



(12) 发明专利

(10) 授权公告号 CN 101133593 B

(45) 授权公告日 2012. 03. 21

(21) 申请号 200480022177. 6

(22) 申请日 2004. 07. 08

(30) 优先权数据

03/09457 2003. 07. 31 FR

(85) PCT申请进入国家阶段日

2006. 01. 28

(86) PCT申请的申请数据

PCT/EP2004/051411 2004. 07. 08

(87) PCT申请的公布数据

W02005/022820 FR 2005. 03. 10

(73) 专利权人 格马尔托股份有限公司

地址 法国默东

(72) 发明人 K·维莱加斯 M·诺耶

B·舍瓦利耶-马梅斯

(74) 专利代理机构 中国专利代理(香港)有限公

司 72001

代理人 刘红 张志醒

(51) Int. Cl.

H04L 9/30(2006. 01)

(56) 对比文件

US 5991415 A, 1999. 11. 23, 全文.

W0 03/028286 A1, 2003. 04. 03, 全文.

审查员 高霞

权利要求书 3 页 说明书 10 页

(54) 发明名称

安全地执行 RSA 型密码术算法的方法及相应部件

(57) 摘要

本发明涉及一种在电子部件中的 RSA 型密码术算法的安全应用的方法。所述方法允许在不需要所述值的先验知识的情况下,从可能值的给定集合中得到公开指数 e 的值,在已经确定了公开指数 e 的所述值后,允许应用使用 e 值的对策以阻挡错误攻击或者侧信道攻击,尤其是可以在密码术算法的私有操作应用上执行的 DPA 型和 SPA 型的侧信道攻击。

1. 一种安全地执行公开密钥密码术算法的方法,所述公开密钥由整数 n 和公开指数 e 构成,所述整数 n 是两个大素数 p 和 q 的乘积,所述算法还包括私有密钥,所述方法包括确定包含预定数量的素数 e_i 的集合 E ,所述素数 e_i 能够对应于公开指数 e 的值,所述方法其特征在于,包括以下步骤:

$$a) \text{ 计算值 } \mathbf{e} = \prod_{e_i \in E} e_i$$

以使对于任意属于 E 的 e_i , $\mathbf{e}/e_i$ 小于 $\Phi(n)$, 此处 Φ 是欧拉 Φ 函数;

b) 将 $\mathbf{e}$ 值应用于预定的计算,所述计算仅仅包含 $\mathbf{e}$ 与所述算法的私有密钥相乘的模数积;

c) 对于每个 e_i , 检验所述预定计算的结果是否等于值 $\mathbf{e}/e_i$;

如果相等,那么将值 e_i 赋给 e , 考虑到在所述密码术算法的计算中使用 e , 因而存储 e ; 否则, 观察到不能执行使用值 e 的密码术算法的计算。

2. 根据权利要求 1 所述的方法, 其特征在于, 所述密码术算法基于标准模式 RSA 型算法。

3. 根据权利要求 2 所述的方法, 其特征在于, 所述步骤 b) 的预定计算包含计算值 C :

$C = \mathbf{e} \cdot d$ 对 $\Phi(n)$ 取模, 此处 d 为使得 $e \cdot d$ 对 $\Phi(n)$ 取模 = 1 的 RSA 算法的相应私有密钥, Φ 为欧拉 Φ 函数。

4. 根据权利要求 2 所述的方法, 其特征在于, 所述步骤 b) 的预定计算包含计算值 C :

$C = \mathbf{e} \cdot d$ 对 $\lambda(n)$ 取模, 此处 d 为使得 $e \cdot d$ 对 $\lambda(n)$ 取模 = 1 的 RSA 算法的相应私有密钥, λ 为卡麦克函数。

5. 根据权利要求 1 所述的方法, 其特征在于, 所述密码术算法基于中国余数定理模式 RSA 型算法。

6. 根据权利要求 5 所述的方法, 其特征在于, 所述步骤 b) 的预定计算包含计算值 C :

$C = \mathbf{e} \cdot d_p$ 对 $(p-1)$ 取模, 此处 d_p 为使得 $e \cdot d_p$ 对 $(p-1)$ 取模 = 1 的 RSA 算法的相应私有密钥。

7. 根据权利要求 5 所述的方法, 其特征在于, 步骤 b) 的预定计算包含值 C 的计算:

$C = \mathbf{e} \cdot d_q$ 对 $(q-1)$ 取模, 此处 d_q 为使得 $e \cdot d_q$ 对 $(q-1)$ 取模 = 1 的 RSA 算法的相应私有密钥。

8. 根据权利要求 5 所述的方法, 其特征在于, 所述步骤 b) 的预定计算包含计算两个值 C_1 和 C_2 使得:

$C_1 = \mathbf{e} \cdot d_p$ 对 $(p-1)$ 取模, 此处 d_p 为使得 $e \cdot d_p$ 对 $(p-1)$ 取模 = 1 的 RSA 算法的相应私有密钥;

$C_2 = \mathbf{e} \cdot d_q$ 对 $(q-1)$ 取模, 此处 d_q 为使得 $e \cdot d_q$ 对 $(q-1)$ 取模 = 1 的 RSA 算法的相应私有密钥;

并且其特征还在于, 所述检验步骤 c) 中包含, 对于每个 e_i 检验 C_1 和 / 或 C_2 是否等于值 $\mathbf{e}/e_i$:

如果相等, 那么将 e_i 的值赋给 e , 考虑到在所述密码术算法计算中使用 e , 因而存储 e ; 否则, 观察到使用值 e 的所述密码术算法的计算不能执行。

9. 根据权利要求 3 或 4 所述的方法, 其中值 e_i 已经赋给 e , 所述方法其特征在于, 使用值 e 的计算包含:

选择随机整数 r ;

计算值 d^* 使得 $d^* = d + r \cdot (e \cdot d - 1)$, 和

执行算法的私有操作, 其中通过应用关系 $x = y^{d^*}$ 对 n 取模从值 y 得到值 x 。

10. 根据权利要求 2 至 4 任一项所述的方法, 其中值 e_i 已经赋给 e , 所述方法的特征在于, 使用值 e 的计算包含检查是否 $x^e = y$ 对 n 取模。

11. 根据权利要求 5 至 8 任一项所述的方法, 其中值 e_i 已经赋给 e , 所述方法的特征在于, 使用值 e 的计算包含首先检查是否 $x^e = y$ 对 p 取模, 其次检查是否 $x^e = y$ 对 q 取模。

12. 根据权利要求 1 至 8 任一项所述的方法, 其特征在于, 所述集合 E 包括至少下列 e_i 值: $3, 17, 2^{16} + 1$ 。

13. 一种安全地执行公开密钥密码术算法的方法, 所述公开密钥由整数 n 和公开指数 e 构成, 所述整数 n 是两个大素数 p 和 q 的乘积, 所述方法包括确定包含预定数量素数 e_i 的集合 E , 所述素数 e_i 能够对应于公开指数 e 的值, 所述方法其特征在于, 包括以下步骤:

a) 从集合 E 的值中选择值 e_i ;

b) 如果 $\delta(p) = \delta(q)$, 检验所选择的 e_i 值是否满足关系:

$$(1 - e_i \cdot d) \text{ 对 } n \text{ 取模} < e_i \cdot 2^{(\delta(n)/2)+1}$$

或者所述关系被简化为

$$(-e_i \cdot d) \text{ 对 } n \text{ 取模} < e_i \cdot 2^{(\delta(n)/2)+1}$$

此处 $\delta(p)$, $\delta(q)$ 和 $\delta(n)$ 为分别给出对数字 p 、数字 q 和数字 n 进行编码的位数的函数;

c) 如果满足在前述步骤中应用的检验关系, 因此 $e = e_i$, 考虑到在所述密码术算法的计算中使用 e , 因而存储 e ;

否则, 重复前面步骤同时从集合 E 中为 e_i 选择另一值, 直到 e_i 值能够赋给 e , 如果没有 e_i 值可以赋给 e , 那么观察到不能执行使用值 e 的所述密码术算法的计算。

14. 根据权利要求 13 所述的安全地执行公开密钥密码术算法的方法, 其特征在于, 该方法包括当 $\delta(p) \neq \delta(q)$ 时, 即当 p 和 q 不平衡时, 以下面的方式执行步骤 b, 检验所选择的 e_i 值是否满足下面关系:

$$(1 - e_i \cdot d) \text{ 对 } n \text{ 取模} < e_i \cdot 2^{g+1}$$

或者所述关系被简化为:

$$(-e_i \cdot d) \text{ 对 } n \text{ 取模} < e_i \cdot 2^{g+1}$$

如果 $\delta(p)$ 和 $\delta(q)$ 已知, 那么 $g = \max(\delta(p), \delta(q))$, 否则 $g = \delta(n)/2 + t$, 此处 t 代表不平衡因子或者对该因子的一个限制。

15. 根据权利要求 13 或 14 所述的方法, 其特征在于, 对于所有 i 值, $e_i \leq 2^{16} + 1$, 并且其特征还在于所述步骤 b) 由另一检验步骤替代, 包含:

b) 如果 $\delta(p) = \delta(q)$, 检验所选择的 e_i 值是否满足关系:

$$(1 - e_i \cdot d) \text{ 对 } n \text{ 取模} < e_i \cdot 2^{(\delta(n)/2)+17}$$

或者所述关系被简化为:

$$(-e_i \cdot d) \text{ 对 } n \text{ 取模} < e_i \cdot 2^{(\delta(n)/2)+17}$$

此处 $\delta(p)$, $\delta(q)$ 和 $\delta(n)$ 为分别给出对数字 p 、数字 q 和数字 n 进行编码的位数的函数；

否则,当 p 和 q 不平衡时,检验所选择的 e_i 值是否满足下面的关系：

$$(1-e_i, d) \text{ 对 } n \text{ 取模} < e_i \cdot 2^{g+17}$$

或者所述关系被简化为：

$$(-e_i, d) \text{ 对 } n \text{ 取模} < e_i \cdot 2^{g+17}$$

如果 $\delta(p)$ 和 $\delta(q)$ 已知,那么 $g = \max(\delta(p), \delta(q))$, 否则 $g = \delta(n)/2+t$, 此处 t 代表不平衡因子或者对该因子的一个限制。

16. 根据权利要求 13 或 14 所述的方法,其特征在于,所述步骤 b) 由另一检验步骤替代,包含：

检验所选择的 e_i 值是否满足关系,由此：

$$(1-e_i, d) \text{ 的对 } n \text{ 取模的第一最高有效位为 } 0；$$

或者简化所述关系,由此：

$$(-e_i, d) \text{ 的对 } n \text{ 取模的第一最高有效位为 } 0。$$

17. 根据权利要求 16 所述的方法,其特征在于,对第一 128 个最高有效位执行检验。

18. 根据权利要求 13 或 14 所述的方法,其特征在于,密码术算法基于标准模式 RSA 型算法。

19. 根据权利要求 13 或 14 所述的方法,其中 e_i 值已经赋给 e , 所述方法其特征在于,使用值 e 的计算包含：

选择随机整数 r 。

$$\text{计算值 } d^* \text{ 使得 } d^* = d + r \cdot (e \cdot d - 1),$$

执行算法的私有操作,其中通过应用关系 $x = y^{d^*}$ 对 n 取模从值 y 得到值 x 。

20. 根据权利要求 13 或 14 所述的方法,其中 e_i 值已经赋给 e , 所述方法其特征在于,使用值 e 的计算包含检查是否 $x_e = y$ 对 n 取模。

21. 根据权利要求 13 或 14 所述的方法,其特征在于,所述集合 E 包括至少下列 e_i 值： $3, 17, 2^{16}+1$ 。

22. 根据权利要求 21 所述的方法,其特征在于以下列顺序从所述集合 E 的值中优先选择值 e_i ： $2^{16}+1, 3, 17$ 。

安全地执行 RSA 型密码术算法的方法及相应部件

[0001] 本发明涉及在电子部件中安全地执行密码术算法的方法,尤其涉及安全地执行 Rivest-Shamir-Adleman (RSA) 型密码术算法的方法。

[0002] 本发明还涉及相应的电子部件。

[0003] 这种部件特别使用在对服务或者数据的存取被严格控制的应用中。

[0004] 这种部件具有“软件”体系结构,即可编程体系结构,所述“软件”体系结构围绕微处理器和围绕存储器形成,所述存储器包括包含一个或多个密码的电子可擦除可编程只读存储器的非易失性存储器 (EEPROM)。该体系结构是适合于执行任意算法的非专用体系结构。

[0005] 这种部件使用在计算机系统、运载工具 (onboard) 或者其它应用中。它们特别使用在用于某种应用的智能卡中。例如,这种使用是用于访问某一数据库的应用、银行应用、远程支付应用,例如电视购物、汽油购买,或者用于高速公路通行费支付。

[0006] 因此这种部件或卡执行用于对所传输的数据进行加密和 / 或对所接收到的数据进行解密的密码术算法,或者用于验证或者数字地签名消息的密码术算法。

[0007] 根据在这种被主机系统 (服务器、自动出纳机等) 使用作为输入至卡中的消息,并根据包含在卡内的密码 (secret number), 该卡向主机系统返回加密、验证或者签名消息,从而使得主机系统对该部件或者卡进行验证,并交换数据等。

[0008] 密码术算法的特性已经公知: 所执行的计算; 所使用的参数。唯一未知的量是密码。这种密码术算法的整体安全依赖于卡中包含的不为卡外世界所知的那些密码。仅仅通过知道使用作为输入的消息和返回中发送的加密消息不能推导出密码。

[0009] 遗憾的是, 已经出现了基于来自部件外部的可测量的物理幅值的外部攻击, 当所述部件运行密码术算法时, 这种攻击使得不良企图者可能找到包含在卡中的密码。这种攻击被称为侧信道攻击 (sidechannel attack)。这些侧信道攻击中, 存在基于一种度量或者几种度量的简单电源分析 (single Power Analysis SPA) 攻击, 和基于由许多度量产生的统计分析的差分电源分析 (Differential PowerAnalysis) 攻击。这种侧信道攻击的原理是基于, 例如这样的事实: 当指令或者数据功能被处理时, 微处理器执行指令的电流消耗发生变化。

[0010] 还存在一种被称之为“故障攻击”类型的攻击。在这种攻击类型中, 当密码术算法正被计算时, 攻击者注入任意故障, 目标是使用故障的出现来提取保密信息。

[0011] 故障还可能来自由于硬件执行密码术算法产生的计算错误。然而, 在这两种情况中, 都认为出现了故障攻击。

[0012] 特别是使用公开密钥的密码术算法可能出现各种类型的攻击, 诸如象是在该应用领域使用最为广泛并且本发明尤其适用的 RSA 算法 (以它的创始人 Rivest、Shamir 和 Adleman 命名)。

[0013] 下面将简要回想一下 RSA 公开密钥加密系统的主要特性。

[0014] 第一公开密钥加密和签名方案是在 1977 年由发明了 RSA 加密系统的 Rivest、shamir 和 Adleman 开发出来的。RSA 的安全是基于对一个大数 (为两个素数的乘积) 进行

因子分解的难度。该系统在公开密钥加密系统使用最为广泛。该系统可以用作加密方法或者用作签名方法。

[0015] RSA 加密系统的原理如下。它首先包含产生 RSA 密钥对。

[0016] 因此,使用下述 5 个步骤,每个用户生成 RSA 公开密钥以及相应的私有密钥:

[0017] 1) 生成两个不同的素数 p 和 q ;

[0018] 2) 计算 $n = pq$ 以及 $\Phi(n) = (p-1)(q-1)$, 此处 Φ 被称为欧拉 Φ 函数 (Eulertotient function 或者 Euler Phifunction);

[0019] 3) 随机地选择一个整数 $e, 1 < e < \Phi(n)$, 使 $\text{pgcd}(e, \Phi(n)) = 1$, 或者根据能够选择 e 为小的用户选择使得 $e = 2^{16}+1$ 或者 $e = 3$ 或者 $e = 17$;

[0020] 4) 计算唯一整数 $d, 1 < d < \Phi(n)$, 以使:

[0021] $e \cdot d$ 对 $\Phi(n)$ 取模 $= 1$; (1)

[0022] 5) 公开密钥为 (n, e) ; 私有密钥为 d 或者 (d, p, q) 。

[0023] 整数 e 和 d 分别称作“公开指数”和“私有指数”。整数 n 被称为“RSA 模数”。

[0024] 一旦定义了公开和私有参数,给定了 $x, 0 < x < n$, 对 x 的公开操作 (可以是例如对消息 x 加密) 包含在计算中:

[0025] $y = x^e$ 对 n 取模 (2)

[0026] 在这种情况下,相应的私有操作是对加密消息 y 进行解密操作,所述私有操作包含在计算中:

[0027] Y^d 对 n 取模 (3)

[0028] 对 x 的公开操作还可以是签名 x 的验证,然后所述公开操作包含在计算中:

[0029] $y = x^e$ 对 n 取模 (2)

[0030] 然后相应的私有操作是根据前面的编码消息 y 通过应用 hash 函数或者“padding”函数 μ 产生签名 x , 所述私有操作包含在计算中:

[0031] Y^d 对 n 取模 (3)

[0032] 此处,由于 $e \cdot d$ 对 $\Phi(n)$ 取模 $= 1$, $x = y^d$ 对 n 取模。

[0033] 下面将介绍另一种被称之为中国余数定理 (chinese RemainderTheorem, CRT) 模式的操作模式。该理论比标准 RSA 算法操作模式快 4 倍。在 CRT 模式中,对 n 取模的计算并非直接执行的,而是首先执行对 p 取模和对 q 取模计算。

[0034] 公开参数为 (n, e) , 但是在 CRT 模式中。私有参数为 (p, q, d) 或者 (p, q, d_p, d_q, i_q) , 此处

[0035] $d_p = d$ 对 $(p-1)$ 取模, $d_q = d$ 对 $(q-1)$ 取模, $i_q = q^{-1}$ 对 p 取模。

[0036] 通过关系 (1), 可以得到以下关系:

[0037] ed_p 对 $(p-1)$ 取模 $= 1$, ed_q 对 $(q-1)$ 取模 $= 1$ (4)

[0038] 对于标准操作模式,以相同的方式执行公开操作。相反,对于私有操作,首先进行下面的计算:

[0039] $x_p = y^{d_p}$ 对 p 取模和 $x_q = y^{d_q}$ 对 q 取模

[0040] 然后,通过应用中国余数定理,通过下式得到 $x = y^d$ 对 n 取模:

[0041] $x = \text{CRT}(x_p, x_q) = x_q + q[i_q(x_p - x_q) \text{ 对 } p \text{ 取模}]$ (5)

[0042] 因此使用 RSA 加密方案的公开密钥密码术的领域的一个重要方面包含执行 RSA 算

法以安全地抵御上述各种可能攻击类型,特别是侧信道攻击,诸如 DPA 和 SPA 攻击,以及“故障”攻击,其中攻击者通过使用任意方法,在 RSA 算法的私有操作计算期间注入故障,其目的是得到被破坏的值,在特定情况下可能从所述被破坏的值推导出保密数据的特定项。

[0043] 本技术领域的情况是已经设计出特定对策方法以避免各种类型的攻击。

[0044] 特别地,一种用于避开 DPA (和 SPA) 类型对标准模式 RSA 攻击的可能对策包含通过在计算中插入一个随机值随机执行 RSA 的私有操作 (签名或者解密)。

[0045] 因此,所述类型的一个对策方法包含在标准模式 (3) $x = y^d$ 对 n 取模以如下方式计算私有操作:

[0046] $x = y^{d+r} \cdot y^r$ 对 n 取模,此处 r 为随机整数。然而,这种对策方法的缺陷在于使计算时间加倍。

[0047] 另一种用于避开 DPA (和 SPA) 类型对标准模式 RSA 攻击的对策方法包含以如下方式计算私有操作 (3) $x = y^d$ 对 n 取模:

[0048] $x = y^{(d+r \cdot \Phi(n))}$ 对 n 取模,此处 r 为随机整数。然而,这种对策方法的缺陷在于它需要知道 $\Phi(n)$ 的值,而对于执行私有操作 (签名或者解密) 的密码术算法来讲, $\Phi(n)$ 的值通常是未知的。

[0049] 因此该方法的变型已经提出,不但基于要知道 $\Phi(n)$ 的值,而且要知道公开指数 e 。(1) 我们假定: $e \cdot d$ 对 $\Phi(n)$ 取模 $= 1$,因此存在一个整数 k 使得 $e \cdot d - 1 = k \cdot \Phi(n)$ 。

[0050] 因此,表达式 $x = y^{(d+r \cdot \Phi(n))}$ 对 n 取模可以如下形式计算:

[0051] $x = y^{(d+r \cdot (ed-1))}$ 对 n 取模,此处 r 为随机整数。

[0052] 因此这种对策方法与仿效的方法在计算上等效,但是它提供了有利之处在于不需要知道 $\Phi(n)$ 的值。由于不需要保持 $\Phi(n)$,因此该对策方法所需要的存储器也较少。

[0053] 然而,为执行该变型的对策,需要知道公开指数 e 的值。遗憾的是,在许多密码术应用中,这种执行 RSA 算法的私有操作的装置或者部件并不总是具有公开指数 e ,特别是当仅仅执行私有操作时。因此在这种环境中,公开指数 e 通常是未知的或者不可用的。

[0054] 上述对策主要目的是避开 DPA 类型的攻击。然而,由于算法的执行是非确定的,因此上述对策还使得 SPA 类型攻击更加困难。

[0055] 关于其它上述类型的攻击,即“故障”攻击,用于在标准模式下避开它的最可能的保护包含检验通过应用私有操作得到的值 x 是否确实满足公开操作的 $x^e = y$ 对 n 取模的关系。如果不满足,则不返回值 y ,以防止该值用于密码分析目的。

[0056] 在 CRT 模式中,保护包含首先检查是否确实满足关系 $x^e = y$ 对 p 取模和 $x^e = y$ 对 q 取模。

[0057] 当这些条件都满足时,就可能确定在 RSA 算法的私有操作运行期间没有出现错误。

[0058] 然而,防止这种检查的执行受到标准模式或者 CRT 模式中故障攻击的缺陷在于,这些检查操作还需要先前知道的公开指数 e 。遗憾的是,正如上面所说明的,执行标准模式或 CRT 模式中 RSA 算法的私有操作的装置或者部件并不总是具有公开指数 e ,特别是当仅仅执行私有操作时。因此在这种环境中,公开指数 e 通常是未知的或者不可用的。

[0059] 为此,专利文件 FR 2 830 146 (D1) 提出了一种方法,使得可能使用不是先前已知的公开指数 e 执行密码术算法的特定步骤,尤其是标准模式或者 CRT 模式的 RSA 类型密码

术算法的特定步骤。

[0060] 在 D1 中公开的方法尤其可能提供一种特别抵御故障攻击的对策,如上所述,该方法甚至当公开指数 e 未知时也提供了可能达到的最好的保护。

[0061] 为了此目的,假设 (e, d) 为相应的分别代表公开指数和私有指数的 RSA 指数对,假设 n 为 RSA 模数。D1 源于下面观察:在 95% 的情况下,公开指数 e 的值是在值 $2^{16}+1, 3, 17$ 中选择的。D1 的方法(此处参考标准模式简要说明,但是 D1 的方法同样可应用于 CRT 模式)包含通过连续地检验是否 e_i, d 对 $\Phi(n)$ 取模 $= 1$ 来检查 e 实际上等于所述值中的一个,直到满足该关系,此处 $e_i \Phi E = \{2^{16}+1, 3, 17\}$ 。

[0062] 当对于一个 e_i 满足关系时,那么就知 $e = e_i$ 。一旦以这种方式确定了公开指数 e 的值,考虑到在 RSA 算法的计算中(目的是检查在 RSA 算法的相应私有操作运行期间没有由于故障攻击产生的错误出现)要使用值 e ,因而存储 e 。因此,知道 e ,仅仅通过检查所得到的值 s 满足相应公开操作的关系 $s^e = \mu(m)$ 对 n 取模,就可能以概率为 1 的方式断定:在没有错误的情况下已经执行了涉及例如生成签名 s 的私有操作,此处 $s = \mu(m)^d$ 对 n 取模, $\mu(m)$ 为对要被签字的消息 m 应用了 Padding 函数 μ 所得到的值。

[0063] 如果没有可能将任何 e_i 的值赋给 e ,那么在 D1 中,需要注意的是,就不能执行用于抵御故障攻击的使用值 e 的 RSA 算法的计算。

[0064] 然而, D1 中所提出的方法的缺陷在于,当对于来自设想值 e_i 的一个值 e_i 进行连续检验,以确定是否满足关系 e_i, d 对 $\Phi(n)$ 取模 $= 1$ 时, D1 的方法需要执行多个模数计算。因此该方法抑制了计算时间上和计算资源。

[0065] 因此,产生的问题是要降低上述缺陷。

[0066] 特别地,本发明的一个目标包含,当 e 的所述值为先前已知时,以一种并不抑制计算速度和复杂度的方式,从预定的可能值的集合中确定公开指数 e 的值,所述指数 e 是在标准模式或者 CRT 模式的 RSA 型密码术算法的特定步骤中被执行的。

[0067] 本发明的另一目标包含,当公开指数 e 的值被确定时,使得能够使用公开指数 e 的值执行对策操作,目的在于首先避开“故障攻击”,其次避开“侧信道攻击”,尤其是在密码术算法(尤其是 RSA 型算法)的私有操作执行期间可能进行的 DPA 和 SPA 类型的攻击。

[0068] 为了实现这些目标,本发明提供了一种安全地执行公开密钥密码术算法的方法,公开密钥由整数 n 和公开指数 e 构成,所述整数 n 是两个大素数 p 和 q 的乘积,所述方法包括确定包含预定数量的值 e_i (能够对应于公开指数 e 的值)的集合 E ,所述 e_i 值为素数,所述方法其特征在于包括以下步骤:

[0069] a) 计算值 $\Phi = \prod_{e_i \in E} e_i$

[0070] 以使对于任意属于 E 的 e_i , Φ/e_i 小于 $\Phi(n)$, 此处 Φ 为欧拉 Φ 函数;

[0071] b) 将 Φ 值应用于预定的计算;

[0072] c) 对于每个 e_i , 检验所述预定计算的结果是否与值 Φ/e_i 相等;

[0073] - 如果相等,那么将值 e_i 赋给 e , 考虑到在所述密码术算法计

[0074] 算中要使用 e , 因而存储 e ;

[0075] - 否则,观察到不能执行使用值 e 的密码术算法的计算。

[0076] 因此,优势很清楚,仅仅存在一个取模乘方(modular multiplication)。

- [0077] 在第一变型中,密码术算法基于标准模式 RSA 型算法。
- [0078] 参考所述第一变型,步骤 b) 的预定计算包含计算值 C:
- [0079] $C = \Phi \cdot d$ 对 $\Phi(n)$ 取模,此处 d 为使得 e. d 对 $\Phi(n)$ 取模 = 1 的 RSA 算法的相应私有密钥, Φ 为欧拉 Φ 函数。
- [0080] 在一个替代方法中,步骤 b) 的预定计算包含计算值 C:
- [0081] $C = \Phi \cdot d$ 对 $\Phi(n)$ 取模,此处 d 为使得 e. d 对 $\Phi(n)$ 取模 = 1 的 RSA 算法的相应私有密钥, Φ 为卡麦克 (Carmichael) 函数。
- [0082] 在第二变型中,加密算法基于 CRT 模式中的 RSA 型算法。
- [0083] 参考所述第二变型,步骤 b) 的预定计算包含值 C 的计算:
- [0084] $C = \Phi \cdot d_p$ 对 $(p-1)$ 取模,此处 d_p 为使得 e. d_p 对 $(p-1)$ 取模 = 1 的 RSA 算法的相应私有密钥。
- [0085] 在一个替代方法中,步骤 b) 的预定计算包含计算值 C:
- [0086] $C = \Phi \cdot d_q$ 对 $(q-1)$ 取模,此处 d_q 为使得 e. d_q 对 $(q-1)$ 取模 = 1 的 RSA 算法的相应私有密钥。
- [0087] 在另一替代方法中,步骤 b) 的预定计算包含计算两个值 C_1 和 C_2 使得:
- [0088] $C_1 = \Phi \cdot d_p$ 对 $(p-1)$ 取模,此处 d_p 为使得 e. d_p 对 $(p-1)$ 取模 = 1 的 RSA 算法的相应私有密钥;
- [0089] $C_2 = \Phi \cdot d_q$ 对 $(q-1)$ 取模,此处 d_q 为使得 e. d_q 对 $(q-1)$ 取模 = 1 的 RSA 算法的相应私有密钥;
- [0090] 并且其中在所述检验步骤 c) 中包含,对于每个 e_i ,检验 C_1 和 / 或 C_2 是否和值 Φ / e_i 相等:
- [0091] - 如果相等,那么将值 e_i 赋给 e,考虑到在所述密码术算法计算中要使用 e 值,因而存储 e;
- [0092] - 否则,观察到不能执行使用值 e 的所述密码术算法的计算。
- [0093] 在第一变型中,当将值 e_i 赋给 e 时,使用值 e 的计算包含:
- [0094] 选择随机整数 r:
- [0095] 计算值 d^* 使得 $d^* = d + r \cdot (e \cdot d - 1)$; 和
- [0096] 执行算法的私有操作,其中通过使用关系 $x = y^{d^*}$ 对 n 取模,从值 y 得到值 x。
- [0097] 在第一变型中,当将值 e_i 赋给 e 时,在算法的私有操作之后,使用值 e 的计算包含: 从值 y 得到值 x,并检查是否 $x^e = y$ 对 n 取模。
- [0098] 在第二变型中,当将值 e_i 赋给 e 时,在算法的私有操作之后,使用值 e 的计算包含: 从值 y 得到值 x,并首先检查是否 $x^e = y$ 对 p 取模,其次检查是否 $x^e = y$ 对 q 取模。
- [0099] 优选地,集合 E 包括至少以下 e_i 值: 3, 17, $2^{16} + 1$ 。
- [0100] 本发明还提供了一种电子部件,其特征在于,包括用于执行上述定义的方法的装置。
- [0101] 本发明还包括包含如所定义的电子部件的智能卡。
- [0102] 本发明还提供了一种安全地执行公开密钥密码术算法的方法,所述公开密钥由整数 n 和公开指数 e 构成,所述整数 n 为两个大素数 p 和 q 的乘积,所述方法包括确定包含预定数量的值 e_i (能够对应于公开指数 e 的值) 的集合 E,所述 e_i 值为素数,所述方法其特征

在于,包含以下步骤:

[0103] a) 从集合 E 的值中选择值 e_i ;

[0104] b) 如果 $\Phi(p) = \Phi(q)$, 检验所选择的 e_i 值是否满足关系:

[0105] $(1-e_i, d)$ 对 n 取模 $< e_i \cdot 2^{(\Phi(n)/2)+1}$

[0106] 或者所述关系被简化为:

[0107] $(-e_i, d)$ 对 n 取模 $< e_i \cdot 2^{(\Phi(n)/2)+1}$

[0108] 此处 $\Phi(p)$, $\Phi(q)$ 和 $\Phi(n)$ 为分别给出对数字 p 、数字 q 和数字 n 进行编码的位数的函数;

[0109] 否则,当 p 和 q 不平衡时,检验所选择的 e_i 值是否满足下列关系:

[0110] $(1-e_i, d)$ 对 n 取模 $< e_i \cdot 2^{g+1}$

[0111] 或者所述关系被简化为:

[0112] $(-e_i, d)$ 对 n 取模 $< e_i \cdot 2^{g+1}$

[0113] 如果 $\Phi(p)$ 和 $\Phi(q)$ 已知,那么 $g = \max(\Phi(p), \Phi(q))$, 否则 $g = \Phi(n)/2+t$, 此处 t 代表不平衡因子或者对该因子的一个限制。

[0114] c) 如果满足在前述步骤中应用的检验关系,因此 $e = e_i$, 考虑到在所述密码术算法计算中使用 e 值,因而存储 e ;

[0115] 否则,重复前面步骤同时从集合 E 中为 e_i 选择另一值,直到一个 e_i 值能够赋给 e , 如果没有 e_i 值可以赋给 e , 那么观察到不能执行使用值 e 的所述密码术算法的计算。

[0116] 以公开指数出现的概率顺序作为选择 e_i 值的顺序,这样的事实使得能够节省时间。因此,可能优选以下面的顺序选择 e_i 值: $e_0 = 2^{16}+1$, $e_1 = 3$, $e_2 = 17$ 。

[0117] 在一个变型中,对于所有 i 的值, $e_i \leq 2^{16}+1$, 并且步骤 b) 由另一检验步骤替代,包含:

[0118] 如果 $\Phi(p) = \Phi(q)$, 检验所选择的 e_i 值是否满足关系:

[0119] $(1-e_i, d)$ 对 n 取模 $< e_i \cdot 2^{(\Phi(n)/2)+17}$

[0120] 或者所述关系被简化为:

[0121] $(-e_i, d)$ 对 n 取模 $< e_i \cdot 2^{(\Phi(n)/2)+17}$

[0122] 此处 $\Phi(p)$, $\Phi(q)$ 和 $\Phi(n)$ 为分别给出对数字 p 、数字 q 和数字 n 进行编码的位数的函数;

[0123] 否则,当 p 和 q 不平衡时,检验所选择的 e_i 值是否满足下面的关系:

[0124] $(1-e_i, d)$ 对 n 取模 $< e_i \cdot 2^{g+17}$

[0125] 或者所述关系被简化为:

[0126] $(-e_i, d)$ 对 n 取模 $< e_i \cdot 2^{g+17}$

[0127] 如果 $\Phi(p)$ 和 $\Phi(q)$ 已知,那么 $g = \max(\Phi(p), \Phi(q))$, 否则 $g = \Phi(n)/2+t$, 此处 t 代表不平衡因子或者对该因子的一个限制。

[0128] 在另一个变型中,步骤 b) 由另一检验步骤替代,包含:

[0129] 检验所选择的 e_i 值是否满足关系,由此:

[0130] $(1-e_i, d)$ 对 n 取模的第一最高有效位为 0;

[0131] 或者简化所述关系,由此:

[0132] $(-e_i, d)$ 对 n 取模的第一最高有效位为 0。

- [0133] 优选地,对第一 128 个最高有效位执行检验。
- [0134] 在本发明的优选实施例中,密码术算法基于标准模式 RSA 型算法。
- [0135] 根据一个特性,当 e_i 值已经赋给 e 时,使用值 e 的计算包含:
- [0136] 选择随机整数 r :
- [0137] 计算值 d^* 使得 $d^* = d + r \cdot (e \cdot d - 1)$, 和
- [0138] 执行算法的私有操作,其中通过使用关系 $x = y^{d^*}$ 对 n 取模从值 y 得到值 x 。
- [0139] 根据另一特性,当 e_i 值已经赋给 e 时,在算法的私有操作之后,使用值 e 的计算包含:从值 y 得到值 x ,并且使用值 e 的计算包含检查是否 $x_e = y$ 对 n 取模。
- [0140] 优选地,集合 E 包括至少下列 e_i 值: $3, 17, 2^{16}+1$ 。
- [0141] 本发明还提供了一种电子部件,其特征在于,它包括用于执行上面所定义的方法的装置。
- [0142] 本发明还提供了包含如所定义电子部件的智能卡。
- [0143] 从下面以非限制表示方式进行的描述中,本发明的其它特征和优势将更加清晰。
- [0144] 因此,本发明描述了各种可能确定非先前公知的公开指数 e 值的技术。这些技术能够通过任意配备有适当的加密计算装置的电子部件或者装置实施,尤其是智能卡。
- [0145] 本发明基于下面的发现:假设集合 E 包括至少下列 e 值: $e_0 = 2^{16}+1, e_1 = 3, e_2 = 17$, 该值的集合 E 涵盖了通常使用在 RSA 型密码术算法计算中的公开指数值的大约 95%。
- [0146] 本发明提出对 RSA 算法标准模式有效的第一技术,通常包含选择 e_0 并检查是否 $e = e_0$; 如果 $e \neq e_0$, 那么对 e_1 进行尝试; 如果 $e \neq e_1$ 那么对 e_2 进行尝试。
- [0147] 可能的是,对于对应于 5% 的其它情况的特定应用, e 既不等于 e_0 也不等于 e_1 , 也不等于 e_2 。因此更加通常的是 e 的值由 e_i 指定。所述方法最终包含从预计的 e_i 值中选择值 e_i 并检查是否 $e = e_i$ 。
- [0148] 更加具体地,用于找出对 RSA 算法标准模式有效的 e 值的第一技术是基于以下推理:
- [0149] 在标准模式中,私有算法(执行用于签名或用于解密消息的操作)具有模数 n 的值和私有指数 d 的值。
- [0150] 因此,根据表达式 (1), 存在一个整数 k 使得:
- [0151] $e \cdot d = 1 + k \Phi(n)$
- [0152] 即, $1 - e \cdot d = -k \Phi(n) = -k \cdot (n - p - q + 1)$
- [0153] 通过对 n 取模简化表达式两端,可以得到下面式子:
- [0154] $1 - e \cdot d = k(p + q - 1) \text{ (对 } n \text{ 取模)}$
- [0155] 注意到当 e 比较小时,总得到 $k < e$, 前面的表达式还可以写为:
- [0156] $(1 - e \cdot d) \text{ 对 } n \text{ 取模} = k(p + q - 1) \quad (6)$
- [0157] 等式 6 的左侧大小与模数 n 大小基本相同,而当 p 和 q 平衡, $\Phi(p) = \Phi(q)$ 时,即大小相同时,右侧具有根据下面表达式定义的大小:
- [0158] $k \cdot (p + q - 1) < e \cdot 2^{(\Phi(n)/2)+1}$
- [0159] 此处 $\Phi(p)$, $\Phi(q)$ 和 $\Phi(n)$ 为分别给出对数字 p 、数字 q 和数字 n 进行编码的位数的函数。
- [0160] 当 p 和 q 大小不同时,当 $\Phi(p)$, $\Phi(q)$ 已知时,函数 $g = \max(\Phi(p), \Phi(q))$, 即被

称为给出 p 和 q 最大长度的函数 ; 否则 $g = \Phi(n)/2+t$, 此处 t 代表不平衡因子, 或者代表对该因子的一个限制。当 p 和 q 不平衡时, 上述表达式的公式为 :

$$[0161] \quad k \cdot (p+q-1) < e \cdot 2^{1+g}$$

[0162] 由于 $n = p \cdot q$, 如果 p 和 q 平衡, 则得到表达式 $p+q < 2^{(\Phi(n)/2)+1}$; 相反, 如果 p 和 q 不平衡, 那么 : $p+q < 2^{1+g}$

[0163] 因此, 对于集合 E 中所有可能的 e_i 值, 如果 $\Phi(p) = \Phi(q)$, 则执行检验以确定所选择的 e_i 值是否满足预定关系 :

$$[0164] \quad (1-e_i \cdot d) \text{ 对 } n \text{ 取模} < e_i \cdot 2^{(\Phi(n)/2)+1} \quad (7)$$

[0165] 否则, 执行检验以确定所选择的 e_i 值是否满足预定关系 :

$$[0166] \quad (1-e_i \cdot d) \text{ 对 } n \text{ 取模} < e_i \cdot 2^{g+1} \quad (7')$$

[0167] 如果满足所应用的预定检验关系, 那么 $e = e_i$ 并存储 e ;

[0168] 否则从集合 E 中为 e_i 选择另一值, 并重复前述步骤。

[0169] 在第一变型中, 用于找出 e 的值的检验 :

$$[0170] \quad (1-e_i \cdot d) \text{ 对 } n \text{ 取模} < e_i \cdot 2^{(\Phi(n)/2)+1} \text{ 或者}$$

[0171] $(1-e_i \cdot d) \text{ 对 } n \text{ 取模} < e_i \cdot 2^{g+1}$, 根据 p 和 q 是否平衡, 可以使用下面检验替换 :

$$[0172] \quad (1-e_i \cdot d) \text{ 对 } n \text{ 取模} < B ;$$

[0173] 此处当 $\Phi(p) = \Phi(q)$ 时 $B \geq [\max(e_i)] 22^{(\Phi(n)/2)+1}$;

[0174] 否则, $B \geq [\max(e_i)] 2^{g+1}$ 。

[0175] 在我们实例中, $E = \{2^{16}+1, 3, 17\}$ 。因此, 对于所有的 i 值, $e_i \leq 2^{16}+1$, 因此前面检验能够以下面的方式简化, 包含检查是否 :

[0176] 当 $\Phi(p) = \Phi(q)$ 时, $(1-e_i \cdot d) \text{ 对 } n \text{ 取模} < B$, 此处 $B = 2^{(\Phi(n)/2)+17}$;

[0177] 否则, $(1-e_i \cdot d) \text{ 对 } n \text{ 取模} < B$, 此处 $B = 2^{g+17}$ 。

[0178] 在检验的第二变型中, 可能进一步通过检查 $(1-e_i \cdot d) \text{ 对 } n \text{ 取模}$ 的最高有效位 (例如 128 个最高有效位) 是否为 0 简化前述检验,。

[0179] 最终, 对于第一技术, 最后的简化包含确定用于检验 e_i 值的预定关系, 该最后的简化从下列关系开始 :

$$[0180] \quad (-e \cdot d) \text{ 对 } n \text{ 取模} = k(p+q-1)-1$$

[0181] 代替关系 (6)。

[0182] 因此, 根据该简化, 可以得到下面的用于检验关系 (7, 7') 的简化 :

[0183] 如果 $\Phi(p) = \Phi(q)$, $(-e_i \cdot d) \text{ 对 } n \text{ 取模} < e_i \cdot 2^{(\Phi(n)/2)+1}$;

[0184] 否则, $(-e_i \cdot d) \text{ 对 } n \text{ 取模} < e_i \cdot 2^{g+1}$ 。

[0185] 对于第一变型, 得到下面简化检验 :

[0186] $(-e_i \cdot d) \text{ 对 } n \text{ 取模} < B$, 此处如果 $\Phi(p) = \Phi(q)$, $B = 2^{(\Phi(n)/2)+17}$, 否则, $B = 2^{g+17}$ 。

[0187] 并且, 对于检验的第二变型, 可以得到以下的简化检验, 包含检查 $(-e_i \cdot d) \text{ 对 } n \text{ 取模}$ 的第一最高有效位是否为 0。

[0188] 不管所执行的变型是否是它的简化形式, 如果对于 e_i 值检验不满足, 则从集合 E 中为 e_i 选择另一值, 直到找到相匹配值。

[0189] 如果, 对于涉及上述第一技术的变型, 在 e_i 值中不存在一个值使得 $e = e_i$ 那么, 仍然观察到涉及 e 的标准模式 RSA 密码术算法的计算不能执行。

[0190] 相反,当通过任一变型从预定值 E 的集合的 e_i 值中找到了 e 的值时,然后通过确认应用私有操作根据 y 值所得到的值 x 满足关系 $x^e = y$ 对 n 取模,就可能检查每个密码术算法(包含对消息解密或者生成签名)的私有操作(3)。否则,不返回解密消息或者签名以避免任意密码分析。

[0191] 如上所述,一旦 e 已知,本发明的方法就可以应用于对策,尤其是抵御 DPA(和 SPA) 类型攻击,如上所述。因此,这种方法包含:选择随机整数 r ;计算值 d^* 使得 $d^* = d + r \cdot (e \cdot d - 1)$,和执行算法的私有操作,其中通过使用关系 $x = y^{d^*}$ 对 n 取模从值 y 得到值 x 。

[0192] 最后,本发明涉及用于从包括预定值 e_i 的集合 E 中找到指数 e 的值的第二技术。如下所述,该技术既可应用于 RSA 算法的标准模式又可用于 CRT 模式。

[0193] 所述技术尤其包含改善 D1 中所提出的方法。因此,执行下列步骤:

[0194] a) 确定值 $\Phi = \prod_{e_i \in E} e_i$

[0195] 以使对于任意属于 E 的 e_i , Φ/e_i 小于 $\Phi(n)$,此处 Φ 为欧拉 Φ 函数;

[0196] b) 将 Φ 值应用于预定的计算;

[0197] c) 对于每个 e_i ,检验所述预定计算的结果是否与值 Φ/e_i 相等;

[0198] 如果相等,那么将值 e_i 赋给 e ,考虑到在所述密码术算法计算中要使用 e ,因而存储 e ;

[0199] 否则,观察到使用值 e 的密码术算法的计算不能执行。

[0200] 在标准模式中,步骤 b) 的预定计算包含计算值 C 以使:

[0201] $C = \Phi \cdot d$ 对 $\Phi(n)$ 取模,此处 d 为标准模式中使得 $e \cdot d$ 对 $\Phi(n)$ 取模 $= 1$ 的 RSA 算法的相应私有密钥。

[0202] 例如,假设 $E = \{e_0 = 3, e_1 = 17, e_2 = 2^{16}+1\}$,那么

[0203] $\Phi = e_0 \cdot e_1 \cdot e_2 = 3 \cdot 17 \cdot (2^{16}+1)$ 。

[0204] 因此,使用 $C = \Phi \cdot d$ 对 $\Phi(n)$ 取模:

[0205] 如果, $C = 17 \cdot (2^{16}+1) = \Phi/e_0$,则 $e = e_0 = 3$;

[0206] 如果, $C = 3 \cdot (2^{16}+1) = \Phi/e_1$,则 $e = e_1 = 17$;

[0207] 如果, $C = 3 \cdot 17 = \Phi/e_2$,则 $e = e_2 = 2^{16}+1$;

[0208] 通过可能得到 C 值的单个模数计算,因此有可能从集合 E 中找到指数 e 的值,作为所述计算的结果函数。

[0209] 在一个替代方法中,步骤 b) 的预定计算包含计算值 C 使得:

[0210] $C = \Phi \cdot d$ 对 $\Phi(n)$ 取模,此处 d 为标准模式 RSA 算法的相应私有密钥,但是以对卡麦克函数取模计算,替代对欧拉 Φ 函数取模,因此, $e \cdot d$ 对 $\Phi(n)$ 取模 $= 1$, Φ 为卡麦克函数。

[0211] 当 e 的值被找到并存储时,执行值 e 的标准模式密码术算法的计算包含避开故障攻击并在一个地方设置对策,尤其是抵御 DPA(和 SPA) 型攻击,这些计算与参考第一技术所描述的计算相同。

[0212] 在一个变型中,当 RSA 算法执行在 CRT 模式中时,步骤 b) 的预定计算包含值 C 的计算使得:

[0213] $C = \Phi \cdot d_p$ 对 $(p-1)$ 取模,此处 d_p 为使得 $e \cdot d_p$ 对 $(p-1)$ 取模 $= 1$ 的 RSA 算法的相

应私有密钥；

[0214] 或者事实上，使得：

[0215] $C = \Phi \cdot d_q$ 对 $(q-1)$ 取模，此处 d_q 为使得 $e \cdot d_q$ 对 $(q-1)$ 取模 = 1 的 RSA 算法的相应私有密钥；

[0216] 或者事实上计算两个 C 值，并考虑两个检验中的至少一个给出的 e 值：

[0217] 当 e 值确实已经找到并存储时，执行值 e 的 CRT 模式密码术算法的计算包含避开故障攻击。

[0218] 然后，通过确认应用 CRT 模式中的私有操作从 y 值得到的值 x 是否满足第一关系 $x^e = y$ 对 p 取模和第二关系 $x^e = y$ 对 q 取模，就可能检查密码术算法的 CRT 模式的每个私有操作（包含解密消息或者产生签名）。