大约 2 个中有一个出现在第一类目中, 其中  $p$  与  $3 \pmod{4}$  同余, 4 个中有一个出现在第二类目中, 其中  $p$  与  $5 \pmod{8}$  同余, 8 个中有一个出现在第三类目中, 其中  $p$  与  $9 \pmod{16}$  同余, 16 个中有一个出现在第四类目中, 其中  $p$  与  $17 \pmod{32}$  同余, 等等; 平均起来,  $2^t$  个中有一个出现在第  $n$  类目中, 其中  $p$  与  $2^t+1 \pmod{2^{t+1}}$  同余。

由于数值  $x$  和  $p-x$  在  $\text{CG}(p)$  中有相同的乘方, 密钥  $\langle 2, p \rangle$  不排列  $\text{CG}(p)$ 。 $\text{CG}(p)$  中的函数“求乘方”可以被表示成一个定向图, 其中域内的各个非零元素有其位置。根据各个元素的秩的奇偶性将图的结构分析成分支和圆圈。

- 设置零元素。这个为 0。不为没有被其它元素涉及到的零元素定义秩; 零元素被隔离。

- 设置单元元素。这个为 1, 唯一秩为 1 的元素。 $\text{CG}(p)$  中所有一

的根均位于涉及 1 的分支内。令  $y$  是  $CG(p)$  的除二次余数之外的任何余数；密钥  $\langle (p-1)/2^t, p \rangle$  将  $y$  变换成 -1 的第  $2^{t-1}$  次原根，原根被表示成  $b$ ；因而我们具有  $y^{(p-1)/2} \equiv -1 \pmod{p}$ 。因而在  $CG(p)$  中， $b$  的指数为 1 到  $2^{t-1}$  的各个幂是一的  $2^{t-1}$  个不等于 1 的根：它们构成涉及 1 的分支。

- 具有偶数秩的任何元素的乘方是另一个秩被 2 整除的元素。因而各个具有偶数秩的元素被放到一个分支中；各个分支包含一个可被 2 整除但不可被 4 整除的秩数，接着，如果  $t \geq 2$ ，包含 2 个可被 4 整除但不可被 8 整除的秩数，如果  $t \geq 3$ ，包含 4 个可被 8 整除但不可被 16 整除的秩数，如果  $t \geq 4$ ，包含 8 个可被 16 整除但不可被 32 整除的秩数，等等。所有分支类似于涉及 1 的分支；各个分支的  $2^{t-1}$  个叶子是非二次余数；每个分支包含  $2^{t-1}$  个元素并且涉及一个具有奇数秩的元素；存在  $(p-1)/2^t$  个均具有相同长度  $t$  的分支。

- 除单位元素之外具有奇数秩的任何元素的乘方是另一个具有相同秩的元素。密钥  $\langle 2, p \rangle$  排列  $(p-1)/2^t$  个具有奇数秩的元素构成的集合。排列被分解成排列圆圈。圆圈的数量取决于  $(p-1)/2^t$  的分解。对于  $(p-1)/2^t$  的各个除数  $p'$ ，存在一个包含  $M(p')$  个具有秩  $p'$  的元素。回忆一下，根据定义，欧拉函数  $M(p')$  是小于  $p'$  并且与  $p'$  互素的数值的数量。例如，当  $p'$  等于  $(p-1)/2^t$  时，互素， $p'-1$  个以  $p'$  为秩的数值构成一个大的排列圆圈。

图 1A-1D 分别针对  $p$  与  $3 \pmod{4}$  同余， $p$  与  $5 \pmod{8}$  同余， $p$  与  $9 \pmod{16}$  同余和  $p$  与  $17 \pmod{32}$  同余图解了一个图段。

- 白圆圈表示分支中的叶子；这些是非二次余数。
- 灰圆圈表示分支中的结点；这些是具有偶数秩的二次元素。
- 圆圈中的结点被表示成黑圆圈；这些是具有偶数秩的二次元素。

$CG(p)$  中的平方根 - 已知  $a$  是  $CG(p)$  的一个二次余数，看看如何计算等式  $x^2 \equiv a \pmod{p}$ ，即  $CG(p)$  中“求平方根”的一个解。当然，有许多种得到相同结果的方式；可以参考 Henri Cohen 的著作，计算代数理论教程，31-36 页，大学生数学系列教材 138 卷(GTM)138, Springer,

**Berlin1993 年出版。**

数值  $s=(p-1+2^t)/2^{t+1}$  提供一个密钥  $\langle s, p \rangle$ , 即:

$\langle (p+1)/4, p \rangle$ , 当  $p$  与  $3 \pmod{4}$  同余时,

$\langle (p+3)/8, p \rangle$ , 当  $p$  与  $5 \pmod{8}$  同余时,

$\langle (p+7)/16, p \rangle$ , 当  $p$  与  $9 \pmod{16}$  同余时,

$\langle (p+15)/32, p \rangle$ , 当  $p$  与  $17 \pmod{32}$  同余时,

等等。

- 密钥  $\langle s, p \rangle$  将一个圈的任何元素变换成圈中前面的元素。当  $a$  具有偶数秩时, 是具有奇数秩的解, 表示成  $w$ 。在  $CG(p)$  中,  $w^2/a$  等于  $a$  至  $(2 \times (p-1+2^t)/2^{t+1})-1=(p-1)/2^t$  的幂。另一个解具有偶数秩; 即  $p-w$ 。

- 通常, 密钥  $\langle s, p \rangle$  将一个第一逼近中的任何二次余数变换成一个称作  $r$  的解。由于  $a$  是一个二次余数, 密钥  $\langle 2^{t-1}, p \rangle$  当然将  $r^2/a$  变换成 1。为了逼近  $a$  的平方根, 取  $r^2/a \pmod{p}$  的  $2^{t-2}$  次幂以便得到 +1 或 -1。如果结果为 +1 则新逼近的余数为  $r$ , 否则如果结果为 -1 则余数为  $b \times r \pmod{p}$ , 已知  $p$  表示域  $CG(p)$  中 1 的任何  $2t$  次原根。因而密钥  $\langle 2^{t-2}, p \rangle$  将新逼近变换成 1。如果必要也可以通过使用密钥  $\langle 2^{t-3}, p \rangle$  并且乘以  $b^2 \pmod{p}$  来进行逼近, 等等。

下面的算法对等待求解。它使用前面定义的数值  $a, b, p, r$  和  $t$  和两个变量:  $c$  表示连续校正,  $w$  表示连续逼近。在算法开始时,  $c=b$  并且  $w=r$ 。在计算结束时, 两个解是  $w$  和  $p-w$ 。

对于从  $t-2$  到 1 的  $i$ , 重复下列序列:

- 对数值  $w^2/a \pmod{p}$  应用密钥  $\langle 2^i, p \rangle$  以获得 +1 或 -1。

- 当得到 -1 时用  $w \times c \pmod{p}$  取代  $w$ 。

- 用  $c^2 \pmod{p}$  取代  $c$ 。

原理的可用性 - 根据定义我们指出当等式  $x^y \equiv g^2 \pmod{p}$  在域  $CG(x)$  内有  $x$  的解时参数  $k$ , 基数  $g$  和素数  $p$  是兼容的, 其中指数  $\Theta$  为  $2k$ 。数值  $k$  和  $g$  较小但大于 1。数值  $p$  是大素数。

-当  $t=1$ , 即  $p \equiv 3 \pmod{4}$  时, 等式有两个解。

-当  $t=2$ , 即  $p \equiv 5 \pmod{8}$  时, 根据  $g$  相对于  $p$  的勒让德符号, 如果  $(g|p)=+1$  则等式有 4 个解, 如果  $(g|p)=-1$  则等式没有任何解。

-当  $t>2$ , 即  $p \equiv 1 \pmod{8}$  时, 令数值  $u$  使得  $2^u$  整除公开数值  $G=g^2$  相对于  $p$  的秩并且使得  $2^{u+1}$  不整除这个秩; 因而  $u$  等于从 0 到  $t-1$  的数值中的一个。如果  $u>0$  并且  $k+u>t$  则等式没有解; 如果  $k+u \leq t$  则等式有  $2^k$  个解; 如果  $u=0$  并且  $k>t$  则有  $2^t$  个解。

因而根据  $G$  是在圆圈内还是在在一个分支内的适当位置上, 存在两种兼容性。

- 当  $G$  在圆圈内, 即  $u=0$  时, 无论  $k$  的值如何, 在圆圈内有一个具有奇数秩的解并且存在具有偶数秩并且散布在  $\Delta=\min(k,t)$  个涉及圆圈的连续分支内的解, 即  $2^a$  个解。图 2A 图解了这种情况, 其中  $k \geq t=3$ , 即一个与  $9 \pmod{16}$  同余的素数, 这表明  $u=0$ 。

-当  $G$  位于一个分支内一个适当位置上, 即  $u>0$  并且  $u+k \leq t$  时, 存在  $2k$  个均具有偶数秩并且位于分支内的解。图 2B 图解了这种情况。

指定一个参数  $k$ , 因而根据  $t$  的值是小于  $k$  还是大于或等于  $k$ , 存在两种素数。

-对于任何素数  $p_j$ , 例如  $t < k$ , 各个  $G_i$  应当位于圆圈内, 并且在涉及  $G_i$  的分支内没有解。定义一个数值  $\Delta_{i,j}$ , 根据  $g_i$  还是  $-g_i$  位于圆圈内该数值为  $+1$  或  $-1$ 。对于  $m$  个数值  $\Delta_{1,j}$  到  $\Delta_{m,j}$  而言这是没有选择的。图 3A 图解了  $t < k$  的情况:  $G_i$  位于一个圆圈内, 其中一个素数  $p_j$  与  $9 \pmod{16}$  同余, 即  $u=0, t=3$  并且  $k>3$ 。

-对于任何使得  $t \geq k$  的素数  $p_j$ , 各个  $G_i$  应当使得  $u+k \leq t$ , 即或者在一个圆圈内并且  $u=0$ , 或者在一个分支的适当位置上并且  $1 \leq u \leq t-k$ 。定义一个数值  $\Delta_{i,j}$ , 根据  $Q_{i,j}$  位于图中涉及  $g_i$  还是  $-g_i$  的部分内该数值为  $+1$  或  $-1$ 。对于  $m$  个数值  $\Delta_{1,j}$  到  $\Delta_{m,j}$  中各个数值而言存在一个选择; 可以单独将各个数值  $\Delta_{i,j}$  从一个值切换成另一个值。图 3B 图解了  $t \geq k$  的情况:  $G_i$  位于一个圆圈内, 其中一个素数  $p_j$  与  $17 \pmod{32}$  同余, 即  $u=1, t=4$  并且  $k=3$ 。

由  $f$  个分量  $\{\Delta_{i,1} \dots \Delta_{i,f}\}$  构成的各个集合是  $CG(p_j)$  中 1 的平方根。根据  $f$  个分量是否相等，这个根是无效解或非无效解。接着规定  $f$  个分量构成的集合是否固定，这表明数值  $q_i$  是否无效数值。因而当一个数值  $q_i$  是非无效数值时，由  $f$  个分量  $\{\Delta_{i,1} \dots \Delta_{i,f}\}$  构成的集合概括了模数的分解。因而可以在计算私有分量  $Q_{i,j}$  之前测试原则。

- 当一个公开数值  $G_i$  位于针对素数  $p_j$  的圆圈内时，根据  $g_i$  还是  $-g_i$  位于圆圈内数值  $\Delta_{i,j}$  为 +1 或 -1。当  $p_j \equiv 3 \pmod{4}$  时，这是一个勒让德符号： $\Delta_{i,j} = (g_i | p_j)$ 。

- 当一个公开数值  $G_i$  位于一个针对素数  $p_j$  的分支内适当位置上时，通过计算私有分量  $Q_i$ ，可以确定为  $\Delta_{i,j}$  指定的值。

密钥集合的产生 - 指定一个参数  $k$ ，存在两个策略。

- 生成器均需要  $f$  个素数以便确定  $m$  个基数。检查第一素数：2, 3, 5, 7, ... 以评估其与  $f$  个大素数  $p_1$  到  $p_f$  中每个素数的兼容性。尽管  $g = 2$  不与  $p \equiv 5 \pmod{8}$  兼容，但 2 可以进入一个基数的成分内。实际上，当两个数值位于一个分支内的一个位置上时，由于平方使圆圈更接近，所以其乘积更接近圆圈。因而通过组成单独考虑均不适当的数值可以获得一个基数。

- 或者，生成器需要  $m$  个基数和模数的特征，使得一个位长（例如 512, 768, 1024, 1536, 2048）和若干个连续到 1 的位具有强权重（例如 1, 8, 16, 24, 32）以便确定  $f \geq 2$  个素数。表示成  $G_1, G_2, \dots, G_m$  的基数通常出现在第一素数：2, 3, 5, 7, 11 ... 中间，或者是第一素数的组合。除非专门指出，这些是前  $m$  个素数： $G_1 = 2, G_2 = 3, G_3 = 5, G_4 = 7, \dots$ 。注意  $p \equiv 5 \pmod{8}$  不与  $G = 2$  兼容。模数  $n$  将是  $f$  个具有接近长度，即为被  $f$  整除的模数分配的长度的素数的乘积。

第一原则 - 参数  $k$ ，各个素数  $p_1$  到  $p_f$  和从  $g_1$  到  $g_m$  的各个基数应当兼容。定义一个数值  $h$ ，使得  $2^h$  整除  $g$  相对于  $p$  的秩，但  $2^{h+1}$  不整除这个秩。为了计算数值  $h$ ，下面过程使用勒让德符号  $(g | p)$  和一个数

值 $b$ ,  $CG(p)$ 中1的第 $2^t$ 次原根。

-如果 $(g|p) = +1$ 并且 $t = 1$ , 返回" $h = 0$ ".

-如果 $(g|p) = +1$ 并且 $t > 1$ , 对 $G$ 应用密钥 $\langle (p-1+2^t)/2^{t+1}, p \rangle$ 到以便获得一个被称作 $w$ 的结果。

-如果 $w = +g$ , 返回" $h = 0$ ".

-如果 $w = p-g$ , 返回" $h = 1$ ".

-否则, 将 $c$ 设置到 $b$ 并且针对从 $t-1$ 到2的 $i$ ,

-对 $w/g(\bmod p)$ 应用密钥  $\langle 2^i, p \rangle$ 以便获得 $\pm 1$ ,

-如果 $-1$ , 将  $h$ 设置成  $i$ 并且用  $w \times c (\bmod p)$ 替换 $w$ ,

-用  $c^2 (\bmod p)$ 替换  $c$ .

-返回"从 2到  $t-1$ 的  $h$ 数值".

-如果 $(g|p) = -1$ , 返回" $h = t$ ".

已知当 $u > 0$ 并且 $k+u > t$ 时 $k$ ,  $g$ 和 $p$ 不兼容; 当 $h = 0$ 或 $1$ 时, 无论 $k$ 的数值如何它们均是兼容的, 并且在 $h > 1$ 和 $k+h \leq t+1$ 时相等。

第二原则 - 下面三个过程对应于第二原则的不同实现。在某些实现中, 第二原则可以被加强到要求各个数值  $q_1$ 到 $q_m$ 均不是无效数值的程度。接着均衡基数的作用; 无论是否均衡第二原则均对方案在安全性方面的某些表现有影响。最终, 当在  $m$ 个数值 $\{q_1 \dots q_m\}$ 中存在  $f > 2$ 个不同素数时, 需要有至少一个含有  $f-1$ 个独立数值的子集。

三个过程使用 $m \times f$ 个被定义如下的数值 $\delta_{i,j}$ 。

-当 $p_i$ 满足 $t < k$ ,  $i$ 从1到 $m$ 时,  $\delta_{i,j} = \Delta_{i,j}$ , 即 $+1$ , 如果 $h_{i,j} = 0$ , 和 $-1$ , 如果 $h_{i,j} = 1$ 。

-当 $p_i$ 满足 $t \geq k$ ,  $i$ 从1到 $m$ 时,  $\delta_{i,j} = 0$ , 这意味着可以根据第二原则选择 $\Delta_{1,j}$ 到 $\Delta_{m,j}$ 。

一个第一过程确定至少一个集合 $\{\delta_{i,1} \dots \delta_{i,f}\}$ 是可变的或零, 即至少一个数值  $q_1$ 到 $q_m$ 是非无效数值, 或者可以被选定成非无效数值。

-对于从1到 $m$ 的  $i$ 和从 1到 $f$ 的  $j$ ,

-如果 $\delta_{i,j} = 0$  或 $\neq \delta_{i,j}$ , 返回"成功"。

-返回"失败".

一个第二过程确定各个集合 $\{\delta_{i,1} \dots \delta_{i,f}\}$ 是可变的或零, 即各个数值  $q_1$ 到 $q_m$ 是非无效数值, 或者可以被选定成非无效数值.

-对于从1到 $m$ 的  $i$ ,

-对于从 1到 $f$ 的  $j$ ,

-如果 $\delta_{i,j}=0$  或 $\neq\delta_{i,j}$ , 则跳到  $i$ 的下一个数值,

-返回"失败".

-返回"成功".

一个第三过程确定, 对于每对素数 $p_{j_1}$ 和 $p_{j_2}$ , 并且 $1 \leq j_1 \leq j_2 \leq f$ , 存在至少一个集合 $\{\delta_{i,1} \dots \delta_{i,f}\}$ , 其中 $\delta_{i,j_1}$ 是零或不同于 $\delta_{i,j_2}$ . 当  $m$ 小于  $f-1$ 时显然会失败. 当在  $m$ 个数值 $\{q_1 \dots q_m\}$ 中成功时, 对于  $f$ 个素数, 需要有至少一个含有  $f-1$ 个独立数值的集合.

-对于从1到 $f-1$ 的 $j_1$ 和从  $j_1+1$ 到  $f$ 的 $j_2$ ,

-对于从1到 $m$ 的  $i$ ,

-如果 $\delta_{i,j_1}=0$  或 $\neq\delta_{i,j_2}$ , 则跳到 $j_1$ 和 $j_2$ 的下一个数值,

-返回"失败".

-返回"成功".

当一个过程失败时, GQ2密钥集合的生成器遵循从两个可能策略中为其选定的策略:

-改变  $m$ 个基数中的一个并且保留  $f$ 个素数,

-改变  $f$ 个素数中的一个并且保留  $m$ 个基数.

第三原则 - 下面过程确定通用化 GQ2密钥的集合在生成或已经生成时属于

-一个基本 GQ2密钥集合, 即 $2 \times m$ 个数值 $\pm g_1$ 到 $\pm g_m$ 均是非二次余数, 或者

-一个补充GQ2密钥集合, 即在 $2 \times m$ 个数值 $\pm g_1$ 到 $\pm g_m$ 中间至少存在一个二次余数.

该过程使用两个勒让德符号 $(g_i|p_j)$ 和 $(-g_i|p_j)$ , 其中 $i$ 从1到 $m$ 而 $j$ 从1

到f.

- 对于从1到m的 i,
- 对于从 1到f的 j,
- 如果 $(g_i|p_j)=-1$ , 则跳到i的下一个数值.
- 返回"补充 GQ2密钥集合".
- 对于从 1到f的 j,
- 如果 $(g_i|p_j)=-1$ , 则跳到i的下一个数值.
- 返回"补充GK2密钥集合".
- 返回"基本GK2密钥集合".

私有分量 - 对于一个直接类型的等式:  $x^v \equiv g_i^2 \pmod{p_j}$ , 下面的计算产生私有分量 $Q_{i,j}$ 的所有可能数值。两个最简单和最常见的情况, 即 $t=1$ 和 $t=2$ , 后面有更加复杂的情况, 即 $t>2$ 。

对于 $t=1$ , 即 $p_j \equiv 3 \pmod{4}$ , 密钥 $\langle (p_j+1)/4, p_j \rangle$ 提CG( $p_j$ )中任意二次余数的二次平方根。据此, 导出一个数值 $s_j \{ ((p_j+1)/4)^k \pmod{(p_j-1)/2}$ , 该数值提供一个密钥 $\langle s_j, p_j \rangle$ , 该密钥将 $G_i$ 转换成 $w \{ G_i^{s_j} \pmod{p_j}$ 。  $Q_{i,j}$ 等于 $n$ 或 $p_j-n$ 。

对于 $t=2$ , 即 $p_j \equiv 5 \pmod{8}$ , 密钥 $\langle (p_j+3)/8, p_j \rangle$ 为CG( $p_j$ )中具有奇数秩的元素提供具有奇数秩的平方根。 据此, 导出一个数值 $s_j \equiv ((p_j+3)/8)^k \pmod{(p_j-1)/4}$ , 该数值提供一个密钥 $\langle s_j, p_j \rangle$ , 该密钥将 $G_i$ 转换成 $w \equiv G_i^{s_j} \pmod{p_j}$ 。注意, 由于2是CG( $p_j$ )中的一个非二次余数, 所以 $z \equiv 2^{(p_j-1)/4} \pmod{p_j}$ 是-1的平方根。  $Q_{i,j}$ 或者等于 $w$ 或 $p_j - w$ , 或者等于 $w' \equiv w \times z \pmod{p_j}$ 或 $p_j - w'$ 。

对于 $p_j \equiv 2^t+1 \pmod{2^{t+1}}$ 和 $t>2$ , 密钥 $\langle (p_j-1+2^t)/2^{t+1}, p_j \rangle$ 为任意具有奇数秩的元素提供具有奇数秩的平方根。  $k$ ,  $g$ 和 $p$ 之间的兼容测试指定 $h$ 的数值,  $u$ 的下一个数值。

-当 $G_i$ 位于圆圈内( $u=0$ , 无论  $k$ 有何数值)时, 建立一个数值 $s_j \equiv ((p_j-1+2^t)/2^{t+1})^k \pmod{(p_j-1)/2^t}$ 。 密钥 $\langle s_j, p_j \rangle$ 将 $G_i$ 转换成具有奇数秩的解 $w \equiv G_i^{s_j} \pmod{p_j}$ 。 在 $\min(k, t)$ 个涉及圆圈的连续分支, 即在 $A$ 个分支内分布有具有偶数秩的解。  $Q_{i,j}$ 等于 $w$ 和CG( $p_j$ )中1(单位)的任意

第 $2^u$ 次根的乘积。

-当 $G_j$ 位于分支( $u > 0, u + k \leq t$ )中一个适用位置上时, 所有的解均和 $G_j$ 位于相同的分支上, 即一个涉及表示数值 $G_i$ 的第 $2^u$ 次幂的圆圈的分支。产生一个数值 $s_j \equiv ((p_j - 1 + 2^t)/2^{t+1})^{k+u} \pmod{(p_j - 1)/2^t}$ 。

密钥 $\langle s_j, p_j \rangle$ 将 $G_i$ 的第 $2^u$ 次幂转换成具有奇数秩的数值 $w$ 。 $w$ 和 $CG(p_j)$ 中1(单位)的第 $2^{k+u}$ 次原根的乘积的集合包括 $2^k$ 个 $Q_{i,j}$ 数值。

当 $p_i$ 使得 $t \geq k$ 时, 由于数值 $b_j$ 是 $CG(p_j)$ 中1(单位)的第 $2^t$ 次原根,  $CG(p_j)$ 中 $b_j$ 的第 $2^{t-u}$ 次幂存在; 这是1的第 $2^k$ 次原根。通过使 $Q_{i,j}$ 与1的一个第 $2^k$ 次原根相乘可以交换数 $\Delta_{i,j}$ 的值。

对于一个反置类型的等式:  $1 \equiv x^v \times g_i^{2^t} \pmod{p_j}$ , 足够用密钥 $\langle s_j, p_j \rangle$ 中的 $((p_j - 1)/2^t) - s_j$ 替换数值 $s_j$ , 这相当于反置 $CG(p_j)$ 中 $Q_{i,j}$ 的值。

具有两个与5(mod 8)同余的素数的密钥集合的例子

$p_1 = \text{E6C83BF428689AF8C35E07EDD06F9B39A659829A58B79CD894C435C95F32BF25}$   
 $p_2 = \text{11BF8A68A0817BFCC00F15731C8B70CEF9204A34133A0DEF862829B2EEA74873D}$   
 $n = p_1 \times p_2 = \text{FFFFF8263434F173D0F2E76B32D904F56F4A5A6A50000C43D32B650E9AB9A}$   
 $\text{AD2EB713CD4F9A97C4DBDA3828A3954F296458D5F42C0126F5BD6B05478BE0A80ED1}$

这里是最前面的素数的勒让德符号。

$(2|p_1) = -1; (3|p_1) = -1; (5|p_1) = +1; (7|p_1) = -1;$   
 $(11|p_1) = +1; (13|p_1) = -1; (17|p_1) = +1;$

在 $CG(p_1)$ 中, -5, -11和17的秩为奇数。

$(2|p_2) = -1; (3|p_2) = +1; (5|p_2) = +1; (7|p_2) = +1;$   
 $(11|p_2) = +1; (13|p_2) = -1; (17|p_2) = -1;$

在 $CG(p_2)$ 中, 3, -5, 7和11的秩为奇数。

Carmichael 函数是

$\lambda(n) = \text{ppcm}((p_1 - 1)/4, (p_2 - 1)/4).$   
 $\lambda(n) = \text{33331A13DA4304A5CFD617BD6F834311642121543334F40C3D57A9C8558555D5BDAA2EF6AED1}$   
 $\text{7B9E3794F51A65A1B37239B18FA9B0F618627D8C7E1D8499C1B}$

$k = 9$ , 数值 $\sigma \equiv \lambda(n) - ((1 + \lambda(n))/2)^9 \pmod{\lambda(n)}$ 被用作私有指数以便使用反置类型的通用等式。

$\sigma = \text{01E66577BC997CAC273671E187A35EFD25373ABC9FE6770E7446C0CCEF2C72AF6E89D0BE277C}$   
 $\text{C6165F1007187AC58028BD2416D4CC1121E7A7A8B6AE186BB4B0}$

数值2, 3, 7, 13和17不适于作为基数。

密钥 $\langle \sigma, n \rangle$ 将 $g_1 = 5$ 转换成一个私有数值 $Q_1$ ,  $Q_1$ 不说明任何因数分解。实际上在两个域中, -5均在一个圆圈上。

$Q_1 = \text{818C23AF3DE333FAECE88A71C4591A70553F91D6C0DD5538EC0F2AAF909B5BDAD491FD8BF13}$

F18E3DA3774CCE19D0097BC4BD47C5D6E0E7EBF6D89FE3DC5176C

密钥 $\langle \sigma, n \rangle$ 将 $g_2 = 11$ 转换成一个私有数值 $Q_2$ ,  $Q_2$ 说明了一个因数分解。实际上, 11在两个域中处于不同的位置上。

$Q_2 = 25F9AFDF177993BE8652CE6E2C728AF31B6D66154D3935AC535196B07C19080DC962E4E86ACF40D01FDC454F2565454F290050DA052089EEC96A1B7DEB92CCA7$

密钥 $\langle \sigma, n \rangle$ 将 $g_3 = 21 = 3 \times 7$ 转换成一个私有数值 $Q_3$ ,  $Q_3$ 说明了一个因数分解。

$Q_3 = 78A8A2F30FEB4A5233BC05541AF7B684C2406415EA1DD67D18A0459A1254121E95D5CAD8A1FE3ECFE0685C96CC7EE86167D99532B3A96B6BF9D93CAF8DF46AF0$

密钥 $\langle \sigma, n \rangle$ 将 $g_4 = 26 = 2 \times 13$ 转换成一个私有数值 $Q_4$ ,  $Q_4$ 说明了一个因数分解。

$Q_4 = 6F1748A6280A200C38824CA34C939F97DD2941DAD300030E481B738C62BF8C673731514D1978AF5655FE493D659514A6CE897AB76C01E50B5488C5DAD12332E5$

还可以通过两个素数, 中国余数的参数和八个私有分量表示私有密钥。

$\alpha = (p_1 \pmod{p_2})^{-1} \pmod{p_1} = ADE4E77B703F5FDEAC5B9AAE825D649E06692D15FBF0DF737B115DC4D012FD1D$

$Q_{1,1} = Q_1 \pmod{p_1} = 7751AEE918A8F5CE44AD73D613A4F465E06C6F9AF4D229949C74DD6C18D76FAF$

$Q_{1,2} = Q_1 \pmod{p_2} = A9EB5FA1B2A981AA64CF88C382923DB64376F5FD46152C08EEB6114F31B7665F$

$Q_{2,1} = Q_2 \pmod{p_1} = D5A7D33C5FB75A033F2F0E8B20274B957FA34004ABB2C2AC1CA3F5320C5A9049$

$Q_{2,2} = Q_2 \pmod{p_2} = 76C9F5EFD066C73A2B5CE9758DB512DFC011F5B5AF7DA8D39A961CC876F2DD8F$

$Q_{3,1} = Q_3 \pmod{p_1} = 2FEC0DC2DCA5BA7290B27BC8CC85C938A514B8F5CFD55820A174FB5E6DF7B883$

$Q_{3,2} = Q_3 \pmod{p_2} = 010D488E6B0A38A1CC406CEE0D55DE59013389D8549DE493413F34604A160C1369$

$Q_{4,1} = Q_4 \pmod{p_1} = A2B32026B6F82B6959566FADD9517DB8ED8524652145EE159DF3DC0C61FE3617$

$Q_{4,2} = Q_4 \pmod{p_2} = 011A3BB9B607F0BD71BBE25F52B305C224899E5F1F8CDC2FE0D8F9FF62B3C9860F$

私有密钥  $GQ_2$  的多态 - 私有密钥  $GQ_2$  的不同可能表示被证明均是等价的: 它们均相当于知道模数  $n$  的因数分解, 即实际的  $GK_2$  私有密钥。  $GQ_2$  私有密钥的表示对证明实体内部而不是审查实体内部的计算进程有影响。这里是  $GQ_2$  私有密钥的三个可能的主要表示。 1)  $GQ$  私有密钥的传统表示是存储  $m$  个私有数值  $Q_i$  和公开检查  $\langle v, n \rangle$ ; 对于  $GQ_2$  方案, 这种表示与下面两个竞争。 2) 就工作负载而言的最优表示是存储参数  $k$ ,  $f$  个素数  $p_j$ ,  $m \times f$  个私有分量  $Q_{i,j}$  和中国余数的  $f-1$  个参数。 3) 就私有密钥尺寸而言的最优表示在于存储参数  $k$ ,  $m$  个基数  $g_i$  和  $f$  个素数  $p_j$ , 接着在开始使用时确定  $m$  个私有数值  $Q_i$  和模数  $n$  以便其等价于第一种表示, 或者确定  $m \times f$  个私有分量  $Q_{i,j}$  和中国余数的  $f-1$  个参

数以便等价于第二种表示。

由于动态认证机制或数字签名机制的安全性等价于知道模数的因数分解，对于GQ2方案，不能简单使用相同模数区分两个实体。通常，各个证明实体具有其自身的GQ2模数。然而可以规定具有四个素数的GQ2模数，一个实体知道其中的两个素数，而另一个实体知道其它两个素数。

**动态认证** - 动态认证机制向一个被称为控制者的实体证明另一个被称为证明者的实体的真实性以及可能相关的消息M的真实性，使得控制者可以确定实际上正与证明者交涉，并且确定其自身和证明者正在说及相同的消息M。相关消息M是可选的，这意味着它可以为空。

动态认证机制是一个四操作序列：一个确认操作，一个质问操作，一个应答操作和一个检查操作。证明者完成确认和应答操作。控制者完成质问和审查操作。

在证明者内，可以隔离一个见证者以便隔离证明者的最敏感参数和功能，即确认和应答的产生。见证者具有参数  $k$  和 GQ2 私有密钥，即根据上述三种表示对模数进行的因数分解： $f$  个素数和  $m$  个基数， $m \times f$  个私有分量， $f$  个素数和  $f-1$  个中国余数参数， $m$  个私有数值和模数  $n$ 。

见证者可以对应于一个具体的实施例，例如一个与共同构成证明者的PC相连的芯片卡，或在PC内特别保护的程序，或在芯片卡内特别保护的程序。如此隔离的见证者类似于签名实体内部定义的见证者。在每次执行机制时，见证者产生一或多个确认  $R$ ，并且接着对一样多的质问  $d$  产生一样多的应答  $D$ 。各个集合  $\{R, d, D\}$  构成一个GQ2三元组。

除了包括见证者之外，证明者在必要时还具有一个散列函数和一个消息M。

控制者具有模数  $n$ ，模数  $n$  来自一个公开密钥目录，甚至来自一个

公开密钥证书；在必要时还具有相同的散列函数和一个消息 $M'$ 。证明者可以将GQ2公开参数，即数值 $k$ ， $m$ 和 $g_1$ 到 $g_m$ 提供给控制者。控制者能够根据任何质问 $d$ 和任何应答 $D$ 重构确认 $R'$ 。参数 $k$ 和 $m$ 为控制者提供信息。除非专门指出， $m$ 个从 $g_1$ 到 $g_m$ 的基数是头 $m$ 个素数。各个质问 $d$ 应当包含 $m$ 个被表示成 $d_1$ 到 $d_m$ 的基本质问：每个基数一个基本质问。从 $d_1$ 到 $d_m$ 的各个基本质问是从0到 $2^{k-1}-1$ 的一个数值(未使用 $v/2$ 到 $v-1$ 中的数值)。通常各个质问被编码成 $m$ 乘 $k-1$ 个位(而不是 $m$ 乘 $k$ 个位)。例如，对于 $k=5$ 和 $m=4$ 个基数5，11，21和26，各个质问包含16位，其中通过4个四位字节发送这16位。当可能的 $(k-1) \times m$ 个质问有同等概率时，数值 $(k-1) \times m$ 确定各个 GQ2三元组带来的安全性：一个根据定义不知道模数 $n$ 的因数分解的冒名顶替者在 $2^{(k-1) \times m}$ 次尝试中只有一次成功机会。当 $(k-1) \times m$ 来自于15至20时，一个三元组足够合理保证动态认证。为了实现任何层次的安全性，可以并行产生三元组；也可以顺序产生它们即重复机制。

1)涉及确认的操作包括下列运算。

当见证者不使用中国余数时，该见证者具有参数 $k$ ，从 $Q_1$ 到 $Q_m$ 的 $m$ 个私有数值和模数 $n$ ；该见证者以随机和秘密的方式选择一或多个随机数值 $r$  ( $0 < r < n$ )；接着通过接连 $k$ 次连续平方(mod  $n$ )运算将各个随机数值 $r$ 转换成确认 $R$ 。

$$R \equiv r^k \pmod{n}$$

这里是一个具有前面无中国余数的密钥集合的例子。

$r=5E94B894AC24AF843131F437C1B1797EF562CFA53AB8AD426C1AC016F1C89CFDA131207$   
 $19477C3E2FB4B4566088E10EF9C010E8F09C60D981512198126091996$   
 $R=6BBF9FFA5D509778D0F93AE074D36A07D95FFC38F70C8D7E3300EBF234FA0BC20A95152A8FB73DE81$   
 $FAEE5BF4FD3EB7F5EE3E36D7068D083EF7C93F6FDDF673A$

当见证者使用中国余数时，见证者具有参数 $k$ ，从 $p_1$ 到 $p_f$ 的头 $f$ 个素数， $f-1$ 个中国余数参数和 $muf$ 个私有分量 $Q_{i,j}$ ；见证者以随机和秘密的方式中抽出一或多个包括 $f$ 个随机数的集合：各个集合针对每个素数 $p_i$  ( $0 < r_i < p_i$ ) 包含一个随机数值 $r_i$ ；接着通过 $k$ 次连续平方(mod  $p_i$ )

运算将各个随机数值 $r_i$ 转换成一个确认分量 $R_i$ 。

$$R_i \equiv r_i^v \pmod{p_i}$$

对于包括 $f$ 个确认分量的各个集合，见证者根据中国余数技术建立一个确认。确认的数量与随机数集合一样多。

$R = \text{中国余数}(R_1, R_2, \dots, R_f)$

这里是一个具有前面的密钥集合和中国余数的例子。

$r_1 = 5C6D37F0E97083C8D120719475E080BBBF9F7392F11F3E244FDF0204E84D8CAE$

$R_1 = 3dddf516ee3945cb86d20d9c49e0da4d42281d07a76074dd4fc20c5c7c5c205d866$

$r_2 = AC8F85034AC78112071947C457225E908E83A2621B0154ED15DBFCB9A4915AC3$

$R_2 = 01168CEC0F661EAA15157C2C287C6A5B34EE28F8EB4D8D340858079BCAE4ECB016$

$R = \text{Chinese remainders}(R_1, R_2) =$

$0AE51D90CB4FDC3DC757C56E063C9ED86BE153B71FC65F47C123C27F082BC3DD15273D4A9238047$   
 $18573F2F05E991487D17DAE0AAB7DF0D0FFA23E0FE59F95F0$

在两种情况下，证明者向控制者发送所有或部分确认 $R$ ，或发送一个散列码 $H$ ，其中通过杂凑各个确认 $R$ 和一个消息 $M$ 来获得上述散列码 $H$ 。

2) 涉及质问的操作包括随机抽出一或多个均由 $m$ 个基本质问 $d_1, d_2, \dots, d_m$ 构成的质问 $d$ ；各个基本质问 $d_i$ 均是0到 $v/2-1$ 中的一个数值。

$$d = d_1 d_2 \dots d_m$$

这里是一个针对两个例子的质问，即 $k = 5$ 和 $m = 4$ 。

$d_1 = 1011 = 11 = 'B'$ ； $d_2 = 0011 = 3$ ； $d_3 = 0110 = 6$ ； $d_4 = 1001 = 9$ ，

$d = d_1 || d_2 || d_3 || d_4 = 1011001101101001 = B369$

控制者向证明者发送各个质问 $d$ 。

3) 应答操作包含下列运算。

当见证者不使用中国余数时，见证者具有参数 $k$ ，从 $Q_1$ 到 $Q_m$ 的 $m$ 个私有数值和模数 $n$ ；见证者使用通过确认操作得到的各个随机数 $r$ 和基于基本质问的私有数值计算一或多个应答 $D$ 。

$$D \equiv r \times Q_1^{d_1} \times Q_2^{d_2} \times \dots \times Q_m^{d_m} \pmod{n}$$

这里是无中国余数的例子的延续。

$D = 027E6E808425BF2B401FD00B15B642B1A8453BE8070D86C0A7870E6C1940F7A6996C2D871EBE611$   
 $812532AC5875E0E116CC8BA648FD8E86BE0B2ABCC3CCBBBE4$

当见证者使用中国余数时，见证者具有参数 $k$ ， $f$ 个从 $p_1$ 到 $p_f$ 的素数， $f-1$ 个中国余数参数和 $m \times f$ 个私有分量 $Q_{i,j}$ ；见证者使用通过确认操作得到的各个随机数集合计算一或多个包含 $f$ 个应答分量的集合；对

于每个素数，各个应答分量集合均包含一个分量。

$$D \equiv \Delta \times Q_{1,j}^{d_1} \times Q_{2,j}^{d_2} \times \dots \times Q_{m,j}^{d_m} \pmod{p_j}$$

针对各个应答分量集合，见证者根据中国余数技术建立一个应答。  
应答的数量与质问一样多。

$$D = \text{中国余数}(D_1, D_2, \dots, D_j)$$

这里是无中国余数的例子的延续。

$$D1 = \tau_1 \times Q_{1,1}^{d_1} \times Q_{2,1}^{d_2} \times Q_{3,1}^{d_3} \times Q_{4,1}^{d_4} \pmod{p_1}$$

C71F86F6FD8F955E2EE434BFA7706E38E5E715375BC2CD2029A4BD572A9EDEE6

$$D2 = \tau_2 \times Q_{1,2}^{d_1} \times Q_{2,2}^{d_2} \times Q_{3,2}^{d_3} \times Q_{4,2}^{d_4} \pmod{p_2}$$

0BE022F4A20523F98E9F5DBEC0E10887902F3AA48C864A6C354693AD0B59D85E

D=90CE7EA43CB8EA89ABDD0C814FB72ADE74F02FE6F098ABB98C8577A660B9CFCEAECEB93BE1  
BCC356811BF12DD667E2270134C9073B9418CA5EBF5191218D3FDB3

在两种情况下，证明者均向控制者发送各个应答D。

4)检查操作包括检查各个三元组{R, d, D}满足下面针对非零数值的等式。

$$R \times \prod_{i=1}^m G_i^{d_i} \equiv D^{2^t} \pmod{n} \text{ 否则 } R \equiv D^{2^t} \times \prod_{i=1}^m G_i^{d_i} \pmod{n}$$

或在恢复各个确认时：没有确认一定为零。

$$R' \equiv D^{2^t} / \prod_{i=1}^m G_i^{d_i} \pmod{n} \text{ 否则 } R' \equiv D^{2^t} \times \prod_{i=1}^m G_i^{d_i} \pmod{n}$$

可选地，控制者接着通过杂凑各个恢复的确认R'和消息M'计算一个散列码H'。当控制者因而检索到在第一确认操作结束时接收的内容，即所有或部分确认R或散列码H时，动态认证成功。

例如，一系列基本运算将应答D转换成一个确认R'。该操作序列包括被k-1个基数除法或基数乘法(mod n)分隔的k个平方(mod n)。对于在第i个平方和第i+1个平方之间执行的第i个除法或乘法，基本质问 d1的第i个位指示是否必须使用 g1，基本质问 d2的第i个位指示是否1必须使用 g2，...，基本质问 dm的第i个位指示是否必须使用 gm。

这里是无中国余数的例子的结束。

D=027E6E808425BF2B401FD00B15B642B1A8453BE8070D86C0A7870E6C1940F7A6996C2D871EBE611  
812532AC5875E0E116CC8BA648FD8E86BE0B2ABCC3CCBBBE4

计算平方模n:

88BA681DD641D37D7A7D9818D0DBEA82174073997C6C32F7FCAB30380C4C6229B0706D1AF6EBD84  
61771C31B4243C2F0376CAF5DCEB644F098FAF3B1EB49R39

乘以5乘26 = 130, 即'82'模n:

6ECABA65A91C22431C413E4EC7C7B39FDE14C9782C94FD6FA3CAAD7AFE192B9440C1113CB8DB  
C45619595D263C1067D3D0A840FDE008B415028AB3520A6AD49D

计算平方模n:

0236D25049A5217B13818B39AFB009E4D7D52B17486EBF844D64CF75C4F652031041328B29EBF0829D  
54E3BD17DAD218174A01E6E3AA650C6FD62CC274426607

乘以21, 即'15'模n:

2E7F40960A8BBF1899A06BBB6970CFC5B47C88E8F115B5DA594504A92834BA405559256A705ABAB6  
E7F6AE82F4F33BF9E91227F0ACFA4A052C91ABF389725E93

计算平方模n:

B802171179648AD687E672D3A32640E2493BA2E82D5DC87DBA2B2CC0325E7A71C50E8AE02E299EF  
868DD3FB916EBCBC0C5569B53D42DAD49C956D8572E1285B0

乘以5乘11乘21 = 1155, 即'483'模n:

3305560276310DEFEC1337EB5BB5810336FDB28E91B350D485B09188E0C4F1D67E68E9590DB7F9F39  
C22BDB4533013625011248A8DC417C667B419D27CB11F72

计算平方模n:

8871C494081ABD1AEB8656C38B9BAAB57DBA72A4BD4EF9029ECBFFF540E55138C9F22923963151F  
D0753145DF70CE22E9D019990E41DB6104005EEB7B1170559

乘以5乘11乘26 = 1430, 即'596'模n:

2CF5F76EEBF128A0701B56F837FF68F81A6A5D175D0AD67A14DAEC6FB68C362B1DC0ADD6CFC00  
4FF5EEACDF794563BB09A17045ECFFF88F5136C7FBC825BC50C

计算平方模n:

6BBF9FFA5D509778D0F93AE074D36A07D95FFC38F70C8D7E3300EBF234FA0BC20A95152A8FB73DE  
81FAEE5BF4FD3EB7F5EE3E36D7068D083EF7C93F6FDDF673A

检索到确认 R 。认证成功。

这里是有中国余数的例子的结束。

D=90CE7EA43CB8EA89ABDD0C814FB72ADE74F02FE6F098ABB98C8577A660B9CFCEAECB93BE1  
BCC356811BF12DD667E2270134C9073B9418CA5EBF5191218D3FDB3

计算平方模n:

770192532E9CED554A8690B88F16D013010C903172B266C1133B136EBE3EB5F13B170DD41F4ABE1473  
6ADD3A70DFA43121B6FC5560CDD4B4845395763C792A68

乘以5乘26 = 130, 即'82'模n:

6EE9BEF9E52713004971ABB9FBC31145318E2A703C8A2FB3E144E7786397CD8D1910E70FA86262DB7  
71AD1565303AD6E4CC6E90AE3646B461D3521420E240FD4

计算平方模n:

D9840D9A8E80002C4D0329FF97D7AD163D8FA98F6AF8FE2B2160B2126CBBDFFC734E39F2C9A39983  
A426486BC477F20ED2CA59E664C23CA0E04E84F2F0AD65340

乘以21, 即'15'模n:

D7DD7516383F78944F2C90116E1BEE0CCDC8D7CEC5D7D1795ED33BFE8623DB3D2E5B6C5F62A56  
A2DF4845A94F32BF3CAC360C7782B5941924BB4BE91F86BD85F

计算平方模 $n$ :

DD34020DD0804C0757F29A0CBBD7B46A1BAF949214F74FDFF021B626ADAFBAB5C3F1602095DA39  
D70270938AE362F2DAE0B914855310C75BCA328A4B2643DCCDF

乘以5乘11乘21 = 1155, 即'483'模 $n$ :

038EF55B4C826D189C6A48EFDD9DADBD2B63A7D675A0587C8559618EA2D83DF552D24EAF6BE983  
FB4AFB3DE7D4D2545190F1B1F946D327A4E9CA258C73A98F57

计算平方模 $n$ :

D1232F50E30BC6B7365CC2712E5CAE079E47B971DA03185B33E918EE6E99252DB3573CC87C604B32  
7E5B20C7AB920FDF142A8909DBBA1C04A6227FF18241C9FE

乘以5乘11乘26 = 1430, 即'596'模 $n$ :

3CC768F12AEDFCD4662892B9174A21D1F0DD9127A54AB63C984019BED9BF88247EF4CCB56D71E0  
FA30CFB0FF28B7CE45556F744C1FD751BFBCA040DC9CBAB744

计算平方模 $n$ :

0AE51D90CB4FDC3DC757C56E063C9ED86BE153B71FC65F47C123C27F082BC3DD15273D4A9238047  
18573F2F05E991487D17DAE0AAB7DF0D0FFA23E0FE59F95F0

正确检索到确认 R。认证成功。

## 数字签名

数字签名机制允许一个被称作签名实体的实体产生已签名消息并且允许一个被称作控制者的实体确定已签名消息。消息M是任意的二进制序列:可以为空。通过向消息M加入一个签名附录对消息M签名,签名附录包括一或多个确认和/或质问,以及对应的应答。

控制者具有模数 $n$ ,模数 $n$ 来自一个公开密钥目录,甚至来自一个公开密钥证书;它也具有相同的散列函数。证明者可以将GQ2公开参数,即数量 $k$ ,  $m$ 和 $g_1$ 到 $g_m$ 提供给控制者,例如通过把它们放在签名附录中。

数值 $k$ 和 $m$ 为控制者提供信息。一方面,从 $d_1$ 到 $d_m$ 的各个基本质问是 $0$ 到 $2^{k-1}-1$ 中的一个数值(未使用 $v/2$ 到 $v-1$ 中的数值)。另一方面,各个质问 $d$ 应当包含 $m$ 个被表示成 $d_1$ 到 $d_m$ 的基本质问,其中基本质问和基数一样多。并且,除非专门指出, $m$ 个从 $g_1$ 到 $g_m$ 的基数是头 $m$ 个素数。在 $(k-1) \times m$ 等于15至20的情况下,可以用四个并行产生的 GQ2三元组签名;在 $(k-1) \times m$ 等于60或更大数值的情况下,可以仅用一个 GQ2三元组签名。例如,对于 $k=9$ 和 $m=8$ ,只有一个GQ2三元组便

足够了；各个质问包含八个字节并且基数为2, 3, 5, 7, 11, 13, 17和19。

签名运算是由三个操作构成的操作序列：一个确认操作，一个质问操作和一个应答操作。各个操作产生一或多个 GQ2三元组，其中每个三元组包括：一个确认 $R(\neq 0)$ ，一个由 $m$ 个基本质问 $d_1, d_2, \dots, d_m$ 构成的质问 $d$ ，和一个应答 $D(\neq 0)$ 。

签名实体具有一个散列函数，参数 $k$ 和GQ2私有密钥，即基于上述三种表示中的一种的模数 $n$ 因数分解。在签名实体内部，可以通过隔离执行确认和应答操作的见证者来隔离证明者的最敏感功能和参数。为了计算确认和应答，见证者具有参数 $k$ 和GQ2私有密钥，即基于上述三种表示中的一种的模数 $n$ 因数分解。如此隔离的见证者类似于证明者内部定义的见证者。它可以对应于一个具体实施例，例如一个与共同构成签名实体的 PC连接的芯片卡，或 PC内部特别保护的程序，或芯片卡内部特别保护的程序。

1)涉及确认的操作包括下列运算。

当见证者具有从 $Q_1$ 到  $Q_m$ 的 $m$ 个私有数值和模数 $n$ 时，该见证者以随机和秘密的方式选择一或多个随机数值 $r(0 < r < n)$ ；接着通过接连 $k$ 次连续自乘(mod  $n$ )运算将各个随机数值 $r$ 转换成一个确认 $R$ 。

$$R \equiv r^k (\text{mod } n)$$

当见证者具有从 $p_1$ 到 $p_f$ 的 $f$ 个素数和 $m \times f$ 个私有分量 $Q_{i,j}$ 时，该见证者以随机和秘密的方式抽出一或多个包含 $f$ 个随机数值的集合：各个集合针对每个素数 $p_i(0 < r_i < p_i)$ 均具有一个随机数值  $r_i$ ；接着通过 $k$ 次连续自乘(mod  $p_i$ )运算将各个随机数值 $r_i$ 转换成一个确认分量 $R_i$ 。

$$R_i \equiv r_i^k (\text{mod } p_i)$$

对于包括 $f$ 个确认分量的各个集合，见证者根据中国余数技术建立一个确认。确认的数量与随机数集合一样多。

$$R = \text{中国余数}(R_1, R_2, \dots, R_f)$$

2)质问操作包括杂凑所有确认 $r$ 和要签名的消息 $M$ 以获得一个被签名实体用来构成一或多个均包括 $m$ 个基本质问的质问的散列码；各

个基本质问的取值范围为0到 $v/2-1$ ；例如对于 $k=9$ 和 $m=8$ ，各个质问包含八个字节。质问的数量与确认一样多。

$d=d_1, d_2, \dots, d_m$ ，即从杂凑 $(M, R)$ 结果中提取的数值

3)应答操作包含下列运算。

当见证者具有从 $Q_1$ 到 $Q_m$ 的 $m$ 个私有数值和模数 $n$ 时，见证者使用通过确认操作得到的各个随机数 $r$ 和基于基本质问的私有数值计算一或多个应答 $D$ 。

$$X \equiv Q_1^{d_1} \times Q_2^{d_2} \times \dots \times Q_m^{d_m} \pmod{n}$$

$$D \equiv r \times X \pmod{n}$$

当见证者具有 $f$ 个从 $p_1$ 到 $p_f$ 的素数和 $m \times f$ 个私有分量 $Q_{i,j}$ 时，见证者使用通过确认操作得到的各个随机数值集合并计算一或多个由 $f$ 个应答分量构成的集合：各个应答分量集合针对每个素数均包括一个分量。

$$X \equiv Q_{1,i}^{d_1} \times Q_{2,i}^{d_2} \times \dots \times Q_{m,i}^{d_m} \pmod{p_i}$$

$$D \equiv r_i \times X \pmod{p_i}$$

针对各个应答分量集合，见证者根据中国余数技术建立一个应答。应答的数量与质问一样多。

$$D = \text{中国余数}(D_1, D_2, \dots, D_f)$$

签名实体通过加入一个签名附录对消息 $M$ 进行签名，签名附录包括：

- 各个GQ2三元组，即各个确认 $R$ ，各个质问 $d$ 和各个应答 $D$ ，
- 或各个确认 $R$ 和各个对应的应答 $D$ ，
- 或各个质问 $d$ 和各个对应的应答 $D$ 。

根据签名附录的内容运行验证运算。区分三种情况。

如果附录包括一或多个三元组，检查运算包含两个时序无关紧要的独立过程。当且仅当下面两个条件被满足时控制者才接受签名消息。

首先，各个三元组必须是一致的(必须满足一个下面类型的适当关系)和可接受的(必须在非零数值上进行比较)。

$$R \times \prod_{i=1}^m G_i^{d_i} \equiv D^{2^k} \pmod{n} \text{ 否则 } R \equiv D^{2^k} \times \prod_{i=1}^m G_i^{d_i} \pmod{n}$$

例如, 通过一个基本运算序列转换应答D: 被k-1个基数乘法或除法运算(mod n)分隔的k个平方(mod n)。对于在第i个平方和第i+1个平方之间执行的第i个乘法或除法, 基本质问 d1的第i个位指示是否有必要使用 g1, 基本质问 d2的第i个位指示是否有必要使用 g2, ..., 基本质问 dm的第i个位指示是否有必要使用 gm。因而有必要检索签名附录中出现的各个确认R。

此外, 一或多个三元组必须与消息M关联起来。通过杂凑所有确认R和一个M, 获得一个散列码, 其中必须根据上述散列码恢复出各个质问d。

$d = d1, d2, \dots, dm$ , 与从杂凑(M, R)结果中提取的数值相同。

如果附录中没有质问, 则检查运算开始通过杂凑所有确认R和消息M重构一或多个质问d'。

$d = d'1, d'2, \dots, d'm$ , 即从杂凑(M, R)结果中提取的数值。

接着, 当且仅当各个三元组是一致的(满足一个下面类型的适当关系)和可接受的(在非零数值上进行比较), 控制者才接受签名消息。

$$R \times \prod_{i=1}^m G_i^{d'i} \equiv D^{2^t} \pmod{n} \text{ 否则 } R \equiv D^{2^t} \times \prod_{i=1}^m G_i^{d'i} \pmod{n}$$

如果附录中没有确认, 则检查运算开始根据下列两个公式中的一个适当的公式重构一或多个确认R'。重新建立的确认不应当为零。

$$R' \equiv D^{2^t} / \prod_{i=1}^m G_i^{d'i} \pmod{n} \text{ 否则 } R' \equiv D^{2^t} \times \prod_{i=1}^m G_i^{d'i} \pmod{n}$$

接着, 控制者必须杂凑所有确认R'和消息M以便重构各个质问d。

$d = d1, d2, \dots, dm$ , 与从杂凑(M, R')结果中提取的数值相同。

当且仅当各个重构的质问与附录中的对应质问相同时控制者才接受签名消息。

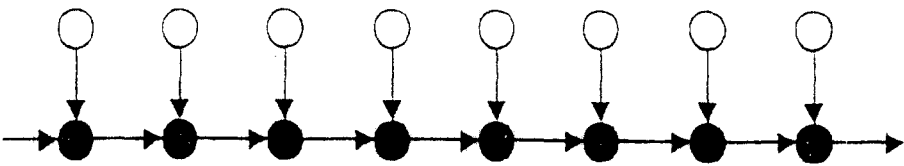


图 1A

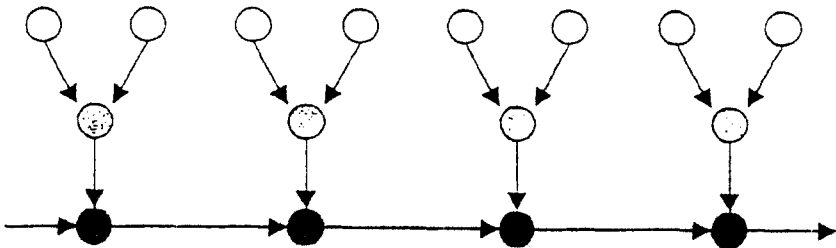


图 1B

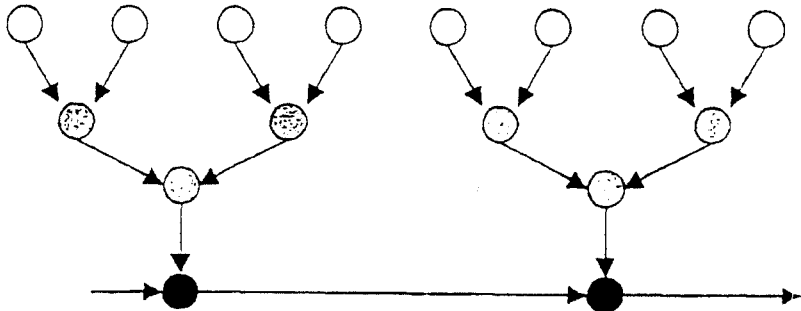


图 1C

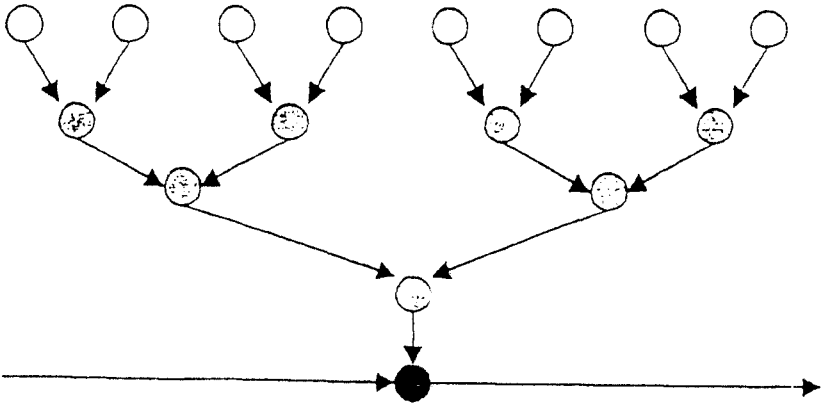


图 1D

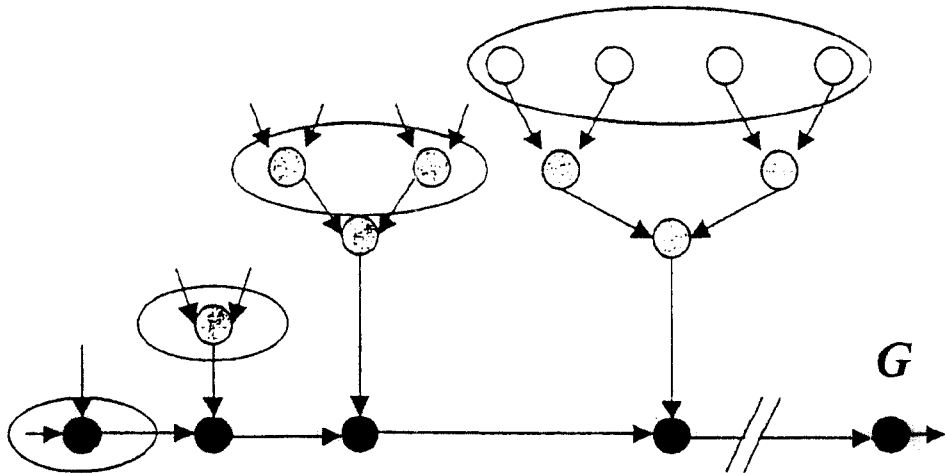


图 2A

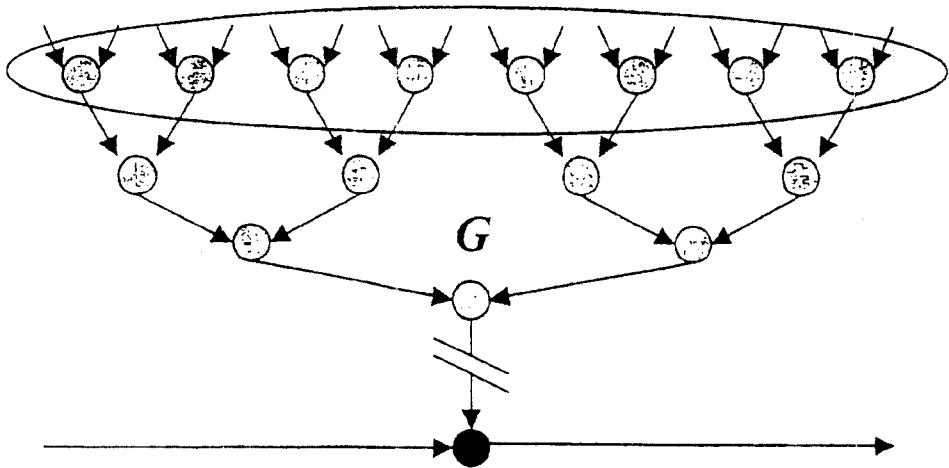


图 2B

