慎用中国剩余定理提高 RSA 算法效率

孙　宇
（北京师范大学，北京 100875）
E-mail：girlinsunshine@263.net

摘　要　模幂运算的效率决定了 RSA 密码系统的执行速度。由于中国剩余定理对于提高 RSA 算法的模幂运算效率有显著作用，因而被广泛使用。但直接使用中国剩余定理是不安全的，容易受到出错攻击。文章就介绍了一种出错攻击方法，并给出了一些对抗这一攻击的具体措施。

关键词　模幂　中国剩余定理　RSA 算法　出错攻击

文章编号 1002-8331-(2004)28-0156-02　**文献标识码** A　**中图分类号** TP301.6

Careful Design RSA Cryptosystem Based on Chinese Remainder Theorem

Sun Yu
(Beijing Normal University, Beijing 100875)

Abstract: Exponentiation often determines whether a give RSA cryptosystem is practical.So Chinese Remainder Theorem (CRT) has been widely employed to speed up the RSA algorithm.However, careless implementations of such systems could be vulnerable.This article describes a fault attack that uses one faulty computation, in some explained context, is enough to recover the secret key.Countermeasures against this attack are also suggested.

Keywords: exponentiation, Chinese Remainder Theorem(CRT), RSA algorithm, fault attack

1　引言

1976 年，Diffie 和 Hellman 发表了开创性的论文“密码学的新方向(New Directions in Cryptography)”[1]，奠定了公钥密码学的基础。此后，提出了多种公钥密码算法，其中许多后来被证明是不安全的，而那些被视为安全的算法，有许多都不实用，要么密钥太大，要么密文远远大于明文。目前，实际应用最广泛的公钥密码算法是依赖于大整数分解问题的 RSA 算法[2]。不过这一算法执行速度比对称算法慢得多，因此，提高算法计算效率一直是国内外学者关注的研究方向。RSA 算法加解密都是做一个模幂运算，出于安全性考虑，密钥一般要求在 1024~2048 比特位之间，所以这一运算最消耗时间，是造成 RSA 算法执行速度缓慢的根本原因。

最近，在“一种高效率的 RSA 模幂算法的研究”[3]一文中提出直接使用中国剩余定理提高模幂运算效率的方法，这虽然能提高运算效率，但也存在严重地安全隐患。该文指出了利用计算中出现的错误来攻击基于中国剩余定理的 RSA 密码系统的方法，并给出了对抗这种攻击的一些措施。

2　中国剩余定理加速 RSA 的模幂运算简介

为使文章便于理解，叙述中国剩余定理加速 RSA 模幂运算的方法如下：

对于用 RSA 签名\加密的一方，是计算一个：

$C=M^d(\mathrm{mod}\ n)$

这里 $n=p\cdot q$，p 和 q 是两个二进制长度接近的大素数。由于签名\加密者实际知道 n 的分解即 p 和 q，所以这一计算可以分解为两部分分别进行：

$C_p=M^d(\mathrm{mod}\ p)$，$C_q=M^d(\mathrm{mod}\ q)$

计算完成后，应用中国剩余定理就能得出最终结果。注意，根据费马小定理知道，上面两式仅需要计算：

$C_p=M^{d_1}(\mathrm{mod}\ p)$，$C_q=M^{d_2}(\mathrm{mod}\ q)$

这里 $d_1=d\mathrm{mod}(p-1)$，$d_2=d\mathrm{mod}(q-1)$。根据 RSA 算法的要求，私钥 d 的二进制长度接近 n 的长度，因此，d_1 和 d_2 的二进制长度仅有 n 的一半左右，这样就节省了大量的计算工作。最后，应用中国剩余定理就能计算出的值：

$$C=C_pc_1\frac{pq}{p}+C_qc_2\frac{pq}{q}(\mathrm{mod}\ n)=C_pc_1q+C_pc_2p(\mathrm{mod}\ n)$$

这里，$c_1=q^{-1}(\mathrm{mod}\ p)$，$c_2=p^{-1}(\mathrm{mod}\ q)$。也就是：$C=C_p(q^{-1}\mathrm{mod}\ p)q+C_q(p^{-1}\mathrm{mod}\ q)p(\mathrm{mod}\ n)$。

假定 p 和 q 的二进制长度均为 $\frac{k}{2}$，d 的二进制长度 2 与 n 相当为 k。d_1，d_2，$q^{-1}(\mathrm{mod}\ p)$，$p^{-1}(\mathrm{mod}\ q)$均预先计算好。再假设乘法需要 2 数量级的位操作，加法和减法需要 k 数量级的位操作。如果应用中国剩余定理计算模幂，主要工作花在计算 C_p 和 C_q 上，而合成 C 的计算至多只需要一个与 k 无关固定数量的位操作，在计算时间复杂度时，可以忽略不计。这样使用标准二进制算法[4]，计算 C_p 和 C_q 都需要 $\frac{3}{2}\left(\frac{k}{2}\right)$ 次 $\frac{k}{2}$ 比特的乘法操

作者简介：孙宇(1973-)，女，博士，现就职于北京师范大学管理学院，研究方向为信息管理。

作，总共需要 $2\frac{3}{2}\left(\frac{k}{2}\right)\left(\frac{k}{2}\right)^2$ 次位操作。如果不用中国剩余定理，同样使用标准二进制算法，需要 $\frac{3}{2}k$ 次 k 比特的乘法操作，总共需要 $\frac{3k^3}{2}$ 次位操作。因此，使用中国剩余定理比不使用大约快 4 倍。这也是国内外，软、硬件执行 RSA 算法普遍使用中国剩余定理的原因。在“一种高效率的 RSA 模幂算法的研究”一文中提到，并行计算 C_p 和 C_q 才能使加速因子接近于 4 的说法是不当的，但这并不是该文讨论的重点。

3 出错攻击方法讨论

3.1 出错攻击方法

在应用中国剩余定理的 RSA 系统中，只要设备执行签名\加密时，满足以下三个条件[5]：

(1)签名\加密消息已知；

(2)在签名\加密时出现了一个错误；

(3)设备输出了错误的签名\密文。

就可能导致系统的大整数 n 被分解开。

如上节所述签名\加密方用自己的私钥计算 $C=M^d(\mathrm{mod}\ n)$。使用中国剩余定理，C 可通过 $C_p=M^d(\mathrm{mod}\ p)$，$C_q=M^d(\mathrm{mod}\ q)$，有效计算出来。假设错误发生在计算 C_p 时，也就是说计算了一个错误值 $C'_p\neq C_p(\mathrm{mod}\ p)$，而 C_q 被正确计算出来。C'_p 和 C_q 就联合产生一个错误的签名\密文 C'。这样有如下性质：

性质，$q=gcd(C'^e-M_p(\mathrm{mod}\ n),n)$ 这里 e 是公开密钥值，$gcd(\cdot)$是求最大公约数。

证明 根据中国剩余定理有：

$$C'=C'_p(q^{-1}\ \mathrm{mod}\ p)q+C_q(p^{-1}\ \mathrm{mod}\ q)p(\mathrm{mod}\ n)$$

$$\therefore\ (C'^e-M(\mathrm{mod}\ n))\mathrm{mod}\ q$$

$$=((C'_p(q^{-1}\ \mathrm{mod}\ p)q)^e+\cdots+(C_p(p^{-1}\ \mathrm{mod}\ q))^e-M(\mathrm{mod}\ n))\mathrm{mod}\ q$$

$$=((C_q(p^{-1}\ \mathrm{mod}\ q))^e-M(\mathrm{mod}\ n))\mathrm{mod}\ q$$

$$=(C^{de}-M)\mathrm{mod}\ q=0$$

而 C' 是一个错误签名\密文：

$$\therefore\ (C'^e-M(\mathrm{mod}\ n))\mathrm{mod}\ p\neq 0$$

$\therefore$ 性质成立。

如果攻击者不知道模数 n，仍有机会恢复得到秘密参数 q。若 e 是一个不太大的数，可能通过直接分解 C'^e-M 得到 q，如果掌握了两个或更多个错误签名\密文，就能通过计算 $\gcd(C_1'^e-M_1,C_2'^e-M_2,\cdots,C_k'^e-M_k)$ 来得到 q 值。

3.2 现实性考虑

出错攻击是一个非常强的攻击方法，在设计 RSA 设备中必须引起重视。只要设备发生了一个错误，将可能导致系统的大整数直接被分解开，使 RSA 系统崩溃。希望 RSA 设备在使用过程中从不出错，显然是不符合实际的。假定使用 RSA 设备的是一个可信第三方，例如，一个银行或认证中心(CA)服务器。它每天可能需要产生成千上万的数字签名，一旦由于某种原因产生了一个错误，整个系统的安全性就不复存在了。这还很自然地导致了“否定服务”攻击，一个攻击者如果发送一封匿名电子邮件，声称自己已经得到了该银行或认证中心服务器的错误签名。无论情况是否属实，都将导致人们不在信任该银行或认证中心，而最终迫使其停止使用当前签名密钥。

如果攻击者采用某些方法恶意诱使设备出错，则攻击成功的可能性将大大增加。可以使用的具体方法包括：重写 ROM，修改 EEPROM，破坏逻辑门电路，监测 RAM 余磁等等。

4 对抗错误攻击的方法

根据出错攻击成功需要的三个必要条件可知，阻断任何一个条件就可以成功阻止出错攻击。以下是几个实用的方法：

(1)冗余计算 C_p 和 C_q 值。做两次 C_p 和 C_q 值的计算，若两次结果不相等，废止本次计算，不输出任何结果数据；否则，计算输出最终值 C。

(2)结构中增加一个认证环节。在 RSA 中签名\加密：$C=M^d(\mathrm{mod}\ n)$，可用公钥 e 加以认证\解密：$M=C^e(\mathrm{mod}\ n)$。将认证\解密计算放在系统的最后一环，系统在自行认证\解密后如与输入数据相等，就输出签名\加密值；否则，本次操作作废。

(3)这一方法是 Shamir[6]提出的。选择一个随机整数 r，并计算如下两个数：

$$C_{pr}=M^{d\ \mathrm{mod}\ \Phi(pr)}(\mathrm{mod}\ pr),C_{qr}=M^{d\ \mathrm{mod}\ \Phi(qr)}(\mathrm{mod}\ pr)$$

这里 $\Phi(\cdot)$是欧拉函数。如果 $C_{pr}=C_{qr}(\mathrm{mod}\ r)$，则认为计算中没有出现错误，最后，用 $C=((C_{pr}\ \mathrm{mod}\ p)(q^{-1}\ \mathrm{mod}\ p)q+(C_{qr}\ \mathrm{mod}\ p)(p^{-1}\ \mathrm{mod}\ q)p)\mathrm{mod}\ n$ 计算出最终值；否则，废止该次操作。

5 结论

设计密码设备，可靠性应该放在首位。通过上面的论述可以看出，在执行 RSA 算法时，直接使用中国剩余定理将给系统带来很大的安全隐患。但是，只要小心使用，基于中国剩余定理的密码系统并不会比一般的密码系统更脆弱。这些工作希望能对设计高可靠性、高效的 RSA 设备有一定的参考价值。

(收稿日期：2004 年 2 月)

参考文献

1.Diffie W，Hellman M E.New directions in cryptography[J].IEEE Transactions on Information Theory，1976，IT-22：644~654

2.Rivest R，Shamir A，Adleman L.A method for obtaining digital signatures and public-key cryptosystems[J].Communications of the ACM，1978，21(2)：120~126

3.饶进平，冯登国.一种高效率的 RSA 模幂算法的研究[J].计算机工程与应用，2003，39(9)：76~77

4.Knuth D E.The art of computer programming，vol.II：seminumerical algorithms[M].Second Edition，MA：Addison-Wesley，1981

5.Joye M，Lenstra A K，Quisquater J-J.Chinese Remaindering based cryptosystems in the presence of faults[J].Journal of Cryptology，1999，2(4)：241~245

6.Shamir A.How to check modular exponentiation[C].In：the rump session of EUROCRYPT'97，1997