

[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 00803197.5

[45] 授权公告日 2008 年 3 月 26 日

[11] 授权公告号 CN 100377520C

[22] 申请日 2000.1.27 [21] 申请号 00803197.5
[30] 优先权

[32] 1999.1.27 [33] FR [31] 99/01065
[32] 1999.3.23 [33] FR [31] 99/03770
[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

[86] 国际申请 PCT/FR2000/000189 2000.1.27

[87] 国际公布 WO2000/046947 法 2000.8.10

[85] 进入国家阶段日期 2001.7.27

[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·基罗

让-加奎斯·奎斯括特

[56] 参考文献

EP0311470A 1989.4.12

EP0381523A 1999.8.8

审查员 崔宪丽

[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 吴丽丽

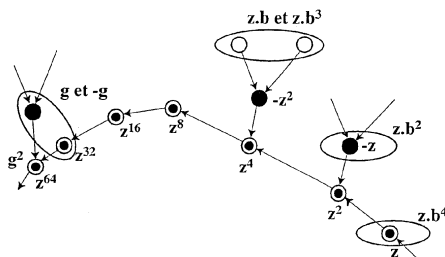
权利要求书 6 页 说明书 29 页 附图 4 页

[54] 发明名称

证实实体的真实性、消息的完整性和/或真实性的方法和系统

[57] 摘要

证明由下述参数提供：一个公共模数 n ，由 f 个素数 p_i 的乘积构成， $f > 2$ ；一个公共上标 v ； m 个基数 g_i ； $m > 1$ 。基数 g_i 是这样的基数，以致不能在整数模数 n 环中，求解两个等式 $x^2 \equiv g_i \pmod{n}$ 和 $x^2 \equiv -g_i \pmod{n}$ 的 x ，并且以致能够在整数模数 n 环中，求解等式 $x^v \equiv g_i^2 \pmod{n}$ 的 x ，其中公式上标 v 采用 $v = 2^k$ 的形式，其中 k 是安全参数。



1. 一种能够产生用于借助由 f 个素数 $p_1, p_2, \dots, p_f$ 的乘积构成的公共模数 n , f 等于或大于 2, 或者借助这 f 个素数, 向控制者实体证实下述内容的协议的 f 个素数 $p_1, p_2, \dots, p_f$ 的方法:

-实体的真实性和/或

-与该实体相关的消息 M 的完整性,

所述方法包括在保持下述条件的情况下, 产生所述 f 个素数 $p_1, p_2, \dots, p_f$ 的步骤:

在整数模数 n 环中, 均不可求解下述两个等式 (1) 和 (2) 的 x :

$$x^2 \equiv g_i \pmod{n} \quad \text{和} \quad x^2 \equiv -g_i \pmod{n}$$

并且能够在整数模数 n 环中, 求解下述等式 (3) 的 x :

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

$g_1, g_2 \dots g_m$ 表示 m 个不同的整数基数, m 大于或等于 1;

v 表示具有下述形式的公共指数:

$$v = 2^k$$

这里, k 是大于 1 的安全参数;

所述方法包括首先选择下述内容的步骤:

- 安全参数 k
- m 个基数 $g_1, g_2 \dots g_m$,
- 模数 n 的大小,
- f 个素数 $p_1, p_2, \dots, p_f$ 的大小。

2. 按照权利要求 1 所述的方法, 其特征在于所述 m 个基数 $g_1, g_2, \dots, g_m$ 是素数。

3. 按照权利要求 1 或 2 所述的方法, 其特征在于安全参数 k 是一个小整数, 尤其是小于 100 的整数。

4. 按照权利要求 1 或 2 所述的方法, 其特征在于模数 n 的大小大于几百个二进制位。

5. 按照权利要求 1 或 2 所述的方法, 其特征在于 f 个素数 $p_1, p_2, \dots$

p_f 的大小接近于被除以素数数目 f 的模数 n 的大小。

6. 按照权利要求 1 或 2 所述的方法, 其特征在于在 f 个素数 $p_1, p_2, \dots, p_f$ 内,

-选择全等于 $1 \pmod{4}$ 的 e 个素数, e 可能为 0 (如果 e 为 0, 则下面将把模数 n 称为基本模数, 如果 $e > 0$, 下面将把模数 n 称为复合模数),

-其它 $f-e$ 个素数被选择为全等于 $3 \pmod{4}$, $f-e$ 至少等于 2。

7. 按照权利要求 6 所述的方法, 其特征在于为了产生全等于 $3 \pmod{4}$ 的 $f-e$ 个素数 $p_1, p_2, \dots, p_{f-e}$,

执行下述步骤:

-选择全等于 $3 \pmod{4}$ 的第一素数 p_1 , 随后

-选择第二素数 p_2 , 以致相对于基数 g_1 , p_2 与 p_1 互补,

-执行下述程序, 区分两种情况, 选择素数 p_{i+1} :

(1) $i > m$ 的情况

-选择全等于 $3 \pmod{4}$ 的素数 p_{i+1} 。

(2) $i \leq m$ 的情况

-计算 g_i 相对于 i 个第一部分素数 p_i 的廓线 ($\text{Profile}_i(g_i)$):

· 如果 $\text{Profile}_i(g_i)$ 平直, 则选择该素数 p_{i+1} , 使得相对于 g_i , p_{i+1} 和 p_1 互补,

· 否则, 在 $i-1$ 个基数 $g_1, g_2, \dots, g_{i-1}$ 和它们的全部乘法组合中, 选择下面称为 g 的数字, 使得 $\text{Profile}_i(g) = \text{Profile}_i(g_i)$, 并且随后选择 p_{i+1} , 使得 $\text{Profile}_{i+1}(g_i) \neq \text{Profile}_{i+1}(g)$ 。

(术语“互补”, “廓线”, “平直廓线”具有在说明部分中定义的含义)。

8. 按照权利要求 7 所述的方法, 其特征在于为了选择最后的素数 p_{f-e} , 使用下述程序区分三种情况:

(1) $f-e-1 > m$ 的情况

· 选择全等于 $3 \pmod{4}$ 的 p_{f-e} ,

(2) $f-e-1 = m$ 的情况

相对于从 $p_1 \sim p_{f-e-1}$ 的 $f-e-1$ 个第一部分素数, 计算 $\text{Profile}_{f-e-1}(g_m)$,

· · 如果 $\text{Profile}_{f-e-1}(g_m)$ 平直, 则选择 p_{f-e-1} , 使得相对于 g_m , p_{f-e-1} 和 p_1 互补,

· · 否则:

· · · 在从 $g_1 \sim g_{m-1}$ 的 $m-1$ 个基数及它们的全部乘法组合中, 选择下面称为 g 的数字, 使得 $\text{Profile}_i(g) = \text{Profile}_i(g_i)$,

· · · 随后选择 p_{f-e} , 使得 $\text{Profile}_{f-e}(g) \neq \text{Profile}_{f-e}(g_m)$,

(3) $f-e-1 < m$ 的情况

· 选择 p_{f-e} , 以便满足下述两个条件:

(3.1) 第一条件

根据从 $p_1 \sim p_{f-e-1}$ 的 $f-e-1$ 个第一部分素数, 计算 $\text{Profile}_{f-e-1}(g_{f-e-1})$,

· · 如果 $\text{Profile}_{f-e-1}(g_{f-e-1})$ 平直, 则选择 p_{f-e} , 使得 p_{f-e} 满足相对于 g_{f-e-1} , p_{f-e} 和 p_1 互补的第一条件,

· · 否则,

· · · 在从 $g_1 \sim g_{m-1}$ 的 $f-e-1$ 个基数及它们的全部乘法组合之内, 选择下面称为 g 的数字, 使得 $\text{Profile}_i(g) = \text{Profile}_{f-e-1}(g_{f-e-1})$,

· · · 随后选择 p_{f-e} , 使得它满足使 $\text{Profile}_{f-e}(g) \neq \text{Profile}_{f-e}(g_m)$ 的第一条件,

(3.2) 第二条件

· 在从 $g_{f-e} \sim g_m$ 的所有最后一些基数之内, 选择其廓线 $\text{Profile}_{f-e-1}(g_i)$ 平直的那些基数, 随后

· 选择 p_{f-e} , 以致 p_{f-e} 满足相对于这样选择的每个基数, p_{f-e} 和 p_1 互补的第二条件。

9. 按照权利要求 7 或 8 所述的方法, 其特征在于为了产生全等于 $1 \pmod{4}$ 的 e 个素数, 在进行下述两个连续测试的情况下, 评估从 $p_{f-e} \sim p_f$ 的每个候选素数 p :

(1) 第一测试

- 计算从 $g_1 \sim g_m$ 的每个基数 g_i 相对于候选素数 p 的 Legendre 符号,

· 如果 Legendre 符号等于 -1 , 则拒绝候选素数 p ,

· 如果 Legendre 符号等于+1, 则转到下一基数, 继续候选素数 p 的评估, 并且随后当已考虑了最后一个基数时, 转到第二测试,

(2) 第二测试

-计算整数 t , 使得 $p-1$ 可被 2^t 除尽, 但是不可被 2^{t+1} 除尽, 随后

-计算整数 s , 使得 $s = (p-1+2^t) / 2^{t+1}$,

-把密钥 $\langle s, p \rangle$ 应用于每个公共值 G_i , 以便得到结果 r

$$r \equiv G_i^s \pmod{p}$$

· 如果 r 等于 g_i 或 $-g_i$, 则转到下一公共值 G_{i+1} , 继续第二测试,

· 如果 r 不等于 g_i 或 $-g_i$, 则应用下述算法, 计算因数 u :

· · 该算法由关于从 $1 \sim t-2$ 的上标 ii 规定的下述序列的重复组成:

· · 该算法实现两个变量: 由 r 初始化的 w 和取从 $2 \sim 2^{t-2}$ 的值的 $jj=2^{ii}$, 以及通过把密钥 $\langle (p-1)/2^t, p \rangle$ 应用于 $CG(p)$ 的非二次剩余而得到的数字 b , 随后重复下述步骤 1 和 2:

· · · 步骤 1: 计算 $w^2/G_i \pmod{p}$,

· · · 步骤 2: 使计算结果自乘到 2^{t-ii-1} 次幂,

· · · · 如果得到+1, 则转到下一公共值 G_{i+1} , 继续第二测试,

· · · · 如果得到-1, 则计算 $jj=2^{ii}$, 用 $w \cdot b^{jj} \pmod{p}$ 替换 w , 随后对具有上标 ii 的下一数值, 继续该算法,

· · 在算法结束时, 依据关系 $jj=2^{t-u}$, 变量 jj 的值被用于计算整数 u , 随后计算表达式 $t-u$, 出现两种情况:

· · · 如果 $t-u < k$, 则拒绝候选素数 p ,

· · · 如果 $t-u > k$, 继续候选素数 p 的评估, 并且随后继续第二测试, 并转到下一公共值 G_{i+1} , 如果在第二测试结束时, 对于所有 m 个公共值 G_i , 该候选素数 p 都未被拒绝, 则候选素数 p 被看作是全等于 $1 \pmod{4}$ 的素数。

10. 按照权利要求 1 或 2 所述的方法, 用于借助 m 对专用值 $Q_1, Q_2, \dots, Q_m$ 和公共值 $G_1, G_2, \dots, G_m$, 或者由这些值得出的参数, 向控

制实体证明下述内容:

-实体的真实性和/或

-与该实体相关的消息 M 的完整性;

所述模数和所述值由下述类型的关系连接:

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

所述公共值 G_i 是小于 f 个素数 $p_1, p_2, \dots, p_f$ 的基数 g_i 的平方 g_i^2 ,

在下述步骤中, 所述协议实现称为证人的实体, 所述证人实体具有 f 个素数 p_i 和/或素数的中国余数参数, 和/或公共模数 n 和/或 m 个专用值 Q_i 和/或专用值 Q_i 的 $f \cdot m$ 分量 $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \text{ mod } p_j$) 的参数, 以及公共指数 v 的参数;

-证人计算整数模数 n 环中的承诺 (commitment) R ; 每个承诺计算如下:

· 通过执行下述类型的运算:

$$R \equiv r^v \text{ mod } n$$

这里 r 是 $0 < r < n$ 的随机因数,

· 或者

· · 通过执行下述类型的运算:

$$R_i \equiv r_i^v \text{ mod } p_i$$

这里 r_i 是与素数 p_i 相关的随机值, 并且 $0 < r_i < p_i$, 每个 r_i 属于一个随机因数集合 $\{r_1, r_2, \dots, r_f\}$,

· · 随后通过应用中国余数方法, 计算每个承诺;

-证人接收一个或多个挑战 d , 每个挑战 d 包含下面称为基本挑战的 m 个整数 d_i , 根据每个挑战 d , 证人计算响应 D :

· 通过执行下述类型的运算:

$$D \equiv r \cdot Q_1^{d_1} \cdot Q_2^{d_2} \cdots Q_m^{d_m} \text{ mod } n$$

· 或者

· · 通过执行下述类型的运算:

$$D_i \equiv r_i \cdot Q_{i,1}^{d_1} \cdot Q_{i,2}^{d_2} \cdots Q_{i,m}^{d_m} \text{ mod } p_i$$

· · 并且随后应用中国余数方法, 计算响应 D ;

所述方法使得存在和挑战 d 及承诺 R 同样多的响应 D ，每组数字 R ， d ， D 构成表示为 $\{R, d, D\}$ 的三元组。

11. 按照权利要求 10 所述的方法，其特征在于为了实现如上所述的多对专用值 $Q_1, Q_2, \dots, Q_m$ 和公共值 $G_1, G_2, \dots, G_m$ ，所述方法使用素数 $p_1, p_2, \dots, p_f$ 和/或中国余数参数，基数 $g_1, g_2, \dots, g_m$ 和/或公共值 $G_1, G_2, \dots, G_m$ ：

-或者通过求 G_i 的第 k 个平方根模数 n ，或者通过取 G_i 的第 k 个平方根模数 n 的倒数，计算专用值 $Q_1, Q_2, \dots, Q_m$ ，

-或者计算专用值 $Q_1, Q_2, \dots, Q_m$ 的 $f \cdot m$ 专用分量 $Q_{i,j}$ ，使得 $Q_{i,j} \equiv Q_i \pmod{p_j}$ 。

12. 按照权利要求 11 所述的方法，其特征在于为了计算专用值 $Q_1, Q_2, \dots, Q_m$ 的 $f \cdot m$ 专用分量 $Q_{i,j}$ ：

-应用密钥 $\langle s, p_j \rangle$ 计算 z ，使得：

$$z \equiv G_i^s \pmod{p_j}$$

-并且使用 t 和 u 值，

-当 p_j 全等于 $1 \pmod{4}$ 时，如前所述计算 t 和 u 值，并且

· 当 p_j 全等于 $3 \pmod{4}$ 时， t 和 u 的值分别取为 1 ($t=1$) 和 0 ($u=0$)，

· · 如果 u 值为 0 ，则认为所有的数字 zz 为：

· · · zz 等于 z ，或者

· · · zz 等于 z 与 1 的 $2^{ii-t} 2^{ii}$ 次原根中的每个原根的乘积 $\pmod{p_j}$ ， ii 从 1 变化到 $\min(k, t)$ ，

· · 如果 u 为正数，则认为所有的数字 zz 等于 za 与 1 的 $2^k 2^k$ 次根中的每个根的乘积 $\pmod{p_j}$ ， za 表示在权利要求 10 中实现的算法结束时，变量 w 的值，

-据此推导出分量 $Q_{i,j}$ 的至少一个值，当使用等式 $G_i \equiv Q_i^v \pmod{n}$ 时，该值等于 zz ，否则，当使用等式 $G_i \cdot Q_i^v \equiv 1 \pmod{n}$ 时，该值等于 zz 的 $zz \pmod{p_j}$ 的倒数。

证实实体的真实性、消息的完整性和/或真实性的方法和系统

本发明涉及用于证实实体的真实性和/或消息的完整性和/或真实性的方法，系统和设备的技术领域。

Louis Guillou 和 Jean-Jacques Quisquater 的专利 EP 0311470B1 描述了这样一种方法。下面，将借助术语“GQ 专利”或“GQ 方法”提及他们的工作。下面，词句“GQ2”或“GQ2 发明”或“GQ2 技术”将用于描述 GQ 技术的新发展，所述 GQ 技术的新发展是由法国电信，TDF 和 Mathrizk 公司在和本申请同一天登记的待审批申请的目的，发明人是 Louis Guillou 和 Jean-Jacques Quisquater。在下面的说明中，每当需要时，就会再引用这些待审批申请的特征。

按照 GQ 方法，称为“受托管理机构”的实体向称为“证人”的每个实体分配一个身份，并计算其 RSA 签名。在定制过程中，受托管理机构给予证人一个身份和签名。之后，证人做出如下声明：“这是我的身份；我了解它的 RSA 签名”。在不泄漏真相的情况下，证人证明他知道他的身份的 RSA 签名。通过受托管理机构分配的 RSA 公用标识密钥，称为“控制者”的实体在不获得有关知识的情况下，确定 RSA 签名和声明实体相符。使用 GQ 方法的机制“在不传送知识的情况下”发生作用。按照 GQ 方法，证人不必知道 RSA 专用密钥，受托管理机构利用所述 RSA 专用密钥签署了大量的身份。

上面描述的 GQ 技术利用了 RSA 技术。但是，虽然 RSA 技术确实依赖于模数 n 的因数分解，但是这种相关性并不等效，如同可在针对实现 RSA 技术的数字签名的各种标准的所谓乘法攻击中看到的那样，事实上离等效差得很远。

GQ2 技术的目标在于两个方面：首先是提高 RSA 技术的工作特性，其次是防止 RSA 技术中固有的问题。GQ2 专用密钥的知识等同

于模数 n 的因数分解的知识。对三元组 GQ2 的任何攻击导致模数 n 的因数分解：此时存在等效性。借助 GQ2 技术，降低了签名或自我证明实体，以及控制实体的工作量。通过在安全和性能两方面，因数分解问题的更好地使用，GQ2 防止了 RSA 技术的缺陷。

GQ 方法实现包含 512 个或更多二进制位的数字的模数计算。这些计算涉及具有自乘到大约 2^{16} 次幂+1 的基本相同大小的数字。现在，现有的微电子基础结构，尤其是银行卡领域中的微电子基础结构使用不具有算术协理器的单片自动编程的微处理器。和诸如 GQ 方法之类的方法中所涉及的多重算术应用相关的工作量导致计算时间很长，在某些情况下，较长的计算时间被证明不利于顾客使用银行卡支付他们的购买。这里会回想起，在设法提高支付卡的安全性的情况下，银行管理机构已引起一个特别难以解决的问题。实际上，必须解决两个明显相互矛盾的问题；一方面，通过对于每个银行卡，使用越来越长并且截然不同的密钥，提高安全性，而另一方面，防止工作量耗费用户过多的计算时间。由于还必须考虑到现有的基础结构和现有的微处理器元件，该问题变得特别严重。

在提高安全性的同时，GQ2 技术提供了该问题的解决方案。

GQ2 技术实现特殊性质的素数。产生这些素数的现有技术有很多种。本发明的目的是这种素数的系统产生方法。本发明还涉及可由尤其是在 GQ2 技术的实现中的这些素数产生的应用。这里必须强调，在 GQ2 技术的领域之外，也可应用这些特殊的素数，以及用于获得这些素数的方法。

本发明可应用于设计成向控制者实体证实下述内容的方法（GQ2 方法）：

- 实体的真实性和/或
- 与该实体相关的消息 M 的完整性。

借助所有或部分下述参数或它们的衍生物产生这种证实：

-由 f 个素数 $p_1, p_2, \dots, p_f$ (f 等于或大于 2) 的乘积构成的公共模数 n ,

-公共指数 v ;

- m 个相异的整数基数 $g_1, g_2 \cdots g_m$ (m 大于或等于 1)。

基数 g_i 是这样的基数, 以致不能在整数模数 n 环中, 求解下述两个等式 (1) 和 (2) 的 x :

$$x^2 \equiv g_i \pmod{n} \quad \text{和} \quad x^2 \equiv -g_i \pmod{n}$$

并且以致能够在整数模数 n 环中, 求解等式 (3) 的 x :

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

根据本发明的方法被用于以满足等式 (1), (2) 和 (3) 的方式, 产生 f 个素数 $p_1, p_2, \cdots p_f$ 。根据本发明的方法包括首先选择下述内容的步骤:

m 个基数 $g_1, g_2 \cdots g_m$,

模数 n 的大小,

f 个素数 $p_1, p_2, \cdots p_f$ 的大小。

该方法涉及公共指数 v 具有下述形式的情况:

$$v = 2^k$$

这里, k 是大于 1 的安全参数。安全参数 k 也被选择为素数。这种特殊值的指数 v 是 GQ2 技术的本质特征之一。

最好, 至少部分地在第一部分整数内选择 m 个基数 $g_1, g_2, \cdots g_m$ 。安全参数 k 最好是一个小整数, 尤其是小于 100 的整数。模数 n 的大小最好大于几百个二进制位。 f 个素数 $p_1, p_2, \cdots p_f$ 的大小最好接近于被除以素数数目 f 的模数 n 的大小。

按照根据本发明的方法的一个主要特征, 不以任何非特定的方式选择 f 个素数 $p_1, p_2, \cdots p_f$ 在 f 个素数之内, 其中的一些素数: e 将被选择为全等于 1 (mod 4)。素数的该数目 e 可能为 0。如果 e 为 0, 则下面将把模数 n 称为基本模数。如果 $e > 0$, 下面将把模数 n 称为复合模数。其它 $f-e$ 个素数被选择为全等于 3 (mod 4)。素数的该数目 $f-e$ 至少等于 2。

全等于 3 (mod 4) 的 $f-e$ 个素数的选择

为了产生全等于 3 (mod 4) 的 $f-e$ 个素数 $p_1, p_2, \cdots p_{f-e}$ 。执行下

述步骤:

-选择全等于 $3 \pmod{4}$ 的第一素数 p_1 ,

-选择第二素数 p_2 , 以致相对于基数 g_1 , p_2 与 p_1 互补。

为了选择素数 p_{i+1} , 使用下述程序区分两种情况:

(1) $i > m$ 的情况

如果 $i > m$, 则选择全等于 $3 \pmod{4}$ 的素数 p_{i+1} 。

(2) $i \leq m$ 的情况

如果 $i \leq m$, 则计算 g_i 相对于 i 个第一部分素数 p_i 的廓线 ($\text{Profile}_i(g_i)$):

如果 $\text{Profile}_i(g_i)$ 平直, 则选择因数 p_{i+1} , 使得相对于 g_i , p_{i+1} 和 p_1 互补,

否则, 在 $i-1$ 个基数 $g_1, g_2, \dots, g_{i-1}$ 和它们的全部乘法组合中, 选择数字 g , 使得 $\text{Profile}_i(g) = \text{Profile}_i(g_i)$, 随后选择 p_{i+1} , 使得 $\text{Profile}_{i+1}(g_i) \neq \text{Profile}_{i+1}(g)$ 。

术语“互补”, “廓线”, “平直廓线”具有在说明部分中定义的含义。

为了选择最后的素数 p_{f-e} , 使用下述程序区分三种情况:

(1) $f-e-1 > m$ 的情况

如果 $f-e-1 > m$, 则选择全等于 $3 \pmod{4}$ 的 p_{f-e} 。

(2) $f-e-1 = m$ 的情况

如果 $f-e-1 = m$, 则相对于从 $p_1 \sim p_{f-e-1}$ 的 $f-e-1$ 个第一部分素数, 计算 $\text{Profile}_{f-e-1}(g_m)$ 。

如果 $\text{Profile}_{f-e-1}(g_m)$ 平直, 则选择 p_{f-e-1} , 使得相对于 g_m , p_{f-e-1} 和 p_1 互补,

否则, 进行下面规定的程序:

在从 $g_1 \sim g_{m-1}$ 的 $m-1$ 个基数及它们的全部乘法组合中, 选择下面称为 g 的数字, 使得 $\text{Profile}_i(g) = \text{Profile}_i(g_i)$, 随后选择 p_{f-e} , 使得 $\text{Profile}_{f-e}(g_i) \neq \text{Profile}_{f-e}(g_m)$ 。

(3) $f-e-1 < m$ 的情况

如果 $f-e-1 < m$, 则选择 p_{f-e} , 以便满足下述两个条件:

(3.1) 第一条条件

根据从 $p_1 \sim p_{f-e-1}$ 的 $f-e-1$ 个第一部分素数, 计算 $\text{Profile}_{f-e-1}(g_{f-e-1})$ 。随后考虑两种情况。根据这两种情况中的任意一种情况, 第一条条件将不同。

如果 $\text{Profile}_{f-e-1}(g_{f-e-1})$ 平直, 则选择 p_{f-e} , 使得 p_{f-e} 满足相对于 g_{f-e-1} , p_{f-e} 和 p_1 互补的第一条件 (根据第一种情况的第一条件)。否则, 在从 $g_1 \sim g_{m-1}$ 的 $f-e-1$ 个基数及它们的全部乘法组合之内, 选择下面称为 g 的数字, 使得 $\text{Profile}_i(g) = \text{Profile}_{f-e-1}(g_{f-e-1})$, 并且随后选择 p_{f-e} , 使得它满足使 $\text{Profile}_{f-e}(g) \neq \text{Profile}_{f-e}(g_m)$ 的条件 (根据第二种情况的第一条件)。

(3.2) 第二条条件

在从 $g_{f-e} \sim g_m$ 的所有最后一些基数之内, 选择其廓线 $\text{Profile}_{f-e-1}(g_i)$ 平直的那些基数, 随后选择 p_{f-e} , 以致 p_{f-e} 满足相对于这样选择的每个基数, p_{f-e} 和 p_1 互补的条件 (第二条条件)。

全等于 $1 \pmod{4}$ 的素数的选择

为了产生全等于 $1 \pmod{4}$ 的 e 个素数, 在进行下述两个连续测试的情况下, 评估从 $p_{f-e} \sim p_f$ 的每个候选素数 p :

(1) 第一测试

计算从 $g_1 \sim g_m$ 的每个基数相对于候选素数 p 的 Legendre 符号,

如果 Legendre 符号等于 -1 , 则拒绝候选素数 p ,

如果 Legendre 符号等于 $+1$, 则转到下一基数, 继续候选素数 p 的评估, 并且随后当已考虑了最后一个基数时, 转到第二测试。

(2) 第二测试

计算整数 t , 使得 $p-1$ 可被 2^t 除尽, 但是不可被 2^{t+1} 除尽, 随后计算整数 s , 使得 $s = (p-1+2^t) / 2^{t+1}$ 。

把密钥 $\langle s, p \rangle$ 应用于每个公共值 G_i , 以便得到结果 r

$$r \equiv G_i^s \pmod{p}$$

如果 r 等于 g_i 或 $-g_i$, 则转到下一公共值 G_{i+1} , 继续第二测试。

如果 r 不等于 g_i 或 $-g_i$, 则通过对于从 $1 \sim t-2$ 的上标 ii , 应用下面规定的算法, 计算因数 u 。该算法实现两个变量: 由 r 初始化的 w 和取从 $2 \sim 2^{t-2}$ 的值的 $jj=2^{ii}$, 以及通过把密钥 $\langle (p-1)/2^t, p \rangle$ 应用于 $CG(p)$ 的非二次剩余, 得到的数字 b 。该算法由根据需要多次重复下述程序组成:

- 步骤 1: 计算 $w^2/G_i \pmod{p}$,
- 步骤 2: 使计算结果自乘到 2^{t-ii-1} 次幂。考虑两种情况。

第一种情况

如果得到 $+1$, 则转到下一公共值 G_{i+1} , 并对该公共值进行第二测试。

第二种情况

如果得到 -1 , 则计算 $jj=2^{ii}$, 随后用 $w \cdot b^{jj} \pmod{p}$ 替换 w 。随后, 对于具有上标 ii 的下一数值, 继续该算法。

在算法结束时, 依据关系 $jj=2^{t-u}$, 变量 jj 的值被用于计算整数 u , 随后计算表达式 $t-u$ 。出现两种情况:

如果 $t-u < k$, 则拒绝候选素数 p ,

如果 $t-u > k$, 则转到下一公共值 G_{i+1} 继续候选素数 p 的评估, 并且随后继续第二测试。

如果在第二测试结束时, 对于所有 m 个公共值 G_i , 候选素数 p 都未被拒绝, 则候选素数 p 被看作是全等于 $1 \pmod{4}$ 的素数。

关于 GQ2 的公共值和专用值的应用

本发明还涉及应用上面描述的方法, 并且可回想起, 使得能够产生具有特殊性质的 f 个素数 $p_1, p_2, \dots, p_f$ 的一种方法 (GQ2 方法)。上面描述的方法的应用方法用于向控制者实体证明下述内容:

-实体的真实性和/或

-与该实体相关的消息 M 的完整性,

借助所有或部分下述参数或者这些参数的衍生物, 建立这种证明:

- m 对专用值 $Q_1, Q_2, \dots, Q_m$ 和公共值 $G_1, G_2, \dots, G_m$ (m 大于或等于 1),

-由所述 f 个素数 $p_1, p_2, \dots, p_f$ 的乘积构成的公共模数 n (f 大于或等于 2),

-公共指数 v .

所述模数, 所述指数和所述值由下述类型的关系连接:

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

所述指数为 $v=2^k$

其中 k 是大于 1 的安全参数。

所述公共值 G_i 是小于 f 个素数 $p_1, p_2, \dots, p_f$ 的基数 g_i 的平方 g_i^2 。
基数 g_i 是这样的基数, 以致不能在整数模数 n 环中, 求解下述两个等式的 x :

$$x^2 \equiv g_i \text{ mod } n \quad \text{和} \quad x^2 \equiv -g_i \text{ mod } n$$

并且以致能够在整数模数 n 环中, 求解下述等式的 x :

$$x^v \equiv g_i^2 \text{ mod } n$$

所述方法按照下述步骤实现称为证人的实体。所述证人实体具有 f 个素数 p_i 和/或素数的中国余数参数, 和/或公共模数 n 和/或 m 个专用值 Q_i 和/或专用值 Q_i 的 $f.m$ 分量 ($Q_{i,j} \equiv Q_i \text{ mod } p_j$) 的参数, 以及公共指数 v 的参数。

证人计算整数模数 n 环中的承诺 (commitment) R 。或者通过执行下述类型的运算, 计算每个承诺, 方式是:

· 通过执行下述类型的运算:

$$R \equiv r^v \text{ mod } n$$

这里 r 是大于 0, 小于 n 的随机因数,

· 或者通过执行下述类型的运算:

$$R_i \equiv r_i^v \text{ mod } p_i$$

这里 r_i 是与素数 p_i 相关的随机值, 并且 $0 < r_i < p_i$, 每个 r_i 属于一组随机因数 $\{r_1, r_2, \dots, r_f\}$ 的集合, 随后通过应用中国余数方法, 计算每个承诺。

证人接收一个或多个挑战 d 。每个挑战 d 包含下面称为基本挑战的 m 个整数 d_i 。根据每个挑战 d , 证人或者通过执行下述类型的运算,

计算响应 D:

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

或者通过执行下述类型的运算:

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

并且随后应用中国余数方法, 计算响应 D。

该方法使得存在和挑战 d 及承诺 R 同样多的响应 D, 每组数字 R, d, D 构成表示为 {R, d, D} 的三元组。

为了实现上面所述的多对专用值 $Q_1, Q_2, \dots, Q_m$ 和公共值 $G_1, G_2, \dots, G_m$, 该方法使用素数 $p_1, p_2, \dots, p_f$ 和/或中国余数参数, 基数 $g_1, g_2, \dots, g_m$ 和/或公共值 $G_1, G_2, \dots, G_m$:

-通过求 G_i 的第 k 个平方根模数 n, 或者通过取 G_i 的第 k 个平方根模数 n 的倒数, 计算专用值 $Q_1, Q_2, \dots, Q_m$

-或者计算专用值 $Q_1, Q_2, \dots, Q_m$ 的 f.m 个专用分量 $Q_{i,j}$, 使得 $Q_{i,j} \equiv Q_i \pmod{p_j}$ 。

更具体地说, 为了计算专用值 $Q_1, Q_2, \dots, Q_m$ 的 f.m 个专用分量 $Q_{i,j}$:

-应用密钥 $\langle s, p_j \rangle$ 计算 z, 使得:

$$z \equiv G_i^s \pmod{p_j}$$

-并且使用 t 和 u 值。

当 p_j 全等于 1 (mod 4) 时, 如前所述计算 t 和 u 值。当 p_j 全等于 3 (mod 4) 时, t 和 u 的值分别取为 1 和 0 ($t=1, u=0$)。

如果 u 值为 0, 我们认为所有的数字 zz 为:

· · · zz 等于 z, 或者

· · · zz 等于 z 与 1 的 $2^{ii-t} 2^{ii}$ 次原根中的每个原根的乘积 (mod p_j),

ii 从 1 变化到 $\min(k, t)$ 。

如果 u 为正数, 我们认为所有的数字 zz 等于 za 与 1 的 $2^k 2^k$ 次根中的每个根的乘积 (mod p_j), za 表示上面描述的算法结束时, 变量 w 的值。

据此推导出分量 $Q_{i,j}$ 的至少一个值。当使用等式 $G_i \equiv Q_i^r \bmod n$ 时,

该值等于 zz , 否则, 当使用等式 $G_i \cdot Q_i^v \equiv 1 \cdot \text{mod } n$ 时, 该值等于 zz 的 $zz(\text{mod } p_j)$ 的倒数。

说明

可回想 GQ 技术的目的: 其目的是实体和相关消息的动态证明, 以及消息的数字签名。

标准形式的 GQ 技术利用 RSA 技术。但是, 尽管 RSA 技术确实依赖于因数分解, 但是这种相关性并不等效, 可从针对实现 RSA 技术的各种数字签名标准的称为乘法攻击的攻击中看到, 事实上离等效差得很远。

在 GQ2 技术的环境下, 本发明的本部分更具体地涉及用于提供动态证明和数字签名的成组 GQ2 密钥的产生。GQ2 技术并不使用 RSA 技术。GQ2 的目标在于两个方面: 首先是提高 RSA 技术的性能, 其次是防止 RSA 技术中固有的问题。GQ2 专用密钥是模数 n 的因数分解。对 GQ2 三元组的任何攻击相当于模数 n 的因数分解: 此时存在等效性。借助 GQ2 技术, 降低了签名或证明实体, 以及控制实体的工作量。通过在安全和性能两方面, 因数分解问题的更好地使用, GQ2 比得上 RSA 技术。

GQ2 技术使用一个或多个大于 1 的小整数, 例如称为基数, 并以 g_i 表示的 m 个小整数 ($m \geq 1$)。随后, 如下所述选择公共验证密钥 $\langle v, n \rangle$ 。公共验证密钥 v 为 2^k , k 是大于 1 的小整数 ($k \geq 2$)。公共模数 n 是大于基数的至少两个素数的乘积, 例如表示为 p_j 的 f 个素数 ($f \geq 2$), $p_1 \cdots p_f$ 。选择 f 个素数, 以便相对于 m 个基数 ($g_1 \cdots g_m$) 中的每个基数, 公共模数 n 具有下述性质:

-首先, 不能用整数模数 n 环中的 x 解答等式 (1) 和 (2), 即, g_i 和 $-g_i$ 是两个非二次剩余 ($\text{mod } n$)。

$$x^2 \equiv g_i (\text{mod } n) \quad (1)$$

$$x^2 \equiv -g_i (\text{mod } n) \quad (2)$$

-其次, 可用整数模数 n 环中的 x 解答等式 (3)。

$$x^{2^t} \equiv g_i^2 (\text{mod } n) \quad (3)$$

下面, 这些性质也被称为 GQ2 原理。

由于按照从 g_1 - g_m ($m \geq 1$) 的基数, 公共验证密钥 $\langle v, n \rangle$ 是固定的, 因此每个基数 g_i 确定包含公共值 G_i 和专用值 Q_i 的一对值 GQ2: 产生表示为 $G_1 Q_1$ - $G_m Q_m$ 的 m 对值。公共值 G_i 是基数 g_i 的平方: $G_i = g_i^2$ 。专用值 Q_i 是等式 (3) 的解答或者这种解答的反 (mod n)。

如同模数 n 被分解为 f 个素数一样, 整数模数 n 环被分解为 f 个伽罗瓦域, 从 $CG(p_1)$ 到 $CG(p_f)$ 。下面是等式 (1), (2) 和 (3) 在 $CG(p_i)$ 中的投影。

$$x^2 \equiv g_i \pmod{p_i} \quad (1.a)$$

$$x^2 \equiv -g_i \pmod{p_i} \quad (2.a)$$

$$x^{2^t} \equiv g_i^2 \pmod{p_i} \quad (3.a)$$

每个专用值 Q_i 可唯一地由 f 个专用分量表示, 每个素数对应一个专用分量: $Q_{i,j} \equiv Q_i \pmod{p_j}$ 。每个专用分量 $Q_{i,j}$ 是等式 (3.a) 的解答或者这种解答的反 (mod p_j)。在计算了每个等式 (3.a) 的所有可能解答之后, 中国余数方法根据 f 个分量 $Q_{i,1}$ - $Q_{i,f}$ 确定每个专用值 Q_i 的可能数值: $Q_i = \text{中国余数}(Q_{i,1}, Q_{i,2}, \dots, Q_{i,f})$, 以便获得等式 (3) 的所有可能解答。

下面是中国余数方法: 假定存在互为素数的两正整数 a 和 b , $0 < a < b$, 以及两个分量, 从 0 到 $a-1$ 的 X_a 和从 0 到 $b-1$ 的 X_b 。需要确定 $X = \text{中国余数}(X_a, X_b)$, 即 0 到 $a.b-1$ 的单一数字 X , 以致 $X_a \equiv X \pmod{a}$ 和 $X_b \equiv X \pmod{b}$ 。下面是中国余数参数: $\alpha \equiv \{b \pmod{a}\}^{-1} \pmod{a}$ 。下面是中国余数运算: $\varepsilon \equiv X_b \pmod{a}$; $\delta = X_a - \varepsilon$; 如果 δ 为负, 用 $\delta + a$ 替换 δ ; $\gamma \equiv \alpha \delta \pmod{a}$; $X = \gamma.b + X_b$ 。

当素数按照升序, 从最小的 p_1 到最大的 p_f 排列时, 中国余数参数可以如下所示 (存在 $f-1$, 即至少素数之一)。第一中国余数参数是 $\alpha \equiv \{p_2 \pmod{p_1}\}^{-1} \pmod{p_1}$ 。第二中国余数参数是 $\beta \equiv \{p_1.p_2 \pmod{p_3}\}^{-1} \pmod{p_3}$ 。第 i 个中国余数参数是 $\lambda \equiv \{p_1.p_2 \dots p_{i-1} \pmod{p_i}\}^{-1} \pmod{p_i}$, 依次类推。最后, 在 $f-1$ 中国余数运算中, 利用第一参数得到第一结果 (mod $p_2 \times p_1$), 随后利用第二参数得到第二结果 (mod $p_1.p_2 \times p_3$), 依次类推, 直到

得到结果 $(\text{mod } p_1 \cdots p_{f-1} \times p_f)$ ，即 $(\text{mod } n)$ 为止。

本发明的目的是一种随机产生所有各组可能的 GQ2 密钥中的任意一组 GQ2 密钥的方法，即：

-所有可能的 GQ2 模数内的任意模数的随机产生，即对于 m 个基数 g_i 中的每个基数，该模数确保不能用整数模数 n 环中的 x 解答等式 (1) 和 (2)，而可用整数模数 n 环中一个整数模数解答等式 (3)，

-计算每个等式 (3.a) 的所有可能解答。中国余数方法使得能够根据每组 f 个分量 $(Q_{i,1}-Q_{i,f})$ ，得到专用值 Q_i ，从而获得所有 ht 可能等式内，等式 (3) 的任意解答 x 。

$$Q_i = \text{中国余数}(Q_{i,1}, Q_{i,2}, \dots, Q_{i,f})$$

为了了解该问题，并且随后理解将针对该问题给出的解决方案，即本发明，我们首先分析 GQ2 技术的原理的适用性。让我们首先从回忆伽罗瓦域 $CG(p)$ 中的秩的概念开始，以便研究函数“ $CG(p)$ 中自乘到平方”和“ $CG(p)$ 中二次剩余的开平方”。随后，我们将分析关于等式 (1.a)，(2.a) 和 (3.a)， $CG(p)$ 中解答 x 的存在及数目。

$CG(p)$ 中元素的秩

取一个奇素数 p 和小于 p 的一个正素数。之后，定义 $\{X\}$ 。

$$\{X\} \equiv \{x_1 = a; \text{ 则对于 } i \geq 1, x_{i+1} \equiv a \cdot x_i (\text{mod } p)\}$$

计算下标为 $i+p$ 的项，并使用 Fermat 定理：

$$x_{i+p} \equiv a^p x_i \equiv a \cdot x_i \equiv x_{i+1} (\text{mod } p)$$

因此，序列 $\{X\}$ 的周期为 $p-1$ 或者 $p-1$ 的除数。该周期取决于 a 的值。根据定义，该周期被称为“ $a (\text{mod } p)$ 的秩”。它是序列 $\{X\}$ 中 1 的出现下标。

$$x_{\text{rank}(a,p)} \equiv 1 (\text{mod } p)$$

例如，当 $(p-1)/2$ 是奇素数 p' 时，伽罗瓦域 $CG(p)$ 包含秩为 1 的单个元素： $(p-1)/2$ 为 1，秩为 2 的单个元素。 $(p-1)/2$ 为 -1，秩为 p' 的 $p'-1$ 个元素，秩为 $2 \cdot p'$ 的 $p'-1$ 个元素，即秩为 $p-1$ 。

$CG(p)$ 的秩为 $p-1$ 的元素被称为基本元素，或者也被称为 $CG(p)$

发生器。该名称缘于 $CG(p)$ 中它们的连续乘幂，即 $\{X\}$ 序列中的下标从 $1 \sim p-1$ 的项构成 $CG(p)$ 的所有非零元素的排列。

根据 $CG(p)$ 的基本元素 y ，我们来求作为 i 和 $p-1$ 的函数的元素 $y^i \pmod{p}$ 的秩。当 i 是具有 $p-1$ 的素数时，秩为 $p-1$ 。当 i 除以 $p-1$ 时，秩为 $(p-1)/i$ 。在所有情况下，秩为 $(p-1)/\text{pgcd}(p-1, i)$ 。

用 ϕ 表示 Euler 函数。根据定义，由于 n 是正整数，因此 $\phi(n)$ 是小于 n 的正整数（包括 n 在内的素数）的数目。于是，在域 $CG(p)$ 中，存在 $\phi(p-1)$ 个基本元素。

举例来说，下面是 RSA 技术的基础。公共模数 n 是从 $p_1 \sim p_f$ ($f \geq 2$) 的 f 个素数的乘积，从而对于每个素数 p_j 来说，公共指数 v 是包括 p_j-1 在内的一个素数。密钥 $\langle v, p_j \rangle$ 遵守 $CG(p_j)$ 的元素的秩：密钥 $\langle v, p_j \rangle$ 排列 $CG(p_j)$ 的元素。利用密钥 $\langle s_j, p_j \rangle$ ，获得反向排列，从而 p_j-1 除以 $v \cdot s_j - 1$ 。

$CG(p)$ 中的平方和平方根

在 $CG(p)$ 中，元素 x 和 $p-x$ 具有相同的平方。由于 $p-1$ 是个偶数值，因此密钥 $\langle 2, p \rangle$ 不排列 $CG(p)$ 的元素。对于每个素数 p ，我们如下定义一个整数 t ： $p-1$ 可被 2^t 除尽，但是不可被 2^{t+1} 除尽，即 p 全等于 $2^{t+1} \pmod{2^{t+1}}$ 。例如，当 p 全等于 $3 \pmod{4}$ 时， $t=1$ ；当 p 全等于 $5 \pmod{8}$ 时， $t=2$ ；当 p 全等于 $9 \pmod{16}$ 时， $t=3$ ；当 p 全等于 $17 \pmod{32}$ 时， $t=4$ ；依次类推。在一个范畴内，并且只在一个范畴内找到各个奇素数：在第 t 个范畴内找到 p 。实际上，如果我们考虑相当大量的连续素数，每 2 个中约有 1 个可在第一范畴内找到，每 4 个中有 1 个可在第二范畴内找到，每 8 个中有 1 个可在第三范畴内找到，每 16 个中有 1 个可在第四范畴内找到，依次类推。总之，平均来说，每 2^t 个中有 1 个可在第 t 范畴内找到。

下面让我们根据变元的秩的奇偶性，来考虑函数“ $CG(p)$ 中自乘到平方”的行为。

-只存在一个固定元素：该元素为 1。奇校验秩的任意其它元素的平方是具有相同秩的另一元素。从而，密钥 $\langle 2, p \rangle$ 排列其所有 $(p-1)$

$/2^t$ 奇校验秩元素。排列循环的数目取决于 $(p-1)/2^t$ 的因数分解。例如，当 $(p-1)/2^t$ 是素数 p' 时，存在包含 $p'-1$ 个元素的大排列循环。

-任意偶校验秩元素的平方是其秩被除以 2 的另一元素。从而，偶校验秩元素被分配在 $(p-1)/2^t$ 个分支上。具有奇校验秩的每个非零元素支承长度为 t 的包含 2^t-1 个元素的分支，即：秩可被 2 除尽，但是不可被 4 除尽的一个元素，随后，如果 $t \geq 2$ ，则秩可被 4 除尽，但是不可被 8 除尽的两个元素，如果 $t \geq 3$ ，则秩可被 8 除尽，但是不可被 16 除尽的四个元素，如果 $t \geq 4$ ，则秩可被 16 除尽，但是不可被 32 除尽的八个元素，依次类推。每个分支的 2^t-1 个末端是非二次剩余；它们的秩可被 2^t 除尽。

图 1A-1D 借助有向图，图解说明了函数“CG(p) 中自乘到平方”，这里域的 $p-1$ 个非零元素中的每个元素找到其自己的位置：非二次剩余为白色，二次剩余为黑色；在二次剩余内，奇校验秩元素在圆圈内。

这些图分别表示了：

- 图 1A: p 全等于 $3 \pmod{4}$ 的情况；
- 图 1B: p 全等于 $5 \pmod{8}$ 的情况；
- 图 1C: p 全等于 $9 \pmod{16}$ 的情况；
- 图 1D: p 全等于 $17 \pmod{32}$ 的情况。

现在我们来考虑计算等式 $x^2 \equiv a \pmod{p}$ 的解答 x 的方法(已知 a 是 CG(p) 的二次剩余)，即如何“在 CG(p) 中开平方”。当然，存在获得相同结果的多种途径：读者可参考 Henri Cohen 的“A Course in Computational Algebraic Number Theory”，Springer, Berlin, 1993 年出版，第 31-36 页，以及“Graduate Texts in Mathematics”，vol. 138 (GTM 138)。

我们来计算整数 $s = (p-1+2^t)/2^{t+1}$ ，以确定密钥 $\langle s, p \rangle$ 。假定：当 p 全等于 $3 \pmod{4}$ 时， $\langle (p+1)/4, p \rangle$ ，当 p 全等于 $5 \pmod{8}$ 时， $\langle (p+3)/8, p \rangle$ ，当 p 全等于 $9 \pmod{16}$ 时， $\langle (p+7)/16, p \rangle$ ，当 p 全等于 $17 \pmod{32}$ 时， $\langle (p+15)/32, p \rangle$ ，依次类推。

-密钥 $\langle s, p \rangle$ 给出任何奇校验秩元素的奇校验秩平方根。实际上，

在 $CG(p)$ 中, r^2/a 等于 a 自乘到 $(2 \cdot (p-1+2^t)/2^{t+1}) - 1 = (p-1)/2^t$ 次幂。从而, 当 a 处于循环中时, 密钥 $\langle s, p \rangle$ 把 a 转换为我们将称之为 w 的解答。另一解答是 $p-w$ 。

-通常, 密钥 $\langle s, p \rangle$ 把任意二次剩余 a 转换为将被称为 r 的解答的一级近似。下面是逐步改进近似, 直到 a 的平方根为止的示意方法之前的两个关键点。

-首先, 由于 a 是二次剩余, 密钥 $\langle 2^{t-1}, p \rangle$ 确实把 r^2/a 转换为 1。

-其次, 可假定我们知道我们命名为 y 的 $CG(p)$ 的非二次剩余; 密钥 $\langle (p-1)/2^t, p \rangle$ 把 y 转换为将被称为 b 的元素: 它是 -1 的第 2^{t-1} 个根。实际上, $y^{(p-1)/2} \equiv -1 \pmod{p}$ 。从而, 在 $CG(p)$ 中, 1 的第 2^t 次根的乘法组与指数为 $1 \sim 2^t$ 的 b 的乘幂的乘法组具有同一构造。

-为了逼近 a 的平方根, 我们使 r^2/a 自乘到 $2^{t-2} \pmod{p}$ 次幂: 结果为 +1 或 -1。如果结果为 +1, 则保持新的近似值, 如果结果为 -1, 则近似值变为 $b \cdot r \pmod{p}$ 。从而, 密钥 $\langle 2^{t-2}, p \rangle$ 必定把新的近似值转换为 1。可以继续逼近所需的数值: 在下一步骤, 如果需要的话, 通过乘以 $b^2 \pmod{p}$, 可进行调整, 依次类推。

下面的算法根据如上定义的整数 r 和 b , 进行逐步逼近, 以便达到 a 的平方根; 它使用两个整数变量: 由 r 初始化的 w , 以表示逐步逼近, 及假定从 $2 \sim 2^{t-2}$ 的 2 的乘幂之中的数值的 jj 。

对于从 $1 \sim t-2$ 的 i , 重复下述程序:

-计算 $w^2/a \pmod{p}$, 随后使结果自乘到 $2^{t-i-1} \pmod{p}$ 次幂: 应得到 +1 或 -1。当得到 -1 时, 计算 $jj=2^i$, 随后用 $w \cdot b^{jj} \pmod{p}$ 替换 w 。当得到 +1 时, 不进行任何操作。

在计算的结尾, w 和 $p-w$ 是 $CG(p)$ 中, a 的两个平方根。此外, 我们认识到在 $CG(p)$ 中, a 的秩可被 $2^t/jj$ 除尽, 但是不可被 $2^{t+1}/jj$ 除尽。下面将进一步领会这种观测结果的相关性。

CG(p) 中, GQ2 技术原理的分析

我们取大于 1 的两个整数 g 和 k , 以及大于 g 的一个素数 p 。我们来分析在 $CG(p)$ 中, 等式 (1.a), (2.a) 和 (3.a) 中的解答的存

在和数目。

在伽罗瓦域 $CG(p)$ 中，我们根据 t 的数值，即除尽 $p-1$ 的 2 的乘幂，来区别不同的情况。可回想起 $p-1$ 可被 2^t 除尽，但是不可被 2^{t+1} 除尽，即， p 全等于 $2^t+1 \pmod{2^{t+1}}$ 。前面的分析给了我们对于引起的问题及大致解决方案的相当精确的了解。

当 $t=1$ 时， p 全等于 $3 \pmod{4}$ 。 g 和 $-g$ 相对于 p 的 Legendre 符号不同： $CG(p)$ 的任意二次剩余具有 $CG(p)$ 中的两个平方根：一个是二次剩余，另一个是非二次剩余。首先，在 $CG(p)$ 中，两个等式 (1.a) 或 (2.a) 之一具有 x 的两个解答，而另一等式不具有任何解答。其次，无论任何 k 值，在 $CG(p)$ 中，等式 (3.a) 都具有 x 的两个解答。

当 $t=2$ 时， p 全等于 $5 \pmod{8}$ 。根据 g 相对于 p 的 Legendre 的符号，产生两种情况。当符号等于 -1 时， g 和 $-g$ 都是 $CG(p)$ 的非二次剩余：在 $CG(p)$ 中，三个等式 (1.a)，(2.a) 和 (3.a) 都不具有 x 的任何解答。当符号等于 $+1$ 时， g 和 $-g$ 是 $CG(p)$ 的两个二次剩余，等式 (1.a) 和 (2.a) 均具有 x 的 2 个解答。此外， $CG(p)$ 中， g^2 的秩为奇校验值，意味着不论什么样的 k 值，在 $CG(p)$ 中，等式 (3.a) 都具有 x 的 4 个解答，其中只有一个具有奇校验秩。

图 2 图解说明了假定 $t=2$ ，在 $k=6$ ， p 全等于 $5 \pmod{8}$ 的情况下，等式 (3.a) 的解答。要指出的是，由于相对于 p 全等于 $5 \pmod{8}$ ，2 的 Legendre 符号等于 -1 。则 $2^{(p-1)/4} \pmod{p}$ 为 -1 的平方根。于是，我们得到：

$$p \equiv 5 \pmod{8} ; \text{ 因此 } (2|p) = -1$$

$$p \equiv 2^{\frac{p-1}{4}} \pmod{p} ; \text{ 从而, } b^2 \equiv -1 \pmod{p}$$

当 $t=3$ 时， p 全等于 $9 \pmod{16}$ 。我们来考虑 g 相对于 p 的 Legendre 符号。当该符号等于 -1 时， g 和 $-g$ 是 $CG(p)$ 中的两个非二次剩余：在 $CG(p)$ 中，三个等式 (1.a)，(2.a) 和 (3.a) 都不具有 x 的任何解答。当符号等于 $+1$ 时， g 和 $-g$ 是 $CG(p)$ 的两个二次剩余，在 $CG(p)$ 中，等式 (1.a) 和 (2.a) 均具有 x 的 2 个解答。等式 (3.a) 的

x 解答的存在取决于 $CG(p)$ 中 g^2 的秩。该秩为奇校验值或者可被 2 除尽, 但是不可被 4 除尽。当 $CG(p)$ 中, g^2 的秩可被 2 除尽, 但是不可被 4 除尽时, 对于 $k=2$, 在 $CG(p)$ 中, 等式 (3.a) 具有 x 的 4 个解答; 它不能超过 $k \geq 3$ 。当 $CG(p)$ 中, g^2 的秩为奇校验值时, 对于 $k=2$, 在 $CG(p)$ 中, 等式 (3.a) 具有 x 的 4 个解答, 对于 $k \geq 3$, 在 $CG(p)$ 中, 等式 (3.a) 具有 x 的 8 个解答。在两种情况下, 只有一个值是奇校验值。

当 $t=4$ 时, p 全等于 $17 \pmod{32}$ 。我们来考虑 g 相对于 p 的 Legendre 符号。当该符号等于 -1 时, g 和 $-g$ 是 $CG(p)$ 的两个非二次剩余: 在 $CG(p)$ 中, 三个等式 (1.a), (2.a) 和 (3.a) 都不具有 x 的任何解答。当符号等于 +1 时, g 和 $-g$ 是 $CG(p)$ 的两个二次剩余, 在 $CG(p)$ 中, 等式 (1.a) 和 (2.a) 均具有 x 的 2 个解答。等式 (3.a) 的 x 解答的存在取决于 $CG(p)$ 中 g^2 的秩。该秩为奇校验值或者可被 2 或 4 除尽, 但是不可被 8 除尽。当 $CG(p)$ 中, g^2 的秩可被 2 除尽, 但是不可被 8 除尽时, 对于 $k=2$, 在 $CG(p)$ 中, 等式 (3.a) 具有 x 的 4 个解答; 它不能超过 $k \geq 3$ 。当 $CG(p)$ 中, g^2 的秩可被 2 除尽, 但是不可被 4 除尽时, 对于 $k=2$, 在 $CG(p)$ 中, 等式 (3.a) 具有 x 的 4 个解答, 或者对于 $k=3$, 在 $CG(p)$ 中, 等式 (3.a) 具有 x 的 8 个解答; 对于 $k \geq 4$, 等式 (3.a) 无解。当 $CG(p)$ 中, g^2 的秩为奇校验值时, 对于 $k=2$, 在 $CG(p)$ 中, 等式 (3.a) 具有 x 的 4 个解答, 对于 $k \geq 3$, 在 $CG(p)$ 中, 等式 (3.a) 具有 x 的 4 个解答, 对于 $k \geq 4$, 在 $CG(p)$ 中, 等式 (3.a) 具有 x 的 16 个解答。在所有三种情况下, 只有一个值是奇校验值。

依次类推, 从而可如下总结 p 全等于 $1 \pmod{4}$ 的情况。

当 p 全等于 $1 \pmod{4}$ 时, 我们来考虑 g 相对于 p 的 Legendre 符号。当该符号等于 -1 时, g 和 $-g$ 是 $CG(p)$ 的两个非二次剩余: 在 $CG(p)$ 中, 三个等式 (1.a), (2.a) 和 (3.a) 都不具有 x 的任何解答。当符号等于 +1 时, g 和 $-g$ 是 $CG(p)$ 的两个二次剩余; 在 $CG(p)$ 中, 等式 (1.a) 和 (2.a) 均具有 x 的 2 个解答。我们来定义一

个整数 u : $CG(p)$ 中, g^2 的秩可被 2^u 除尽, 但是不可被 2^{u+1} 除尽。值 u 是从 $0 \sim t-2$ 的 $t-1$ 个可能值之一。 $CG(p)$ 中, 等式 (3.a) 的 x 解答的存在及数目取决于 k , t 和 u 的值。当 u 是正数, 并且 k 大于 $t-u$ 时, 在 $CG(p)$ 中, 等式 (3.a) 不具有 x 的解答。当 u 为零, 并且 k 大于 t 时, 在 $CG(p)$ 中, 等式 (3.a) 具有 x 的 2^t 个解答。当 k 小于或等于 $t-u$ 时, 在 $CG(p)$ 中, 等式 (3.a) 具有 x 的 2^k 个解答。

GQ2 原理在整数模数环中的适用性

为了在整数模数 n 的环中, 等式 (1) 和 (2) 均不具有 x 的解, 其必要充分条件是, 对于从 $p_1 \sim p_r$ 的 至少一个素数 p , 等式 (1.a) 和 (2.a) 必须在 $CG(p)$ 中均不具有 x 的解答。

为了在整数模数 n 的环中, 等式 (3) 具有 x 的解, 其必要充分条件是, 对于从 $p_1 \sim p_r$ 的每个素数 p , 等式 (3.a) 在 $CG(p)$ 中具有 x 的解答。

对于从 $g_1 \sim g_m$ 的基数 g 之一, 等式 (3) 尽快地禁止全等于 $1 \pmod{4}$ 的任意素数 p : 或者 g 相对于 p 的 Legendre 符号等于 -1 ; 或者在 u 为正数, 并且大于 $t-k$ 的条件下, g 相对于 p 的 Legendre 符号等于 $+1$ 。为了全等于 $1 \pmod{4}$ 的素数 p 成为可能, 根据上面定义的两个整数, 对于从 $g_1 \sim g_m$ 的每个基数 g , 必须达到下述两个条件之一。或者 $G=g^2$ 的秩为 $CG(p)$ 中的奇校验秩, 即 $u=0$, 不论 k 为什么值。或者 $G=g^2$ 的秩为 $CG(p)$ 中的偶校验秩, 即 $u > 0$, 并且满足条件 $u+k \leq t$ 。

全等于 $1 \pmod{4}$ 的素数的乘积不能实现所有的 GQ2 技术原理。每个 GQ2 模数必须至少具有两个全等于 $3 \pmod{4}$ 的素数, 从而对于每个基数 g 来说, g 相对于这些素数之一的 Legendre 符号不同于 g 相对于另一素数的 Legendre 符号。当所有素数全等于 $3 \pmod{4}$ 时, 可认为 GQ2 模数是基本模数。当除了全等于 $3 \pmod{4}$ 的至少两个素数之外, 模数包括全等于 $1 \pmod{4}$ 的一个或多个素数时, 可认为模数 GQ2 是复合模数。

GQ2 模数的系统结构

开始, 必须确定将限定模数 n 的全部约束条件: 以二进制位表示

的大小(例如 512 或 1024 位), 以及为 1 的最高有效连续位的数目(至少 1 个, 通常 16 或 32 个二进制位), 素数的数目 f , 必须全等于 $1 \pmod{4}$ 的素数的数目 e (可能为 0); 其它素数, 即 $f-e$ 素数, 中的至少两个, 必须全等于 $3 \pmod{4}$ 。模数 n 将是类似大小的 f 个素数的乘积。当 $e=0$ 时, 得到基本模数 $GQ2$ 。当 $e>0$ 时, 得到复合模数 $GQ2$ 。基本模数是均全等于 $3 \pmod{4}$ 的素数的乘积。于是, 复合模数 $GQ2$ 表示为基本模数 $GQ2$ 乘以一个或多个全等于 $1 \pmod{4}$ 的其它素数的乘积。首先, 产生全等于 $3 \pmod{4}$ 的素数。随后, 如果 $e>0$, 产生全等于 $1 \pmod{4}$ 的素数。

对于 $GQ2$ 模数的结构的效能来说, 在设法查明候选数字是否是素数之前, 选择每个候选数字无疑较好。

用 $g_1, g_2 \dots$ 表示, 通常在第一部分素数: 2, 3, 5, 7... 中查找基数。如果没有相反的指示, m 个基数是 m 个第一部分素数: $g_1=2, g_2=3, g_3=5, g_4=7, \dots$ 。但是, 必须注意下述几点: 如果预先使用了全等于 $5 \pmod{8}$ 的因数, 则必须避开 2; 如果公共密钥 $\langle 3, n \rangle$ 必须被用作 RSA 公共验证密钥, 则必须避开 3。

全等于 $3 \pmod{4}$ 的 $f-e$ 个素数的选择

根据第二因数, 对于每个因数, 程序请求并使用一个基数。对于全等于 $3 \pmod{4}$ 的最后一个因数的选择来说, 程序查明是否存在其它基数, 即 m 是否等于或大于 $f-e$, 并且如果 m 等于或大于 $f-e$, 则请求并考虑从 $g_{f-e} \sim g_m$ 的最后几个基数。为了使全等于 $3 \pmod{4}$ 的素数的选择形式化, 我们引入廓线 (profile)的概念。廓线表征了整数 g 相对于一组大于 g , 并且全等于 $3 \pmod{4}$ 的素数的特征。

-当整数 g 具有和两个素数相同的 Legendre 符号时, 一般认为相对于 g , 这两个素数等效。否则, 相对于 g , 这两个素数互补。

-用 $\text{Profile}_f(g)$ 表示, 整数 g 相对于 f 个素数 $p_1 p_2 \dots p_f$ 的廓线是一个 f 个二进制位的序列, 每个素数一个二进制位。第一位等于 1; 根据相对于 g , 下一因数是和 p_1 等效, 还是和 p_1 互补, 后面的每个二进制位等于 1 或 0。

-当廓线的所有二进制位等于 1 时, 一般认为该廓线平直。这种情况下, g 的所有 Legendre 符号等于+1 或者等于-1。当 g 的廓线不平直时, 在整数模数 n 环中, 不可关于 x 求解等式 (1) 和 (2)。

-根据定义, 相对于全等于 $3 \pmod{4}$ 的单个素数, g 的廓线始终是平真的。这种扩展被用于归纳选择全等于 $3 \pmod{4}$ 的素数的算法。

当两个基数 g_1 和 g_2 的廓线不同时, 这意味着全等于 $3 \pmod{4}$ 的至少三个素数, 两个专用值 Q_1 和 Q_2 导致模数 n 的两种不同分解。当基数是小素数时, 程序确保 $f-e-1$ 个基本素数的 2^{f-e-1} 乘法组合都不相同: 它们取所有可能的数值。廓线概念不扩展到全等于 $1 \pmod{4}$ 的素数。

全等于 $3 \pmod{4}$ 的第一素数 p_1 : 每个候选值必须全等于 $3 \pmod{4}$, 没有其它任何特殊约束条件。

当考虑第一基数 g_1 时, 全等于 $3 \pmod{4}$ 的第二素数 p_2 : 相对于 g_1 , 每个候选值必须和 p_1 互补。

当考虑第二基数 g_2 时, 全等于 $3 \pmod{4}$ 的第二素数 p_3 : 根据相对于两个第一部分素数 p_1 和 p_2 , g_2 的廓线, 产生两种情况。当 $\text{Profile}_2(g_2)$ 平直时, 相对 g_2 , 每个候选值必须和 p_1 互补。否则, 我们得到 $\text{Profile}_2(g_1) = \text{Profile}_2(g_2)$; 则每个候选值必须确保 $\text{Profile}_3(g_1) \neq \text{Profile}_3(g_2)$ 。

当考虑基数 g_i 时, 全等于 $3 \pmod{4}$ 的第 i 个素数 p_{i+1} 的选择: 根据相对于 i 个第一部分素数 $p_1, p_2, \dots, p_i$ 的 g_i 的廓线, 产生两种情况。当 $\text{Profile}_i(g_i)$ 平直时, 相对 g_i , 每个候选值必须和 p_1 互补。否则, 在 $i-1$ 个基数 $g_1, g_2, \dots, g_{i-1}$ 和它们的所有乘法组合 $g_1 \cdot g_2, g_1 \cdot g_2 \cdot \dots \cdot g_{i-1}$, 即总共 $2^{i-1}-1$ 个整数之中, 有且只有一个整数 g 使得 $\text{Profile}_i(g_i) = \text{Profile}_i(g)$; 则每个候选值必须确保 $\text{Profile}_{i+1}(g_i) \neq \text{Profile}_{i+1}(g)$ 。

当考虑基数 g_{f-e-1} , 以及从 $g_{f-e} \sim g_m$ 的其它基数时, 全等于 $3 \pmod{4}$ 的最后一个素数 p_{f-e} : 如上所述考虑归因于基数 g_{f-e-1} 的约束条件。此外, 当 m 等于或大于 $f-e$ 时, 相对于 $f-e$ 个素数, 每个候选值必须提供从 $g_{f-e} \sim g_m$ 的最后几个基数的非平直廓线。相对于 $\text{Profile}_{f-e-1}(g_i)$ 平直的所有

g_i 值, 每个候选值必须和 p_1 互补。

总之, 全等于 $3 \pmod{4}$ 的素数被选为相互的函数。

对于从 $0 \sim f-e-1$ 的 i , 选择全等于 $3 \pmod{4}$ 的第 $i+1$ 个素数, 候选素数 p_{i+1} 必须成功通过下述检查:

√ 如果 $i > m$ 或者如果 $i=0$, 则候选 p_{i+1} 无其它约束条件; 于是接受候选 p_{i+1} 。

√ 如果 $0 < i \leq m$, 则候选 p_{i+1} 必须考虑第 i 个基数 g_i 。相对于从 $p_1 \sim p_i$ 的 i 个第一部分素数, 计算基数 g_i 的廓线 $\text{Profile}_i(g_i)$ 。根据计算结果, 会发生下两种情况中的一种情况, 并且只会发生一种情况:

-如果廓线平直, 则相对于 g_i , 候选 p_{i+1} 必须和 p_1 互补; 否则, 拒绝该候选 p_{i+1} 。

-如果廓线不平直, 在 $i-1$ 个基数 $g_1, g_2, \dots, g_{i-1}$ 和它们的所有乘法组合之中, 有且只有一个我们称为 g 的数字使得 $\text{Profile}_i(g_i) = \text{Profile}_i(g)$; 则候选 p_{i+1} 必须确保 $\text{Profile}_{i+1}(g_i) \neq \text{Profile}_{i+1}(g)$; 否则, 必须拒绝该候选 p_{i+1} 。

√ 如果 $i+1=f-e$, 并且 $i < m$, 即当剩余还未被考虑的从 $g_{f-e} \sim g_m$ 的基数时, 选择全等于 $3 \pmod{4}$ 的最后一个素数, 候选 p_{f-e} 必须把剩余的这些基数考虑进去: 在这些基数中, 选择其廓线 $\text{Profile}_{f-e-1}(g_i)$ 平直的那些数字; 相对于这样选择的每个基数, 候选 p_{f-e} 必须与 p_1 互补; 否则拒绝候选 p_{f-e} 。

由于候选素数已成功通过了适当的测试, 接受该候选素数。

全等于 $1 \pmod{4}$ 的 e 个素数的选择

为了可被接受, 相对于从 $g_1 \sim g_m$ 的每个基数, 全等于 $1 \pmod{4}$ 的每个候选素数 p 必须满足下述条件。

-我们来计算每个基数 g_i 相对于 p 的 Legendre 符号。如果该符号等于 -1 , 则拒绝该候选素数 p , 并转到下一候选素数。如果该符号等于 $+1$, 就继续该候选素数的评估。必须指出的是, 如果整数 2 被用作基数, 则必须除去全等于 $5 \pmod{8}$ 的所有候选素数: 基数 2 和全等于 $5 \pmod{8}$ 的素数不相容。

-计算整数 $s = (p-1+2^t)/2^{t+1}$ ，以便确定密钥 $\langle s, p \rangle$ 。我们把密钥 $\langle s, p \rangle$ 应用于每个公共值 G_i ，以便得到结果 r 。产生两种情况。

-如果 r 等于 g_i 或 $-g_i$ ，则 $u=0$ 。这种情况下，并且也只有在这种情况下， G_i 处于一个环中。可提及的一种普通情况是：如果 p 全等于 $5 \pmod{8}$ ，并且 g_i 相对于 p 的 Legendre 符号等于 $+1$ ，则 G_i 处于环中。可回想起在这种情况下， G_i 不可能等于 4 。

-如果 r 既不等于 g_i ，也不等于 $-g_i$ ，则 $u > 0$ ；必须指出的是密钥 $\langle (p-1)/2^t, p \rangle$ 把各个非二次剩余 y 转换为元素 b ，元素 b 是 1 的第 2^t 次原根。下述算法通过使用两个整数变量：由 r 初始化的 w 和取 $2 \sim 2^{t-2}$ 的值的 jj ，根据 r 和 b ，计算 u 。

对于从 $1 \sim t-2$ 的 i ，重复下述程序：

-计算 $w^2/G_i \pmod{p_i}$ ，随后把结果自乘到 $2^{t-i-1} \pmod{p_i}$ 次幂：我们必定得到 $+1$ 或 -1 。当得到 -1 时，计算 $jj=2^i$ ，则用 $w \cdot b^{jj} \pmod{p_i}$ 替换 w 。当得到 $+1$ 时，不进行任何操作。

在计算结束时，变量 w 的值为 g_i 或 $-g_i$ 。此外，我们知道 $CG(p_i)$ 中， G_i 的秩可被 $2^t/jj$ 除尽，但是不可被 $2^{t+1}/jj$ 除尽，即，通过 $jj=2^{t-u}$ ， jj 确定 u 的值。当 v 大于 jj ，即 $k > t-u$ 时，拒绝该候选素数，并转到另一候选素数。当 v 小于或等于 jj ，即 $k \leq t-u$ 时，继续评估该候选素数。

当已产生 f 个素数时，公共模数 n 是这 f 个素数 $p_1, p_2, \dots, p_f$ 的乘积。无符号的整数 n 可由二进制序列表示；该序列遵守程序开始时，关于二进制位的大小，以及为 1 的连续最高有效位的数目强加的约束条件。素数的选择提供了模数 n 相对于 m 个基数 $g_1, g_2, \dots, g_m$ 中的每个基数的下述性质。此外，在整数模数 n 环中，等式 (1) 和 (2) 不具有 x 的任何解答。其次，在整数模数 n 环中，等式 (3) 具有 x 的解答。

总之，相互独立地选择全等于 $1 \pmod{4}$ 的素数。当全等于 $3 \pmod{4}$ 的因数逐渐考虑基数时，全等于 $1 \pmod{4}$ 的每个素数必须考虑由各个基数限定的所有约束条件。从 $p_{f-e} \sim p_f$ 的每个全等于 $1 \pmod{4}$

的素数，即 p 应分两步成功地通过下述检查。

1) 对于从 $g_1 \sim g_m$ 的 m 个基数中的每个基数，连续执行步骤 (1)。

计算当前基数 g 相对于候选素数 p 的 Legendre 符号。产生并且只产生下述两种情况之一：如果该符号等于 -1，则拒绝候选素数。否则（该符号等于 +1），则在步骤 (1) 之后，转到基数 g 继续该检查。

当对于所有 m 个基数，该候选素数都是可接受的时，则操作转到步骤 (2)。

2) 对于从 $G_1 \sim G_m$ 的 m 个公共值中的每个值，连续执行步骤 (2)。

计算整数 t ，从而 $p-1$ 可被 2^t 除尽，但是不可被 2^{t+1} 除尽，则整数 $s = (p-1+2^t)/2^{t+1}$ ，以便确定密钥 $\langle s, p \rangle$ 。把密钥 $\langle s, p \rangle$ 应用于当前的公共值 $G=g^2$ ，得到结果 r ，即： $r \equiv G^s \pmod{p}$ 。根据该结果，产生并且只产生下述情形之一：

a) 如果 r 等于 g 或 $-g$ ，则 $u=0$ ；在步骤 (2) 转到后面的公共值 G ，继续该候选素数的检查。

b) 否则，取从 $1 \sim t-2$ 的值中的一个值，应用下述算法计算正数 u ，所述算法实现两个变量：取从 $2 \sim 2^{t-2}$ 的值的 jj ，和由 r 初始化的 w ，以及通过把密钥 $\langle (p-1)/2^t, p \rangle$ 应用于 $CG(p)$ 的非二次剩余得到的整数 b 。

对于从 $1 \sim t-2$ 的上标 ii ，重复下述操作：

计算 $w^2/G \pmod{p}$ ，随后把密钥 $\langle 2^{t-ii-1}, p \rangle$ 应用于计算结果，得到 +1 或 -1（否则，证明该候选因数不是素数）。如果得到 -1，则计算 $jj=2^{ii}$ ，随后 $c \equiv b^{jj} \pmod{p}$ ，随后用 $w \cdot c \pmod{p}$ 替换 w ，则转到下一上标 ii 。如果得到 +1，则转到下一上标 ii 。

在算法结束时，依据关系 $jj=2^{t-u}$ 确定变量 jj 中的值；变量 w 的值是 G 的平方根，即 g 或 $-g$ （否则，证明该候选因数不是素数）。产生两种情况：

■ 如果 $t-u < k$ ，则由于出现 G 的支路的长度不够，拒绝候选素数 p 。

■ 如果 $(t-u \geq k)$ ，则在步骤 (2) 之后转到下一公共值 G ，继续

候选素数的评估。

当对于所有 m 个公共值来说，候选素数合格时，把该候选因数看作全等于 $1 \pmod{4}$ 的素数。

相关值的计算

为了获得专用分量，在着手处理通常情况之前，我们首先计算两种最简单，并且最通行情况中，等式 (3.a) 的所有解答。

对于全等于 $3 \pmod{4}$ 的每个素数 p_j 来说，密钥 $\langle (p_j+1)/4, p_j \rangle$ 给出任意二次剩余的平方根。根据这一点，得出计算等式 (3.a) 的解答的方法：

$$s_j \equiv ((p_j+1)/4)^k \pmod{(p_j-1)/2}; \quad \text{则, } Q_{i,j} \equiv G_i^{s_j} \pmod{p_j}$$

或者这种解答的反 $\pmod{p_j}$ 。

$$s_j \equiv (p_j-1)/2 - ((p_j+1)/4)^k \pmod{(p_j-1)/2}; \quad \text{则, } Q_{i,j} \equiv G_i^{s_j} \pmod{p_j}$$

则在 $CG(p_j)$ 中，有且只有 1 的两个平方根：+1 和 -1；于是存在等式 (3.a) 的两个 x 解答：这两个数字 $Q_{i,j}$ 和 $p_j - Q_{i,j}$ 都是相同平方的 $G_i \pmod{p_j}$ 。

对于全等于 $5 \pmod{8}$ 的每个素数 p_j 来说，密钥 $\langle (p_j+1)/4, p_j \rangle$ 给出任意奇校验秩元素的奇校验秩平方根。根据这一点，得出等式 (3.a) 的解答：

$$s_j \equiv ((p_j+3)/8)^k \pmod{(p_j-1)/4}; \quad \text{则, } Q_{i,j} \equiv G_i^{s_j} \pmod{p_j}$$

或者这种解答的反 $\pmod{p_j}$ 。

$$s_j \equiv (p_j-1)/4 - ((p_j+3)/8)^k \pmod{(p_j-1)/4}; \quad \text{则, } Q_{i,j} \equiv G_i^{s_j} \pmod{p_j}$$

则在 $CG(p_j)$ 中，有且只有 1 的 4 个平方根；于是存在等式 (3.a) 的 4 个 x 解答。注意，由于相对于全等于 $5 \pmod{8}$ 的 p ，2 的 Legendre 符号等于 -1，因此 $2^{(p-1)/4} \pmod{p}$ 是 -1 的平方根。如果 $Q_{i,j}$ 是一个解，则 $p_j - Q_{i,j}$ 是另一个解， $Q_{i,j}$ 与 -1 的一个平方根的乘积 $\pmod{p_j}$ 也是一个解。

对于全等于 $2^t+1 \pmod{2^{t+1}}$ 的素数 p_j ，密钥 $\langle (p_j-1+2^t) 2^{t+1}, p_j \rangle$ 给出任意奇校验秩元素的奇校验秩平方根。于是能够计算等式 (3.a) 的解答。

-首先计算整数 $s_j \equiv ((p_j - 1 + 2^t) / 2^{t+1})^k \pmod{(p_j - 1) / 2^t}$, 以确定密钥 $\langle s_j, p_j \rangle$ 。

-当密钥 $\langle (p_j - 1 + 2^t) 2^{t+1}, p_j \rangle$ 把 G_i 转换为 g_i 或 $-g_i$ 时, G_i 的秩为 $CG(p_j)$ 中的奇校验值 ($u=0$)。随后, 密钥 $\langle s_j, p_j \rangle$ 把 G_i 转换为数字 z : 这是等式 (3.a) 的奇校验秩解答。根据 t 和 k 的值, 在一个或多个分支上, 仍然存在 $\min(2^k - 1, 2^t - 1)$ 个其它解答。 z^2 分支携带有另一解答: 即 $p_j - z$ 。当 $t \geq 2$ 时, z^4 分支具有两个其它解答: 它们是 z 与 -1 的两个平方根中的每个平方根, 即 1 的两个第四原根中的每个原根的乘积。现在, 如果 y 是 $CG(p_j)$ 的非二次剩余, 则 $y^{(p_j-1)/4} \pmod{p_j}$ 是 -1 的平方根。一般来说, 对于取从 $1 \sim \min(k, t)$ 中的各个值的 i 来说, z^{2^i} 分支具有 2^{i-1} 个解答: 这些解答是 z 与 1 的 2^{i-1} 个第 2^i 原根中的每个原根的乘积 ($\pmod{p_j}$)。现在如果 y 是 $CG(p_j)$ 中的非二次剩余, 则 $y^{(p_j-1)/2^i}$ 是 1 的第 2^i 次原根, 我们称之为 c 。 1 的第 $2^{i-1} \sim 2^i$ 次原根是 c 的奇校验幂: $c, c^3 \pmod{p_j}, c^5 \pmod{p_j}, \dots, c^{2^i-1} \pmod{p_j}$ 。

-当密钥 $\langle (p_j - 1 + 2^t) 2^{t+1}, p_j \rangle$ 把 G_i 转换为既不是 g_i 也不是 $-g_i$ 的整数 r 时, G_i 的秩为 $CG(p_j)$ 中的偶校验值 ($u > 0$)。随后, 假定 G_i 被恰当地放置在相当长的分支上, 即 $t \geq k + u$, 在 G_i 所处的分支上, 存在 2^k 个解答。为了计算第 2^k 个根, 把上面所述的平方根计算算法重复 k 次就足够了, 以便计算直到解答 z 的连续结果的平方根。当然, 可优化该计算, 以便直接逼近第 2^k 次根, 随后在单个操作中调整第 2^k 次根的近似值, 以获得解答 z 。要获得所有其它解答, 首先要注意的是如果 y 是 $CG(p_j)$ 的非二次剩余, 则 $y^{(p_j-1)/2^k}$ 是 1 的第 2^k 次原根, 我们称之为 d 。 1 的第 2^k 次根是 d 的连续乘幂: $d, d^2 \pmod{p_j}, d^3 \pmod{p_j}, \dots, d^{2^k-1} \pmod{p_j}$, 等于 1 的 $d^{2^k} \pmod{p_j}$ 。 G_i 所处分支上的 2^k 个解答是 z 和这些根中的每个根的乘积 ($\pmod{p_j}$)。

总之, 在已知 k, t 和 u 的情况下, 使用下述程序计算素数 p 和基数 g 的分量:

1) 计算整数: $s \equiv ((p - 1 + 2^t) / 2^{t+1})^k \pmod{(p - 1) / 2^t}$, 确定密钥 $\langle s, p \rangle$ 。

随后,把密钥 $\langle s, p \rangle$ 应用于 G , 得到 $z \equiv G^s \pmod{p}$ 。根据 u 的值, 转到步骤 (2) 或 (3)。

2) 如果 $u=0$, z 是等式 (3.a) 的奇校验解答。在一个或多个分支上, 正好在 $\min(k, t)$ 个其它分支上, 还存在 $\min(2^k-1, 2^t-1)$ 个其它偶校验秩解答。对于从 $1 \sim \min(k, t)$ 的 i 来说, z^{2^i} 分支具有 2^{i-1} 个解答: 这些解答是 z 与 1 的 2^{i-1} 个原根中的每个原根的乘积 $\pmod{p}$ 。等式 (3.a) 的类属解答由 zz 表示。运算转到步骤 (4)。

3) 如果 $u > 0$, 等式 (3.a) 的所有解答都是偶校验解答。这些偶校验解答的数目为 2^k , 并且它们都在 G 所处的分支中; 实际上, $t-u \geq k$ 。为了计算解答, 下述算法实现两个变量: 取从 $2 \sim 2^{t-2}$ 的值的 jj 和由 z 初始化的 w , 以及通过把密钥 $\langle (p-1)/2^t, p \rangle$ 应用于 $CG(p)$ 的非二次剩余, 得到的整数 b 。

下述序列被重复 k 次。

对于从 $1 \sim t-2$ 的上标 ii , 重复下述运算: 计算 $w^2/G \pmod{p}$, 随后把密钥 $\langle 2^{t-ii-1}, p \rangle$ 应用于计算结果, 得到 +1 或 -1 (否则证明 p 不是素数)。如果得到 -1, 则计算 $jj=2^{ii}$, 随后 $c \equiv b^{jj} \pmod{p}$, 随后用 $w \cdot c \pmod{p}$ 替换 w , 则转到下一上标 ii 。如果得到 +1, 则转到下一上标 ii 。

在算法结束时, 变量 w 的值为 za 。 G 所处分支上的 2^k 个解答是 za 和 1 的 2^k 次根中的每个根的乘积 $\pmod{p}$ 。等式 (3.a) 的类属解答由 zz 表示。运算转到步骤 (4)。

4) 在已知 zz 的情况下, 根据其推导出分量值: 当使用等式 $G \cdot Q^v \equiv 1 \pmod{n}$ 时, 该分量值是 $zz \pmod{p}$ 的倒数。当使用等式 $G \equiv Q^v \pmod{n}$ 时, 该分量值是 zz 。

注意: 获得专用分量和专用值的方法有许多种。如果已知一组 f 个分量, 即对于给定基数的 f 个分量, 则使用中国余数方法计算相应的专用值。可看出对于给定的公共值 G 和模数 n , 可能具有几个专用值 Q 。当 n 是全等于 $3 \pmod{4}$ 的两个素数的乘积时, 存在 4 个专用值 Q ; 当 n 是全等于 $3 \pmod{4}$ 的三个素数的乘积时, 存在 8 个专用值

Q; 当 n 是全等于 $3 \pmod{4}$ 的两个素数和全等于 $5 \pmod{8}$ 的一个素数的乘积时, 存在 16 个专用值 Q ; 合理地使用这些多个数值可使得难以通过分析使用 GQ2 的芯片卡的电子消费进行攻击。

从而, 随着 t 的增大, 对于越来越稀少的情况, 程序变得复杂难解。实际上, 素数如下所述被平均分配: $t=1$ 时, 两个中有一个, $t=2$ 时, 四个中有一个, $t=3$ 时, 8 个中有一个, 依次类推。此外, 归因于 m 个基数的约束条件使候选因数逐渐变得不可接受。无论情况是什么样, 复合模数决定性地构成 GQ2 技术的一部分; GQ2 模数的类型决不影响动态证明和数字签名协议。

图 3 图解说明了在具有全等于 $9 \pmod{16}$ 的素数, 即 $t=3$, $u=0$, 以及 $k \geq 3$ 的环中的 $G_i = g_i^2$ 。要注意的是:

$$b \equiv y^{\frac{p-1}{8}} \pmod{p}$$

$$b^8 \equiv 1 \pmod{p}$$

$$b^4 \equiv -1 \pmod{p}$$

图 4 图解说明了在具有全等于 $65 \pmod{128}$ 的素数, 即 $t=6$, $k=4$ 和 $u=2$ 的分支上的 $G_i = g_i^2$ 。

这里是 $k=6$ 的第一组密钥 GQ2, 给出 $v=64$, $m=3$, 给出三个基数: $g_1=3$, $g_2=5$, $g_3=7$, 并且 $f=3$, 即具有三个素数的模数: 两个全等于 $3 \pmod{4}$ 的素数和一个全等于 $5 \pmod{8}$ 的素数。必须注意的是 $g=2$ 和全等于 $5 \pmod{8}$ 的素数不相容。

$$p_1 = 03CD2F4F21E0EAD60266D5CFCEBB6954683493E2E833$$

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

$$p_2 = 0583B097E8D8D777BAB3874F2E76659BB614F985EC1B$$

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

$$p_3 = 0C363CD93D6B3FEC78EE13D7BE9D84354B8FDD6DA1FD$$

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

$$n = p_1 \cdot p_2 \cdot p_3 = FFFF81CEA149DCF2F72EB449C5724742FE2A3630D9$$

$$02CC00EAFEE1B957F3BDC49BE9CBD4D94467B72AF28CFBB26144$$

$$CDF4BBDBA3C97578E29CC9BBEE8FB6DDDD$$

$Q_{1,1}=0279C60D216696CD6F7526E23512DAE090CFF879FDDE$

$Q_{2,1}=7C977FC38F8413A284E9CE4EDEF4AEF35BF7793B89$

$Q_{3,1}=6FB3B9C05A03D7CADA9A3425571EF5ECC54D7A7B6F$

$Q_{1,2}=0388EC6AA1E87613D832E2B80E5AE8C1DF2E74BFF502$

$Q_{2,2}=04792CE70284D16E9A158C688A7B3FEAF9C40056469E$

$Q_{3,2}=FDC4A8E53E185A4BA793E93BEE5C636DA731BDCA4E$

$Q_{1,3}=07BC1AB048A2EAFDAB59BD40CCF2F657AD8A6B573BDE$

$Q_{2,3}=0AE8551E116A3AC089566DFDB3AE003CF174FE4E4877$

$Q_{3,3}=01682D490041913A4EA5B80D16B685E4A6DD88070501$

$Q_1=D7E1CAF28192CED6549FF457708D50A7481572DD5F2C335D8$
 $C69E22521B510B64454FB7A19AEC8D06985558E764C6991B05FC2A$
 $C74D9743435AB4D7CF0FF6557$

$Q_2=CB1ED6B1DD649B89B9638DC33876C98AC7AF689E9D1359E4$
 $DB17563B9B3DC582D5271949F3DBA5A70C108F561A274405A5CB8$
 $82288273ADE67353A5BC316C093$

$Q_3=09AA6F4930E51A70CCDFA77442B10770DD1CD77490E3398A$
 $AD9DC50249C34312915E55917A1ED4D83AA3D607E3EB5C8B197$
 $697238537FE7A0195C5E8373EB74D$

下面是和全等于 $5 \pmod{8}$ 的 p_3 相关的分量的其它可能值。

下面是 $CG(p_3)$ 中, -1 的平方根: $c = 2^{(p_3-1)/4} \pmod{p_3} =$

$0C3000933A854E4CB309213F12CAD59FA7AD775AAC37$

$Q'_{1,3} = c \cdot Q_{1,3} \pmod{p_3} =$

$050616671372B87DEC9AEEAC68A3948E9562F714D76C$

$Q'_{2,3} = c \cdot Q_{2,3} \pmod{p_3} =$

$06F308B529C9CE88D037D01002E7C838439DACC9F8AA$

$Q'_{3,3} = c \cdot Q_{3,3} \pmod{p_3} =$

$015BE9F4B92F1950A69766069F788E45439497463D58$

给出:

$Q'_1 = 676DF1BA369FF306F4A1001602BCE5A008DB82882E87C148D0$

D820A711121961C9376CB45C355945C5F2A9E5AFAAD7861886284A
9B319F9E4665211252D74580

$Q'_2 = \text{CAEC4F41752A228CF9B23B16B3921E47C059B9E0C68634C2C}$
64D6003156F30EF1BC02ADA25581C8FDE76AA14AB5CC60A2DE1C
565560B27E8AA0E6F4BCA7FE966

$Q'_3 = \text{2ACEF5161FE53B68CC7C18B6AFE485815B46599F44C51A6A1}$
A4E858B470E8E5C7D2200EF135239AF0B7230388A6A5BDD8EE15B
0D094FC2BFA890BFDA669D9735

下面是第二组密钥 GQ2, $k=9$, 即 $v=512$, $m=2$, 即两个基数 $g_1=2$
和 $g_2=3$, 并且 $f=3$, 给出具有全等于 $3 \pmod{4}$ 的三个素数的模数。

$p_1 = \text{03852103E40CD4F06FA7BAA9CC8D5BCE96E3984570CB}$
 $(2 \mid p_1) = -1; (3 \mid p_1) = -1$; 并且我们得到: $(6 \mid p_1) = +1$

$p_2 = \text{062AC9EC42AA3E688DC2BC871C8315CB939089B61DD7}$
 $(2 \mid p_2) = +1; (3 \mid p_2) = -1$; 并且我们得到: $(6 \mid p_2) = -1$

$p_3 = \text{0BCADEC219F1DFBB8AB5FE808A0FFCB53458284ED8E3}$
 $(2 \mid p_3) = -1; (3 \mid p_3) = +1$; 并且我们得到: $(6 \mid p_3) = -1$

$n = p_1 \cdot p_2 \cdot p_3 = \text{FFFF5401ECD9E537F167A80C0A9111986F7A8EBA4D}$
6698AD68FF670DE5D9D77DFF00716DC7539F7CBBCF969E73A0C49
761B276A8E6B6977A21D51669D039F1D7

$Q_{1,1} = \text{0260BC7243C22450D566B5C6EF74AA29F2B927AF68E1}$

$Q_{2,1} = \text{0326C12FC7991ECDC9BB8D7C1C4501BE1BAE9485300E}$

$Q_{1,2} = \text{02D0B4CC95A2DD435D0E22BFBB29C59418306F6CD00A}$

$Q_{2,2} = \text{045ECB881387582E7C556887784D2671CA118E22FCF2}$

$Q_{1,3} = \text{B0C2B1F808D24F6376E3A534EB555EF54E6AEF5982}$

$Q_{2,3} = \text{0AB9F81DF462F58A52D937E6D81F48FFA4A87A9935AB}$

$Q_1 = \text{27F7B9FC82C19ACAE47F3FE9560C3536A7E90F8C3C51E13C}$
35F32FD8C6823DF753685DD63555D2146FCDB9B28DA367327DD6
EDDA092D0CF108D0AB708405DA46

$Q_2 = \text{230D0B9595E5AD388F1F447A69918905EBFB05910582E5BA64}$

**9C94B0B2661E49DF3C9B42FEF1F37A7909B1C2DD54113ACF87C6
F11F19874DE7DC5D1DF2A9252D**

本发明已描述了一种多组 GQ2 密钥，即模数 n 和多对公共值和专用值 G 和 Q 的产生方法，其中指数 v 等于 2^k 。如同所描述的那样，所述多组密钥被用于实现用于证明实体的真实性和/或消息的完整性和/或真实性的方法。

在法国电信，TDF 和 Math RiZK 公司在同一天申请的待审批申请（其发明人为 Louis Guillou 和 Jean-Jacques Quisquater）中，要求保护证明实体的真实性和/或消息的完整性和/或真实性的方法，系统和设备的特征。这两个申请作为参考包含于此。

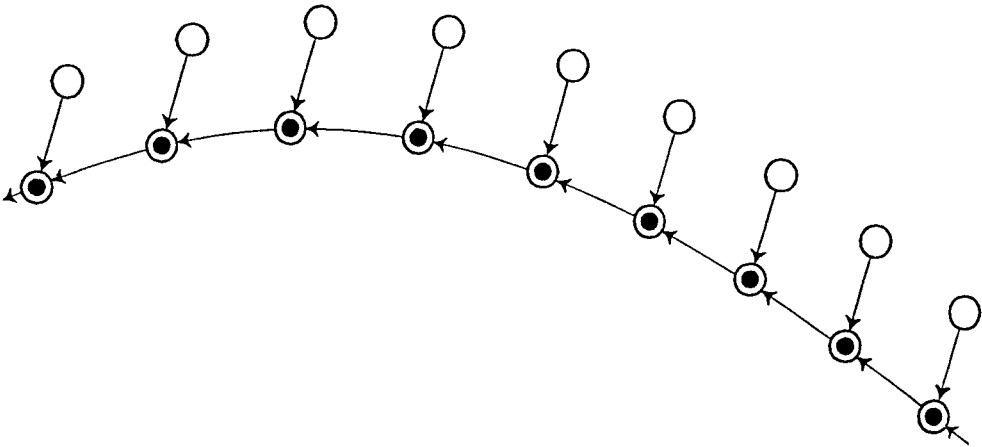


图1A

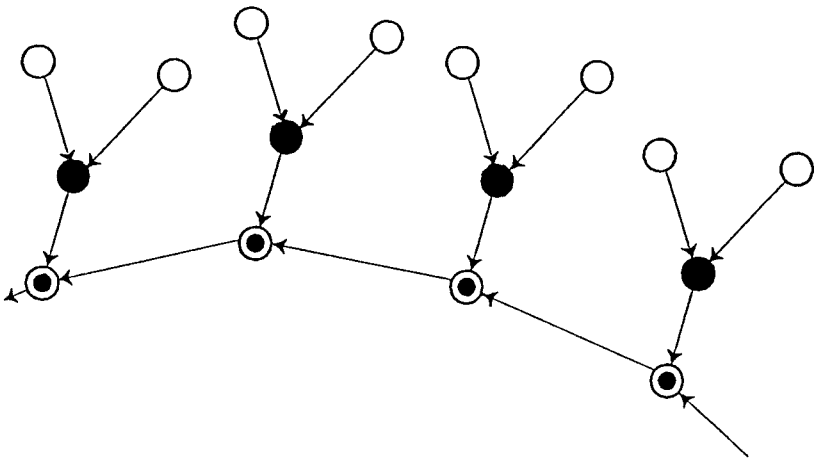


图1B

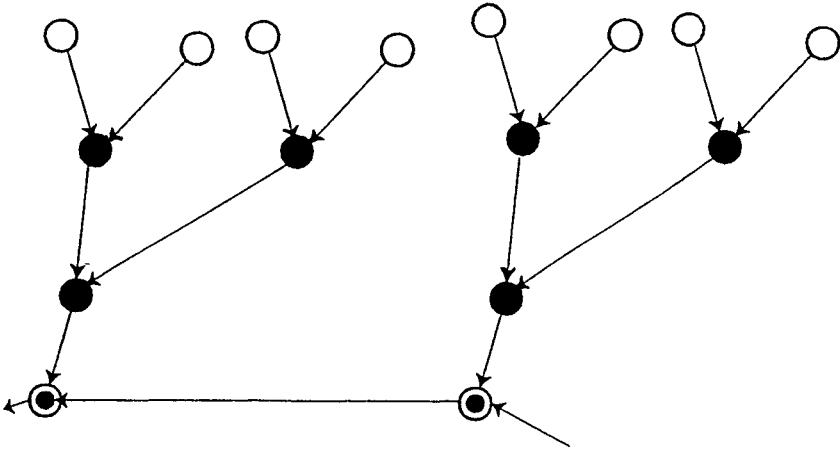


图1C

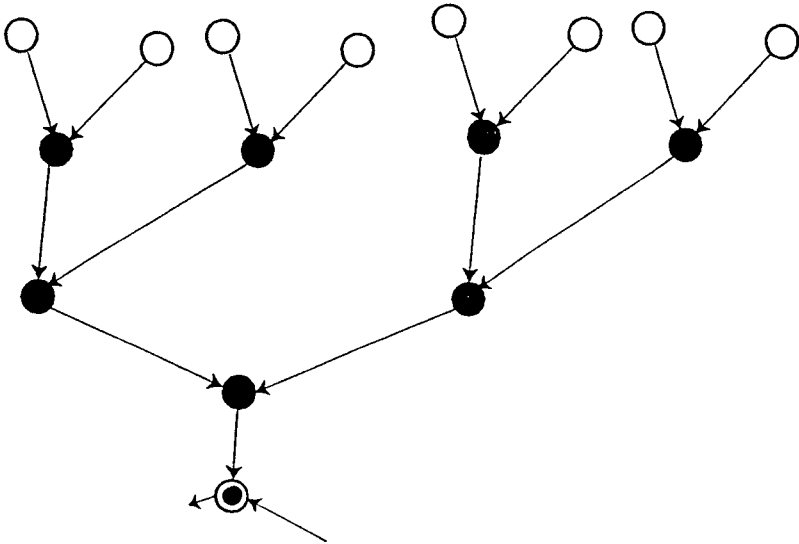


图1D

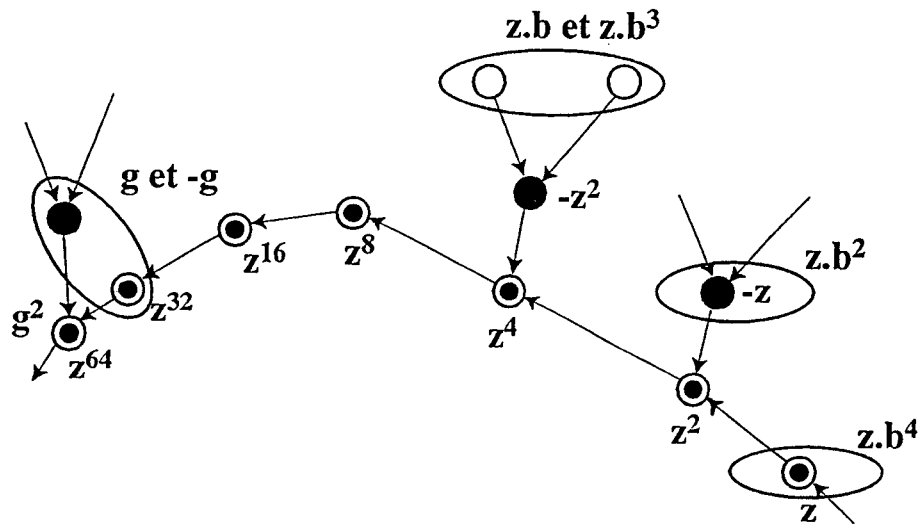


图2

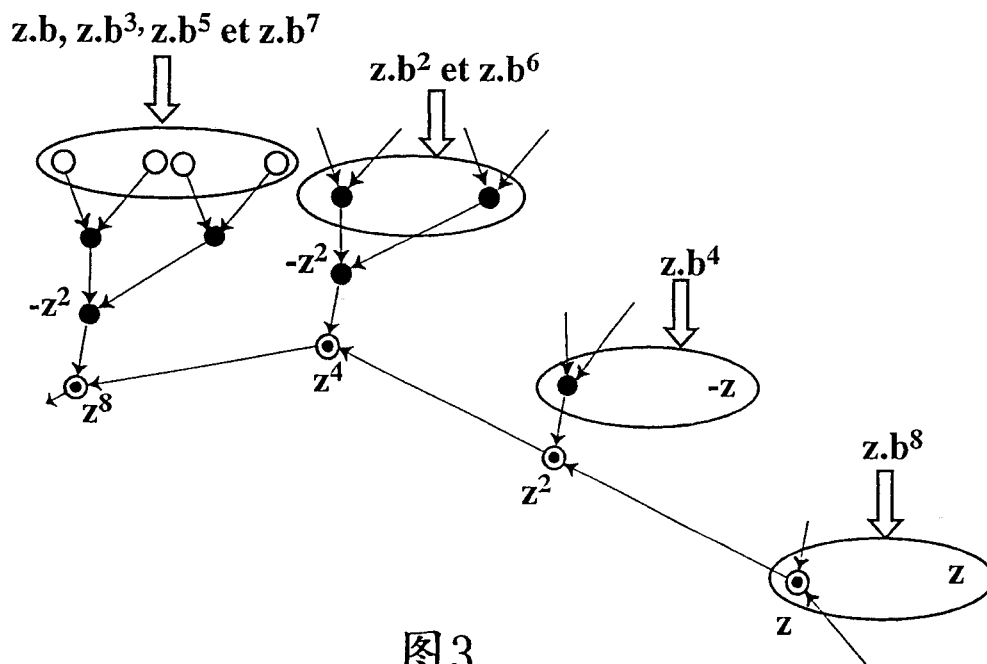


图3

